GEIR ELLINGSRUD

MA4200—COMMUTATIVE ALGEBRA

These are informal notes for the course MAT4200 autumn 2018. As you will see they are "under construction", so they highly unfinished and errors abound. Some chapters, the first two or three, are not that preliminary and should be readable. Hopefully the rest will improve during the semester. Each chapter has its own version number. If the number is positive, the chapter should be readable(and as usual the higher version number the more ready the chapter is), but if negative (like $-\infty$) it is sketchy if existing at all. I shall indicate major changes, so you can follow the development.

Geir

Contents

Lecture 1

Rings

Preliminary version 1.1 as of 2018-08-22 at 08:11 (typeset 3rd December 2018 at 10:03am)—Prone to misprints and errors and will change.

2018-08-21 Added a few sentences in paragraph 1.2.
2018-08-22 Added some words about isomorphisms, paragraph 1.6.
2018-08-23 Added exersices 1.13 and 1.20. Section 1.3 rewritten in a simpler manner.
30/08/2018 Added a hint to exercise 1.15.

06/09/2018 Added exercise 1.16.

The starring role in commutative algebra is played by the commutative rings and their ideals— they are even the main targets of the investigations. In this chapter we become acquainted with the rings, and the ideals will be introduced in the next chapter.

Commutative rings come in various flavours and arise from different sources. Some are best though of as "number systems" like the ring $\mathbb{Z}$ of integers and its well-known larger siblings the field of rationals $\mathbb{Q}$, the field of real numbers $\mathbb{R}$, and the field of complex numbers $\mathbb{C}$ (this suite continues, but in a non-commutative way; the next two members of the family being the quaternions and the octonians), there are also some little brothers; the fields $\mathbb{Z}/p\mathbb{Z}$ of integral residue classes modulo primes p and the the other finite fields $\mathbb{F}_q$. The earliest systematic study of commutative rings was of various "generalized number systems"; certain subrings of the ring of algebraic numbers. Already Gauss undertook such studies, but it really took off in the nineteenth century with the work of Kronecker's and Dedekind's.

Other commutative rings resemble rings of functions on different kinds of spaces, like continuous functions on topological spaces (with real or complex values) or holomorphic functions in open domains in the complex plain, but the rings most relevant in our context arise in algebraic geometry. These are rings of polynomial functions on so-called algebraic varieties.

The development took a new direction around the middle of the twentieth century, when mathematicians like Zariski and Weil strived for establishing a sound foundation of algebraic geometry, and the recognition of the power of algebraic geometric methods in number theory eventually lead to the happy marriage of algebraic geometry and number theory — consummated by Groethendieck and his invention of schemes.

1.1 Rings

1.1 Recall that a ring is an algebraic structure consisting of a set endowed with two binary operations; an addition which makes A an abelian group, and a multiplication. The multiplication is assumed to be distributive over the addition, and in this course it will always be associative and commutative (or at least almost always). There are of course many extremely interesting non-commutative rings and non-associative rings, but this course is dedicated to rings that are associative and commutative.

The sum of two elements will of course be denoted as $a + b$, and the product will we indicated in the traditional way by a dot or simply by juxtaposition; that is, as $a \cdot b$ or just by ab. The *left distributive law* asserts that $a(b + c) = ab + bc$, and since rings for us are commutative, it follows that the *right distributive law* $(b + c)a = ba + ca$ holds as well.

We shall also assume that all rings have a *unit element*; that is, an element 1_A such that $1_A \cdot a = a$ for all members a of the ring. At most occasions the reference to A will be dropped, and we shall write 1 for the unit element whatever the ring is.

EXAMPLE 1.1 The simplest of all rings are the ring $\mathbb{Z}$ of integers and the rings $\mathbb{Z}/n\mathbb{Z}$ of residue classes of integers modulo n. The traditional numbers systems of real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ are well-known rings. ☆

Zero divisors and nilpotents

1.2 Generally, ring-elements can behave quite differently than we are used to in a classical setting. It might very well happen that $ab = 0$ without neither a nor b being zero. Such elements are called *zero divisors*. Be aware that the familiar *cancellation law* does not hold in a ring with zero divisors in that $ab = ac$ not necessarily implies that $b = c$. Rings without zero divisors are called *integral domains* or, for short, *domains*.

Zero divisors (*nulldivisorer*)

Integral domains (*Integritetsområder*)

Obviously, elements that are not zero divisors are called *non-zero divisors*, another name being *regular elements*. A regular element a has the virtue that $xa = 0$ implies that $x = 0$ and can therefore be cancelled from equalities like $ab = ac$ (the difference $b - c$ being killed by a vanishes).

Non-zero divisors (*Ikke-nulldivisorer*)

Regular elements (*Regulære elementer*)

For instance, in case n is a composite number, say $n = pq$, the ring $\mathbb{Z}/n\mathbb{Z}$ has zero divisors; it holds true that $pq = 0$, and p and q are both different from zero (neither having n as a factor).

A more geometric example could be the ring of continuous functions on the space X which is the union of the x-axis and the y-axis in the plane. On X the function xy vanishes identically, but neither x nor y does (x does not vanish on the y-axis and y not on the x-axis).

1.3 It might also happen that a powers of a non-zero elements vanish, *i.e.* one has $a^n = 0$ for some natural number n, but $a \neq 0$. For instance, in the ring

$\mathbb{Z}/p^2\mathbb{Z}$ one has $p^2 = 0$, but $p \neq 0$. Such elements are called *nilpotent*. Rings deprived of nilpotent elements, are said to be *reduced*.

Nilpotent elements (*nilpotente elementer*)
Reduced rings (*reduserte ringer*)

Units and fields

1.4 Division by non-zero elements is generally not possible in rings. For instance, if p and q are two different primes in $\mathbb{Z}$, the fraction p/q is not an integer and does not lie in $\mathbb{Z}$. Elements in a ring A that are invertible, *i.e.* ring-elements a for which there is an element a^{-1} in A with $aa^{-1} = 1$, are called *units*. They form an abelian group under multiplication which we shall denote by A^*.

Units (*enheter*)

Rings A all whose non-zero members are invertible; that is, which satisfy $A^* = A\backslash\{0\}$, are called *fields*. In fields division by non-zero elements can be performed unconditionally.

Fields (*kropper*)

EXAMPLE 1.2 Well-known fields are the fields of rational numbers $\mathbb{Q}$, of real numbers $\mathbb{R}$ and of complex numbers $\mathbb{C}$. If p is a prime number, the ring $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p is a field usually denoted by $\mathbb{F}_p$. It is a finite field having p elements. ☆

Examples

1.3 We do not assume that $1 \neq 0$ although it holds in all but one ring. The exception is the so-called *null-ring*. If in a ring it holds that $0 = 1$, one has $a = a \cdot 1 = a \cdot 0 = 0$, so zero will be the sole element. The only role the null-ring plays and the only reason not to throw it over board, is that it allows significantly simpler formulations of a few results. It does not merit a proper notation (well…, one alway has the alternative 0).

The null-ring (*nullringen*)

1.4 The set of polynomials $\mathbb{Q}[x_1, \ldots, x_r]$ in r variables $x_1, \ldots, x_r$ with rational coefficients is clearly a ring with the usual sum and product, as are the set of real polynomials $\mathbb{R}[x_1, \ldots, x_r]$ and the set of complex polynomials $\mathbb{C}[x_1, \ldots, x_r]$.

1.5 The complex rational functions in a variable x form a field $\mathbb{C}(x)$. The elements are meromorphic functions in $\mathbb{C}$ expressible as the quotient $p(x)/q(x)$ of two polynomials p and q and q not being identically zero.

1.6 For any set $X \subseteq \mathbb{C}^r$ one may consider the set of *polynomial functions* on X; that is, the functions on X that are restrictions of polynomials in r variables. They form a ring $A_{\mathbb{C}}(X)$ under point-wise addition and multiplication.

Polynomial functions (*polynomiale funskjoner*)

1.7 Associated with any topological space X are the sets $C_{\mathbb{R}}(X)$ and $C_{\mathbb{C}}(X)$ of of continuous functions on X assuming respectively real or complex values. Point-wise addition and multiplication make them (commutative) rings. When X has more structure than just a topology, there are further possibilities. Two

instances being the ring of smooth functions on a smooth manifold, and the ring $\mathcal{O}(\Omega)$ of holomorphic functions in an open domain Ω of the complex plane.

1.8 An example of a class of rings, important in algebraic number theory, is the class of the *quadratic extensions* $\mathbb{Z}[\sqrt{n}] = \{ a + b\sqrt{n} \mid a, b \in \mathbb{Z} \}$, where n is any integer (positive or negative). These rings are contained in the field of complex numbers $\mathbb{C}$ and inherit their ring structure from $\mathbb{C}$; they are closed under addition (which is obvious) and multiplication:

quadratic extensions (kvadratiske utvidelser)

$$(a + b\sqrt{n})(a' + b'\sqrt{n}) = (aa' + nbb') + (ab' + a'b)\sqrt{n}.$$

☆

Homomorphisms

When studying mathematical objects endowed with a certain structure—like rings for instance—maps preserving the structure are fundamental tools. Working with topological spaces one uses continuous maps all the time, and linear algebra is really about linear maps between vector spaces. And of course, the theory of groups is inconceivable without group homomorphisms; that is, maps respecting the group laws. A new class of objects in mathematics is always accompanied by a new class of maps. This observation can be formalized and leads to the definition of *categories*—see xxx.

categories (kategorier)

1.5 In our present context the relevant maps are the so-called *ring homomorphism*, which also will be referred to as *maps of rings* or *ring-maps*. These are maps $\phi\colon A \to B$ between two rings A and B preserving all the structures around; that is, the additive group structure, the multiplication and the unit element 1. In other words, they comply to the rules

Ring homomorphisms (ringhomomorfier)

- $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(0) = 0$;
- $\phi(ab) = \phi(a)\phi(b)$ and $\phi(1) = 1$.

The sum of two maps of rings is in general *not* a map of rings (it is additive, but does not respect the multiplication) neither is their product (it respects multiplication, but not addition), but of course, the composition of two composable ring-maps is a ring-map.

1.6 A homomorphism $\phi\colon A \to B$ is an *isomorphism* if there is a ring homomorphism $\psi\colon B \to A$ such that the two relations $\psi \circ \phi = \mathrm{id}_A$ and $\phi \circ \psi = \mathrm{id}_B$ hold true. One most often writes ϕ^{-1} for the inverse map, and it is common usage to call isomorphisms *invertible* maps. For ϕ to be invertible it suffices it be *bijective*. Multiplication will then automatically be respected since when ϕ is injective, $\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b)$ is equivalent to $ab = \phi(\phi^{-1}(a)\phi^{-1}(a))$, and

Isomorphisms of rings (isomorfier av ringer)

the latter relations is a consequence of ϕ respecting multiplication. Applying ϕ^{-1} to $\phi(1_A) = 1_B$ one sees that $\phi^{-1}(1_B) = 1_A$, so the inverse map sends the unit element to the unit element as well.

Examples

1.9 So-called *evaluation maps* are omnipresent examples of ring homomorphisms. To illustrate this concept, we pick a point $a \in \mathbb{C}^n$. Sending a polynomial f to the value it assumes at a, gives a map $\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$, and by the very definition of the ring structure of the polynomial ring this is a map of rings.

Any ring A of functions—say with complex values—on any topological space X possesses analogue evaluation maps. The operations in A being defined point-wise the map $f \mapsto f(x)$ is a ring-map from A to $\mathbb{C}$ for any point $x \in X$.

1.10 Another series of well-known examples of ring-maps are the maps $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ that send an integer a to its residue class $[a]$ modulo the integer n.

☆

Subrings and polynomial expressions

1.7 We begin by recalling the notion of a polynomial expression. Assume given a ring A and sequence $a = (a_1, \ldots, a_r)$ of elements from A. For any multi-index $\alpha = (\alpha_1, \ldots, \alpha_n)$; that is, a sequence on non-negative integers, one has the *monomial expression*

Monomial expression (*monomiale uttrykk*)

$$a^\alpha = a_1^{\alpha_1} \cdot \ldots \cdot a_n^{\alpha_n}.$$

These expressions show an exponential behavior in that $a^\alpha \cdot a^\beta = a^{\alpha+\beta}$. A *polynomial expression* in the a_i's is just a finite linear combination of such monomials. Frequently one wants to confine the coefficients to lie in a specific subset S of A, and then one speaks about *polynomial expressions with coefficients in S*. They are thus elements of A shaped like

Polynomial expressions (*polynomiale uttrykk*)

$$\sum_\alpha s_\alpha \cdot a^\alpha = \sum_\alpha s_\alpha \cdot a_1^{\alpha_1} \cdot \ldots \cdot a_n^{\alpha_n},$$

where the summation extends over all multi-indices, and where the non-zero coefficients are finite in number and confined to lie in S.

A successive application of the distributive law gives the classical formula for the product of two polynomial expressions:

$$(\sum_\alpha s_\alpha \cdot a^\alpha) \cdot (\sum_\beta t_\beta \cdot a^\beta) = \sum_\gamma (\sum_{\alpha+\beta=\gamma} s_\alpha t_\beta) \cdot a^\gamma. \tag{1.1}$$

Subrings (*Underringer*)

1.8 A *subring* B of A is a ring contained in A whose ring operations are induced from those of A. Phrased differently, it is an additive subgroup containing the unit element which is closed under multiplication; to be specific, it holds that $0 \in B$ and $1 \in B$, and for any two elements a and b belonging to B, both the sum $a + b$ and the product ab belong to B. The intersection of any number of subrings of A is a clearly subring.

EXAMPLE 1.11 The integers $\mathbb{Z}$ is a subring of the rationals $\mathbb{Q}$. ☆

1.9 Given a ring A and a subring B and a set of elements $a_1, \ldots, a_r$ from A. One constructs a subring $B[a_1, \ldots, a_r]$ of A as the set of all polynomial expressions

$$\sum b_\alpha \cdot a_1^{\alpha_1} \cdot \ldots \cdot a_r^{\alpha_r}$$

where $\alpha = (\alpha_1, \ldots, \alpha_r)$ runs through the multi-indices and the b_α's are elements from B, only finitely many of which are different from zero. It is straightforward to check, using the classical formula (1.1) above, that this subset is closed under multiplication and hence is a subring of A (it is obviously closed under addition). It is called the *subring generated* by the a_i's over B, and is the smallest subring of A containing the ring B and all the elements a_i. Common usage is also to say that $B[a_1, \ldots, a_r]$ is obtained by adjoining the a_i's to B.

Subrings generated by elements (*underringer generert av elementer*)

This construction works fine even for infinitely many a_i's since each polynomial expression merely involves finitely many of them. Thus there is a subring $B[a_i | i \in I]$ for any subset $\{a_i\}_{i \in I}$ of A.

Examples

1.12 Let n be an integer. The ring $\mathbb{Z}[1/n] = \{ m/n^i \mid i \in \mathbb{N}_0, m \in \mathbb{Z} \}$ is a subring of $\mathbb{Q}$. The elements are the rational numbers whose denominator is a power of n. More generally, if S is any set of integers, one may form $\mathbb{Z}[n^{-1} | \, n \in S]$, which is the subring of $\mathbb{Q}$ consisting of the rational numbers whose denominator is a product of numbers from S.

Be aware that quite different sets S can give rise to the same subring. For instance, when $p_1, \ldots, p_r$ are the primes occurring in the prime factorization of the integer n, it holds true that $\mathbb{Z}[1/n] = \mathbb{Z}[p_1^{-1}, \ldots, p_r^{-1}]$.

1.13 The subring $\mathbb{C}[t^2, t^3]$ of $\mathbb{C}[t]$ is a ubiquitous example in algebraic geometry; it is the coordinate ring of a so-called cusp and consists of all polynomials whose first derivative vanishes at the origin; of phrased differently, the polynomials without a linear term.

1.14 The subring $\mathbb{C}[x, 1/x]$ of the rational function field $\mathbb{C}(x)$ consists of elements of the form $p(x^{-1}) + c + q(x)$ where p and q are polynomials vanishing at the origin and c a complex constant.

☆

The prime ring and the characteristic

1.10 Every ring has a canonical subring called the *prime ring*. The unit element 1 in A generates an additive cyclic subgroup of A whose elements are just sums of 1 or -1 a certain number of times; that is, they are shaped like $n = 1 + \ldots + 1$ or $n = -1 - \ldots - 1$. This subgroup is obviously closed under multiplication and is hence a subring. It is called *the prime ring* of A.

The prime ring (*primringen*)

As is well known, a cyclic group is either finite and isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some positive integer n, or it is infinite and isomorphic to $\mathbb{Z}$. The prime ring is therefore either isomorphic to one of the rings $\mathbb{Z}/n\mathbb{Z}$ or to $\mathbb{Z}$. In the former case the integer n is called the *characteristic* of A, in the latter case one says that A is of *characteristic zero*. So, in any case, the characteristic of a ring A is a non-negative integer attached to A.

The characteristic of a ring (*karakteristikken til en ring*)

1.11 Any field contained in A contains the prime ring. Hence, if A contains a field, the characteristic is either prime or zero. In case it is prime, the prime ring equals the field $\mathbb{F}_p$, and in case the characteristic is zero, the ring A contains $\mathbb{Q}$ as well. We say that $\mathbb{F}_p$ respectively $\mathbb{Q}$ is the *prime field* of A.

The prime field (*primkroppen*)

Algebras

Frequently when working in commutative algebra there are "coefficients" around; that is, one is working over a "ground ring". So the most natural objects to work with are perhaps not rings, but the so-called *algebras*.

1.12 The notion of an algebra is a relative notion involving two rings A and B. To give a *B-algebra structure* on A is just to give a map of rings $\phi\colon B \to A$. One may then form products $\phi(b) \cdot a$ of elements a from A with elements of the form $\phi(b)$. The map ϕ (even though it is an essential part of the B-algebra structure of A) is often tacitly understood and suppressed from the notation; one simply writes $b \cdot a$ for $\phi(b) \cdot a$. Later on, when we have introduced modules, a B-algebra structure on a ring A will be the same as a B-module structure on A.

Algebras (*Algebraer*)

Example 1.15 Every ring has a canonical structure as a $\mathbb{Z}$-algebra (defined as in Paragraph 1.10 above). The class of algebras is therefore a strict extension of the class of rings. Since a ring is an algebra over any subring, over-rings give a large number of examples of algebras. ☆

1.13 Faithful to the principle that any new type of objects is accompanied by a corresponding new type of maps; one says that a map of rings $\phi\colon A \to A'$ between two B-algebras is an *B-algebra homomorphism*[1] if it respects the action of B; in other words, it holds true that $\phi(b \cdot a) = b \cdot \phi(a)$ for all elements $a \in A$ and $b \in B$. Composition of two composable B-algebra homomorphisms is a B-algebra homomorphism so that the B-algebras form a category denoted Alg_B.

Algebra homomorphisms (*algebrahomomorfismer*)

[1] Or any morphological derivative thereof, like *map of B-algebras* or *B-algebra-map* etc.

1.14 One says that A is *finitely generated over B*, or is of *finite type* over B, if $A = B[a_1, \ldots, a_r]$ for elements $a_1, \ldots, a_r$ from A.

Finitely generated algebras (*endeliggenererte algebraer*)

Finite type algebras (*algebraer av endelig type*)

EXAMPLE 1.16 A note of warning might be appropriate, algebra structures can be delusive. Every ring is of course an algebra over itself in a canonical way (the algebra structure is given by the identity map), but there can be other unorthodox ways A can be an A-algebra. A simple example to have in mind is the field $\mathbb{C}$ of complex numbers which has an alternative algebra structure induced by complex conjugation. In this structure z acts on w as $\bar{z} \cdot w$.

The two structures are *not* isomorphic as $\mathbb{C}$-algebras although the underlying rings are the same. A good try for an isomorphism would be the identity map, but it does not respect the two algebra-structures[2].

[2] Of course, it holds true that $\mathrm{id}_{\mathbb{C}}(zw)$ equals $z\,\mathrm{id}_{\mathbb{C}}\, w$ and not $\bar{z}\,\mathrm{id}_{\mathbb{C}}\, w$

Another examples of unorthodoxy are funished by the *Frobenius homomorphism* of rings of positive characteristic (see Exercsise 1.7 below). ☆

Problems

1.1 Find all nilpotent and all zero-divisors in $\mathbb{Z}/72\mathbb{Z}$. What are the units? ✳

1.2 Generalize the previous exercise: Let n be a natural number. Determine nilpotents, zero-divisors and units in $\mathbb{Z}/n\mathbb{Z}$. ✳

1.3 Assume that A is finite integral domain. Show that A is a field. ✳

1.4 Show that prime ring is the smallest subring; *i.e.* it is contained in all other subrings of the given ring.

1.5 Convince yourself that the binomial theorem persists being true in any commutative ring; that is, check that your favourite proof still holds water.

1.6 Show that the sum of two nilpotent elements is nilpotent. HINT: You can rely on the binomial theorem.

1.7 *(The Frobenius homomorphism.)* Let A be a ring of positive characteristic p. Show that the relation

$$(a+b)^p = a^p + b^p$$

holds true for all $a, b \in A$. Hence there is a ring homomorphism $A \to A$ sending a to a^p. It is called the *Frobenius homomorphism*. HINT: The binomial coefficients $\binom{p}{r}$ have p as factor when $1 < r < p$.

1.8 Show that any intermediate ring $\mathbb{Z} \subseteq A \subseteq \mathbb{Q}$ is of the form $A = \mathbb{Z}[p^{-1} | p \in S]$ for some set S of primes.

1.9 Let $\phi\colon A \to B$ be a map of rings. Show that ϕ induces a group homomorphism mapping A^* into B^*.

1.10 Let n be a natural number. Show that an element $x \in \mathbb{Z}[\sqrt{-n}]$ is a unit if and only if $\|x\| = 1$ (where $\|x\|$ denotes the ordinary absolute value of the complex number x), and use this to determine the units in $\mathbb{Z}[\sqrt{-n}]$. ✳

1.11 *(The Eisenstein integers.)* Let ω be the cube root $\omega = e^{2\pi i/3}$ of unity. Show that the subring $\mathbb{Z}[\omega]$ of $\mathbb{C}$ is given as ✳

$$\mathbb{Z}[\omega] = \{\, n + m\omega \mid n, m \in \mathbb{Z} \,\}.$$

Determine the group of units $\mathbb{Z}[\omega]^*$. HINT: It holds true that $\omega^2 + \omega + 1 = 0$.

1.12 Assume that a is a nilpotent element of the ring A. Show that $1 + a$ is invertible. More precisely: If $a^n = 0$, the inverse is given as $(1 + a)^{-1} = 1 - a + a^2 - \ldots + (-1)^{n-1}a^{n-1}$. Conclude that if u is a unit and a nilpotent, then $u + a$ is invertible. HINT: Use the good old formula for the sum of a geometric series. ✳

★

1.2 *Polynomials*

We are well acquainted with polynomials with real or complex coefficients; we met them already during the happy days at school. They were then introduced as functions depending on a of real (or a complex one if you went to a French school) variable whose values were given by a polynomial expressions. We shall in this section introduce polynomials with coefficients in any (commutative) ring A. The point of view will necessarily be formal and without reference to functions, and there will be more than just one variable.

1.15 In an earlier paragraph we met polynomial expressions in a set of ring elements. In the present situation where there is no surrounding ring, we must, as signalled above, proceed in a formal way. A *polynomial* in the variables $x_1, \ldots, x_r$ is defined as a formal sum

Polynomials (*Polynomer*)

$$f(x_1, \ldots, x_n) = \sum_{\alpha} a_\alpha x_1^{\alpha_1} \cdot \ldots x_n^{\alpha_n}, \tag{1.2}$$

where the summation extends over all multi-indices $\alpha = (\alpha_1, \ldots, \alpha_n)$ with the α_i's being non-negative integers, and where the coefficients a_α are elements from the ground ring A, only finitely many of which are non-zero. Do not speculate much[3] about what the term "formal sum" means, the essential point is that two such "formal sums" are equal exactly when corresponding coefficients agree.

[3] Or do Exercise 1.19 below where the more general construction of the so-called *monoidal algebras* is described in a precise manner.

1.16 The "pure" terms $a_\alpha x_1^{\alpha_1} \cdot \ldots x_n^{\alpha_n}$ occurring in (1.2) are called *monomials*. The abbreviated notation $x^\alpha = x_1^{\alpha_1} \cdot \ldots x_n^{\alpha_n}$ is convenient and practical. The *degree* of a non-zero monomial $a_\alpha \cdot x^\alpha$ is the sum $\sum_i \alpha_i$ of the exponents, and the highest degree of a non-zero monomial term in a polynomial, is the *degree* of the polynomial. Non-zero constants are of degree zero, but the zero polynomial is not attributed a well-defined degree—it is rather considered to be of any degree (it equals $0 \cdot x^\alpha$ for any α).

Monomials (*Monomer*)

The degree of a polynomial (*Graden til et polynom*)

A polynomial is said to be *homogenous* if all its monomial terms are of the same degree. For example the polynomial $x^2y + z^3$ is homogeneous of degree three whereas $x^2y + z^2$ is not; it is still of degree three, but not homogeneous.

Homogenous polynomials (Homogene polynomer)

Every polynomial may be expressed as a sum of homogenous polynomials of different degrees—just recollect the homogenous terms with the same degree—and these are called the *homogenous components* of f. They are unambiguously associated with f.

Homogenous components of a polynomials (Homogene komponenter til et polynom)

1.17 Adding two polynomials is simply done term by term, and neither is there any hocus-pocus about multiplying them. The good old pattern is followed where

$$\sum_\alpha a_\alpha x^\alpha \cdot \sum_\beta b_\beta x^\beta = \sum_\gamma \Big(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta \Big) x^\gamma. \tag{1.3}$$

In particular, the product of monomials comply to the exponential law $x^\alpha x^\beta = x^{\alpha+\beta}$; with this in mind, the content of formula (1.3) is that the product is bilinear over A.

Equipped with the operations just described the set $A[x_1, \dots, x_r]$ of polynomials in the variables $x_1, \dots, x_r$ becomes a ring. Of course, there are axioms to be verified; a tedious and uninteresting process without even small obstacles, so we voluntarily skip it (if you suffer from mathematical paranoia, feel free to do the checking).

PROBLEM 1.13 Let $f = \sum_\alpha a_\alpha x^\alpha$ and $g = \sum_\alpha b_\alpha x^\alpha$ be two polynomials with coefficients from the rig A. Show that $\deg fg \leqslant \deg f + \deg g$ (recall the convention that 0 has all degrees). Show that equality holds when A is an integral domain. Give examples that strict inequality holds ★

1.18 There is a slight difference between a polynomial and a polynomial function. Over finite rings, like $\mathbb{Z}/n\mathbb{Z}$ for instance, different polynomials can give rise to identical polynomial functions. Simple examples being polynomials in $\mathbb{F}_2[t]$; that is, polynomials in one variable over the field $\mathbb{F}_2$ with two elements. For instance, such polynomials without constant term and with an even number of non-zero terms will vanish identically as a function on $\mathbb{F}_2$. Over infinite fields however, the two notions coincide.

The universal mapping property

1.19 The polynomial ring $A[x_1, \dots, x_r]$ has a so-called *universal mapping property*; one may *freely* assign values to the variables to obtain homomorphisms.

A universal mapping property (En universell avbildningsegenskap)

PROPOSITION 1.20 (THE UNIVERSAL MAPPING PROPERTY) *Let A be a ring. Assume given a sequence $b_1, \dots, b_r$ of elements from an A-algebra B. Then there is a uniquely determined algebra homomorphism $\phi\colon A[x_1, \dots, x_r] \to B$ such that $\phi(x_i) = b_i$ for $1 \leqslant i \leqslant r$.*

PROOF: A polynomial p is given as $p = \sum_\alpha a_\alpha x^\alpha$. Since the coefficients a_α are unambiguously determined by p, setting $\phi(p) = \sum_\alpha a_\alpha \beta_1^{\alpha_1} \cdot \ldots \cdot b_r^{\alpha_r}$ gives a well-defined map which easily is seen to be additive. Since a relation like the one in (1.3) is universally valid in commutative rings, ϕ respects multiplication as well, and we have an algebra homomorphism. ❑

EXAMPLE 1.17 The universal mapping property is a very particular property most algebras do not have. For instance, the algebra $\mathbb{C}[x^2, x^3]$ from example 1.13 on page 12 does not have it. That algebra has the generators x^2 and x^3, and the equality $(x^2)^3 = (x^3)^2$ imposes a constraint on the values homomorphisms can assume on the two generators; it must hold true that $\phi(x^2)^3$ coincides with $\phi(x^3)^2$ (even though there is no such thing as $\phi(x)$). ☆

Two further constructions

There are two further constructions closely related to the construction of the polynomial rings.

1.21 One may consider polynomial expressions over A in infinite number of variables $x_1, x_2, \ldots, x_n, \ldots$, although each polynomial merely involves finitely many of the variables. For every n the polynomial ring $A[x_1, \ldots, x_n]$ is obviously contained in $A[x_1, \ldots, x_{n+1}]$ and the polynomial rings thus form a nested sequence of rings. The polynomial in countably many variables $A[x_1, x_2, \ldots]$ is just the union of all these.

PROBLEM 1.14 Convince yourself that the universal mapping property holds even for polynomial rings in infinitely many variables. ✳ ★

1.22 The second type of ring we have in mind, are the rings of *formal power series*. A formal power series is an expression like in (1.2)

Rings of formal power series (*Ringen av formelle potensrekker*)

$$f(x_1, \ldots, x_n) = \sum_\alpha a_\alpha x^{\alpha_1} \cdot \ldots x_n^{\alpha_n},$$

except that the sum is not require be to finite. Addition is done term by term, and the multiplication is defined by formula (1.3), which is legitimate since the expression for each coefficient involves only finitely many terms. The formal power series ring is denoted $A[\![x_1, \ldots, x_n]\!]$.

Problems

1.15 Show that a polynomial $f(x) = \sum_i a_i x^i$ in $A[x]$ is invertible if and only if a_0 is invertible and all the other coefficients are nilpotent. HINT: Assume that $f(x) = 1 + a_1 x + \ldots + a_n x^n$ is invertibel with inverse $f(x)^{-1} = 1 + b_1 + \ldots + b_m x^m$. Show that $a_n^{i+1} b_{m-i} = 0$ for $0 \leqslant i < n + m$. Conclude that a_n is nilpotent. ✳

1.16 Let A be a reduced ring. Show that group of units in the polynomial ring $A[x]$ equals A^*.

1.17 Assume that k is a field. Show that $k[t]$ and $k[t, 1/t]$ are not isomorphic as rings. ✳

1.18 Assume that k is field. Show that a the number of zeros of a non-zero polynomial in $k[t]$ is less than the degree. Show that if two polynomials in $k[t]$ define the same function on k and k is infinite, then they coincide as polynomials. If k is finite, exhibit a polynomial that vanish identically on k.

1.19 *(Monoidal algebras.)* In this exercise the definition of polynomial rings is made precise and generalized. ✳

Let G be commutative monoid[4] written additively. As an abelian group $A[G]$ is the direct sum of copies of A indexed by G; that is, $A[G] = \bigoplus_{\alpha \in G} A$. The elements are sequences $p = (p_\alpha)_{\alpha \in G}$ with finite support, and addition is defined component-wise. Introduce a product on $A[G]$ by the formula

$$(p \cdot q)_\alpha = \sum_{\beta \in G} p_\beta \cdot q_{\alpha - \beta}$$

Let x^α denote the sequence all whose components are zero apart from the one in the slot with index α which equals one.

a) Show that x^α form an additive basis for $A[G]$.

b) Show that $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$.

c) Show that $(\sum_\alpha p_\alpha x^\alpha)x^\beta = \sum_\alpha p_\alpha x^{\alpha+\beta}$. Verify that $A[G]$ is a ring.

d) Show that $A[\mathbb{N}_0^r] \simeq A[x_1, \ldots, x_r]$.

[4] A *monoid* is a set endowed with an associative binary operation that has a neutral element, in which the cancellation law holds. The set $\mathbb{N}_0$ of non-negative integers and its cartesian products $\mathbb{N}_0^r$ are arch-examples of monoids.

1.20 Let $\{A_i\}$ be a collection of subrings of the ring A. Prove that the intersection $\bigcap_{i \in I} A_i$ is a subring.

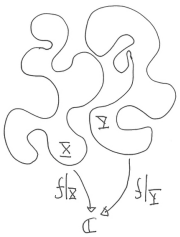
Give examples of two subrings A_1 and A_2 of A such that their union is not a subring. Assume that the collection has the property that any two rings from the collection are contained in a third. Prove that in that case the union $\bigcup_{i \in I} A_i$ is a subring.

★

1.3 *Direct products and idempotents*

As a motivation consider the disjoint union $X \cup Y$ of two topological spaces X and Y. Giving a continuous function on $X \cup Y$ is of course the same as giving one continuous function on X and one on Y. Therefore the ring of continuous functions $C_{\mathbb{R}}(X \cup Y)$ decomposes as the product $C_{\mathbb{R}}(X \cup Y) = C_{\mathbb{R}}(X) \times C_{\mathbb{R}}(Y)$ and both addition and multiplication are given component-wise.

This indicates that in the interplay between geometry and rings, direct product of rings correspond to disconnected spaces.



Below we define the direct product of a collection of rings regardless of the cardinality of the collection and introduce the notion of idempotent elements (elements e such that $e^2 = e$). Multiplication by idempotents are projection operators (equal to their squares) and serve to decompose rings (and later on modules) into direct products.

The archetype of an idempotent function is the characteristic function e_X of a connected component, say X, of a topological space Z; that is, the function that assumes the value one on X and zero on the rest of Z. Since X is a connected component of Z, this function is continuous and of course, $e_X^2 = e_X$. Moreover, the restriction $f|_X$ of any function f equals $e_X f$, or put more precisely, $e_X f$ is the restriction $f|_X$ extended by zero to the entire space Z. Anyhow, in this way the set $e_X C_{\mathbb{R}}(Z)$ is a ring naturally identified with $C_{\mathbb{R}}(X)$ with the idempotent e_X corresponding to unit element in $C_{\mathbb{R}}(X)$. The lesson learned is that idempotents are algebraic counterpart to the geometric connected components.

Direct products of rings

We start out by considering two rings A_1 and A_2. The cartesian product $A = A_1 \times A_2$ consisting of the pairs (a_1, a_2) is a ring when equipped with the pairwise operations. The underlying additive group is the direct product of the underlying groups of the two rings, and the product is given as

$$(a_1, a_2) \cdot (a_1', a_2') = (a_1 \cdot a_1', a_2 \cdot a_2').$$

The unit element is the pair $(1, 1)$, and the two projections $\pi_i \colon A \to A_i$ are ring homomorphisms. Moreover, the direct product possesses two special elements $e_1 = (1, 0)$ and $e_2 = (0, 1)$, which satisfy $e_i^2 = e_i$ and $e_1 e_2 = 0$. The sets $e_i A$ equal respectively $A_1 \times \{0\}$ or $\{0\} \times A_2$, and are, with a liberal interpretation[5], subrings of A isomorphic to respectively A_1 and A_2.

1.23 To generalize what we just did for a pair of rings, let $\{A_i\}_{i \in I}$ be any collection of rings, which can be of any cardinality. In our context it will mostly be finite, but occasionally will be countable. The direct product $\prod_{i \in I} A_i$ has as underlying additive group the direct product of the underlying additive groups of the A_i's. The elements are "*tuples*" or *strings* $(a_i)_{i \in I}$ indexed[6] by I whose i-th component a_i belongs to A_i, and the addition of two such is performed component-wise. The same is true of the multiplication, also performed component for component; that is, it holds true that $(a_i) \cdot (b_i) = (a_i \cdot b_i)$. The ring axioms can be checked component-wise and thus come for free.

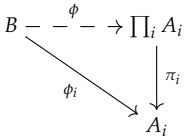
Interpreting tuples $a = (a_i)$ as maps $a \colon I \to \bigcup_{i \in I} A_i$, the ring operations of the direct product are just the point-wise operations. The unit element, for instance, is the "constant[7]" function that sends each index i to 1.

[5] Since the unit element $(1, 1)$ does not lie in either A_i, they are properly speaking not subrings even though they are closed under both addition and multiplication.

[6] The reference to the index set I will frequently be dropped and the strings written (a_i).

[7] Why the quotation marks?

1.24 The projections $\pi_i\colon \prod_{i\in I} A_i \to A_i$ are ring homomorphisms (this is just another way of saying that the ring operations are defined componentwise) and enjoy the following universal property. Given any ring B and any collection $\phi_i\colon B \to A_i$ of ring homomorphisms, there is an unambiguously defined map of rings $\phi\colon B \to \prod_{i\in I} A_i$ such that $\phi_i = \pi_i \circ \phi$ for all $i \in I$: Indeed, this amounts to the map given by $\phi(x) = (\phi_i(x))_{i\in I}$ being a ring homomorphism.



Idempotents

1.25 In any ring A an element e satisfying $e^2 = e$ is said to be *idempotent*, and if f is another idempotent, one says that f and g are *orthogonal* when $fg = 0$. The element $1 - e$ is always idempotent when e is and is orthogonal to e as shown by the little calculations

Idempotent elements (idempotente elementer)
Orthogonal idempotents (ortogonale idempotenter)

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e,$$
$$e(1-e) = e - e^2 = e - e = 0.$$

The subset $eA = \{\, ea \mid a \in A \,\}$ is a ring with e as a unit element. Indeed

$$ea \cdot eb = e^2ab = eab,$$

so eA is closed under multiplication and trivially it is closed under addition as well; finally

$$e \cdot ea = e^2a = e,$$

and e serves as the unit element.

It is common usage to count the unit element and zero among the idempotents; they are called *the trivial idempotents*.

The trivial idempotents (De trivielle idempotentene)

1.26 We saw above that in direct product $A_1 \times A_2$ there appears two natural defined idempotents. Conversely, let A a ring. To any family $\{e_i\}_{1\leqslant i\leqslant r}$ family of mutually orthogonal idempotents that add up to 1 there corresponds a decomposition of A as direct product:

PROPOSITION 1.27 *Let $e_1, \ldots, e_r$ be pairwise orthogonal idempotents in a ring A and assume that $\sum_i e_i = 1$. Then each set e_iA is a subring in the restricted sense, and the association $x \to (e_1x, \ldots, e_rx)$ gives an isomorphism of rings*

$$A \xrightarrow{\simeq} \prod_i e_iA.$$

The projection onto e_iA is realized as multiplication by e_i.

PROOF: To begin with, we verify that the map in the proposition, call it ϕ, is a ring homomorphisms. So let x and y be two elements from A. The e_i's being idempotents we find

$$\phi(x)\phi(y) = (e_ix)(e_iy) = (e_ie_ixy) = (e_ixy) = \phi(xy).$$

Thus ϕ respects the multiplication, and moreover ϕ is clearly additive. The unit element 1 maps to the string (e_i) which is the unit element in the product since each e_i serves as the unit element in e_iA.

Now, we have supposed that the e's add up to one; that is $1 = \sum_i e_i$. Hence $x = \sum_i e_i x$, and it ensues that ϕ injective; indeed, that $\phi(x) = (e_i x) = 0$ means that each $e_i x = 0$.

Finally, let us check that ϕ is surjective. Given an element $(e_i x_i)$ in the product, and put $x = \sum_i x_i$. Using that the e_i's are mutually orthogonal, we find $e_j x = \sum_i e_j e_i x = e_j x$, and we see that x maps to the given element $(e_i x_i)$. ❑

Problems

1.21 Determine the idempotents in $\mathbb{Z}/12\mathbb{Z}$ and in $\mathbb{Z}/36\mathbb{Z}$.

1.22 *(The p-adic integers.)* Let p be a prime number and let $\rho_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ be the reduction map that sends the residue class $[a]_{p^{n+1}}$ of an integer a modulo p^{n+1} to the residue class $[a]_{p^n}$ of a modulo p^n. Let $\mathbb{Z}_p$ be the subset of the direct product $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ whose members are strings $(a_n)_{n\in\mathbb{N}}$ such that $\rho_n(a_{n+1}) = (a_n)$.

a) Show that $\mathbb{Z}_p$ is a subring of the product.

b) Show that the map $\mathbb{Z} \to \mathbb{Z}_p$ sending an integer a to the string $([a]_{p^n})$ is an injective ring homomorphism.

c) Show that $\mathbb{Z}_p$ is an integral domain,

d) Let $\pi \colon \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ be induced by the projection from $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ onto $\mathbb{Z}/p\mathbb{Z}$. Show that an element a in $\mathbb{Z}_p$ is invertible if and only if $\pi(a) \neq 0$.

★

Lecture 2

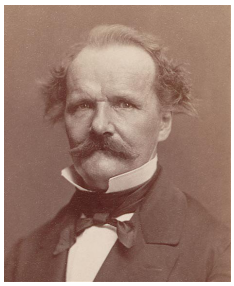
Ideals

The *ideals* were first defined by Richard Dedekind in 1876, but the name comes from the so called "ideal numbers" of Ernst Kummer which he introduced in a series of papers around 1847.

Richard Dedekind
(1831–1916)
German mathematician

Working with rings of integers in algebraic number fields, the algebraists of that period realized that analogues of the Fundamental Theorem of Arithmetic does not always hold in such rings. Recall that this theorem asserts that any integer is a product $n = p_1 \cdot \ldots \cdot p_r$ of signed primes and the factors are unique up to order and sign—changing the order of the factors does not affect the product, and changing the sign of one factor can be compensated by simultaneously changing the sign of another.

It is not too complicated to show that in a vast class of rings, including the rings of algebraic numbers above, any element can be expressed as a product of irreducible elements; that is, elements that can not be factored further (they can of course always be altered by a unit, but that is not an honest factorization). However the point is, that these factors are not unique (up to order and units) in general.



Ernst Eduard Kummer
(1810–1893)
German mathematician

The classical example omnipresent in text books, is the factorisazion $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ in the ring $\mathbb{Z}[i\sqrt{5}]$. The four involved numbers are all irreducible and no two of them related by units.

The ideals came about to remedy this fault and, in fact, in certain rings called Dedekind rings, the situation can be salvaged; there is a factorization theorem of *ideals* replacing the Fundamental Theorem of Arithmetic. Hence the name *ideals*, they were "the ideal numbers"

Dedekind rings are however a very restricted class of rings, and today ideals play an infinitely wider role than just being "ideal numbers". In algebraic geometry for instance, they appear as the sets of polynomials in $k[x_1, \ldots, x_r]$ vanishing along a subset of k^r, and this is the clue to the coupling between algebra and geometry.

2.1 Ideals

2.1 Let A be a ring. An additive subgroup $\mathfrak{a}$ of A is called an *ideal* if it is closed under multiplication by elements from A. That is, $\mathfrak{a}$ satisfies the two following requirements; the first merely being a rephrasing that $\mathfrak{a}$ is a subgroup.

Ideals (*Idealer*)

- If $a \in \mathfrak{a}$ and $b \in \mathfrak{a}$, then $a + b \in A$ and $0 \in \mathfrak{a}$;
- If $a \in A$ and $b \in \mathfrak{a}$, then $ab \in \mathfrak{a}$.

Both the trivial additive subgroup 0 and the entire ring satisfy these requirements and are ideals, although special ideals. In many texts the ring when considered an ideal, is denoted by (1).

2.2 An ideal $\mathfrak{a}$ is said to be a *proper ideal* if it is not equal to the entire ring. This is equivalent to no member of $\mathfrak{a}$ being invertible. Indeed, if $a \in \mathfrak{a}$ is invertible one has $b = ba^{-1} \cdot a \in \mathfrak{a}$ for any $b \in A$; and if $\mathfrak{a} = A$, of course, $1 \in \mathfrak{a}$.

Proper ideals (*Ekte idealer*)

From this observation ensues the following characterization of fields in terms of of ideals:

PROPOSITION 2.3 *A ring A is a field if and only if its only ideals are the zero ideal and A itsef.*

PROOF: We just saw that an ideal $\mathfrak{a}$ equals A precisely when $\mathfrak{a} \cap A^* \neq \varnothing$. If A is a field, $A^* = A\backslash\{0\}$, and any ideal, apart from the zero ideal, meets A^*. The other way round, any non-zero and proper ideal must contain a non-zero element, which cannot be invertible, and consequently A is a not a field. ❑

Examples

2.1 The subset $n\mathbb{Z}$ of $\mathbb{Z}$ consisting of all multiples of the integer n is an ideal; a so-called *principal ideal*. The ideal $n\mathbb{Z}$ is frequently written (n).

2.2 For any subset $S \subseteq \mathbb{C}^r$ be a subset the polynomials in $\mathbb{C}[x_1, \ldots, x_r]$ vanishing on S form an ideal.

☆

Operations on ideals—the lattice of ideals

2.4 The set $\mathcal{I}(A)$ of ideals in the ring A has—in addition to being partially ordered under inclusion—a lot of structure. One may form *the intersection* $\bigcap_{i\in I} \mathfrak{a}_i$ of any family $\{\mathfrak{a}_i\}_{i\in I}$ of ideals. It is easily seen to be an ideal, and is the largest ideal contained in all the $\mathfrak{a}_i$'s. Likewise, one has the notion of *the sum* of a family of ideals. It is the ideal consisting of all finite sums of elements from the $\mathfrak{a}_i$'s:

$$\sum_{i\in I} \mathfrak{a}_i = \{\, a_1 + \ldots + a_r \mid a_i \in \mathfrak{a}_i,\ r \in \mathbb{N} \,\},$$

and is the smallest ideal containing all the $\mathfrak{a}_i$'s. So $\mathcal{I}(A)$ is what one technically calls a *complete lattice*; every subset of $\mathcal{I}(A)$ has a greatest lower bound (the sum) and a smallest upper bound (the intsersection). It is the *lattice of ideals*in A.

The lattice of ideals (*Ideallattiset(???)*)

2.5 A construct similar to the sum of a family of ideals is the ideal generated by a set of elements $\{a_i\}_{i\in I}$ from A. It will be denoted $(a_i|i \in I)$, or in case the set $S = \{a_1, \ldots, a_r\}$ is finite, the alternative notation $(a_1, \ldots, a_r)$ is common usage. Its members are all finite linear combinations of the a_i's with coefficients from the ring A; that is, it holds that

$$(a_i|i \in I) = \{ \textstyle\sum_{i\in J} c_i a_i \mid c_i \in A, J \subseteq I \text{ finite} \}.$$

The elements a_i are called *generators*. Ideals which are generated by finitely many elements are naturally called *finitely generated*. An ideal generated by a single element, is called a *principal ideal*; it consists of all multiples of the generator. If a is the generator, it is denoted by (a) or by aA, and it holds that $(a) = \{ c \cdot a \mid c \in A \}$.

Generators (*Generatorer*)

Finitely generated ideals (*Endeliggenererte idealer*)

Principal ideals (*Hoved-idealer*)

2.6 The *product* of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal generated by all products of one element from $\mathfrak{a}$ and one from $\mathfrak{b}$; that is, the product $\mathfrak{ab}$ is formed of all finite sums of such products:

The product of ideals (*Produktet av idealer*)

$$\mathfrak{ab} = \{ a_1b_1 + \ldots + a_rb_r \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, r \in \mathbb{N} \}.$$

2.7 The last operation we offer is the formation of *the transporter* between two ideals. Some texts call it the *quotient* of the two deals—however, this term should be reserved for another construction we shortly come to, and hence should be avoided. So let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in A. We define the *transporter* $(\mathfrak{a} : \mathfrak{b})$ to be set of elements which on multiplication send $\mathfrak{b}$ into $\mathfrak{a}$; that is

The transporter (*Transportøren*)

$$(\mathfrak{a} : \mathfrak{b}) = \{ x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a} \}.$$

It is easily seen to be an ideal. In the particular case that $\mathfrak{a} = (0)$ and $\mathfrak{b}$ is a principal ideal, say $\mathfrak{b} = (a)$, the transporter $(0 : a)$ (an immediate simplification of the overloaded expression $((0) : (a))$) coincides with the *annihilator* of a; that is

The annihilator of an element (*Annihilatoren til et element*)

$$(0 : a) = \operatorname{Ann} a = \{ x \mid xa = 0 \}.$$

Examples

2.3 In $\mathbb{Z}$ it holds that $\big(100 : 10\big) = (10)$. More generally if a and b are elements from the ring A and b is a non-zero divisor, one has $(ab : b) = (a)$. Indeed, $xb = yab$ is equivalent to $x = ya$ since cancellation by b is allowed b being a non-zero divisor. If b is a zero-divisor it anyhow holds that $(ab, b) = (a) + \operatorname{Ann} b$.

2.4 In the polynomial ring $\mathbb{C}[x,y]$ it holds that $\big((xy,y^2):(x,y)\big)=(y)$.

Clearly (y) is contained in $\big((xy,y^2):(x,y)\big)$. For the converse inclusion assume that $fx=gxy+hy^2$ where f, g and h are polynomials in $\mathbb{C}[x,y]$. Since x divides the terms fx and gxy, it divides hy^2 as well, and by cancelling x, we infere that $f=gy+h'y$ with $h'\in\mathbb{C}[x,y]$; that is, $f\in(y)$.

2.5 In $\mathbb{Z}/40\mathbb{Z}$ one has $\operatorname{Ann}2=(20)$, that $\operatorname{Ann}4=(10)$ and that $\operatorname{Ann}20=(5)$.

☆

Functorially

A map of rings $\phi\colon A\to B$ induces two maps between the ideal-lattices $\mathcal{I}(A)$ and $\mathcal{I}(B)$, one in a covariant and one in a contravariant way. One can move ideals forward with the help of ϕ and the the usual inverse image construct is a way move ideals backwards along ϕ. The new ideals are in some texts either called *extensions* or *contractions* in the respective case.

Extensions of ideals (*Utvidlese av ideal*)
Contractions of ideals (*Tilbaketrekning*)

2.8 We start with the contravariant one. The inverse image $\phi^{-1}(\mathfrak{b})$ of an ideal $\mathfrak{b}$ in B is an ideal in A; indeed, $\phi(ab)=\phi(a)\phi(b)$ belongs to $\mathfrak{b}$ whenever $\phi(b)$ does, and this gives rise to a map $\phi^{-1}\colon\mathcal{I}(B)\to\mathcal{I}(A)$. Obviously it preserves inclusions and takes intersections to intersections since the pullback of sets respects intersections in general. Sums and products of ideals however, are not generally preserved. One has

- $\phi^{-1}(\mathfrak{a})\cap\phi^{-1}(\mathfrak{b})=\phi^{-1}(\mathfrak{a}\cap\mathfrak{b})$,
- $\phi^{-1}(\mathfrak{a})+\phi^{-1}(\mathfrak{b})\subseteq\phi^{-1}(\mathfrak{a}+\mathfrak{b})$,
- $\phi^{-1}(\mathfrak{a})\cdot\phi^{-1}(\mathfrak{b})\subseteq\phi^{-1}(\mathfrak{a}\cdot\mathfrak{b})$,

but equality in the last two does not hold in general.

In the frequently occurring case that A is a subring of B one usually suppresses the reference to the inclusion map and uses the natural notation $\mathfrak{a}\cap A$ for the "pullback" of an ideal $\mathfrak{a}$. We shall here give an example showing that the inclusion in the second relation can be strict, but postpone giving an example for the last inclusion (see Example 2.8 below on page 30).

EXAMPLE 2.6 A simple example of strict inclusion in the second relation above is the diagonal map $\delta\colon A\to A\times A$ sending a to (a,a). The two ideals $\mathfrak{b}=\{(0,a)\mid a\in A\}$ and $\mathfrak{b}'=\{(a,0)\mid a\in A\}$ are both pulled back to the zero ideal, but since $\mathfrak{b}+\mathfrak{b}'=A\times A$, their sum is pulled back to the entire ring A. ☆

2.9 We then come to the covariant construction. If $\mathfrak{a}$ is an ideal in A, the image $\phi(\mathfrak{a})$ is not necessarily an ideal in B unless ϕ is surjective. A stupid example can be the image of any ideal in $\mathbb{Z}$ under the inclusion $\mathbb{Z}\subseteq\mathbb{Q}$. The ideal generated by $\phi(\mathfrak{a})$ however is, and we shall usually denote this ideal by $\phi(\mathfrak{a})B$

or simply by $\mathfrak{a}B$. This induces a map $\mathcal{I}(A) \to \mathcal{I}(B)$. Inclusions are preserved, and one easily verifies the following relations

- $\phi(\mathfrak{a} \cdot \mathfrak{b})B = (\phi(\mathfrak{a})B) \cdot (\phi(\mathfrak{b})B)$,
- $\phi(\mathfrak{a} + \mathfrak{b})B = \phi(\mathfrak{a})B + \phi(\mathfrak{b})B$,
- $\phi(\mathfrak{a} \cap \mathfrak{b})B \subseteq \phi(\mathfrak{a})B \cap \phi(\mathfrak{b})B$.

The inclusion in the last line may be strict, see Example 2.9 on page 30 below.

Problems

2.1 Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in a ring A. Show that the relations $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ and $(\mathfrak{a} \cap \mathfrak{b})^2 \subseteq \mathfrak{a} \cdot \mathfrak{b}$ hold. Show by giving examples that there might be a strict inclusion in both cases. ✲

2.2 Assume that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in a ring A satisfying $\mathfrak{a} + \mathfrak{b} = (1)$. Show that $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$. ✲

2.3 Let $\mathfrak{a}$,$\mathfrak{b}$ and $\mathfrak{c}$ be ideals in the ring A. Show that $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$. Show that $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \subseteq \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$, and by exhibiting an example, show that the inclusion can be strict.

2.4 Verify the equalities in paragraphs 2.8 and 2.9.

2.5 Let $\{\mathfrak{a}_i\}$ be a collection of ideals in the ring A. Show that for any ideal $\mathfrak{b}$ it holds true that $(\bigcap_{i\in I} \mathfrak{a}_i : \mathfrak{b}) = \bigcap_{i\in I}(\mathfrak{a}_i : \mathfrak{b})$ and that $(\mathfrak{b} : \sum_{i\in I} \mathfrak{a}_i) = \bigcap_{i\in I}(\mathfrak{b} : \mathfrak{a}_i)$. ✲

2.6 Show that any ideal in the ring $\mathbb{Z}$ of integers is generated by one element, which is unique up to sign.

2.7 Let m and n be two integers. Show that $(n) \cdot (m) = \big((n) \cap (m)\big) \cdot (n, m)$.

2.8 Consider the two ideals $\mathfrak{a} = (144)$ and $\mathfrak{b} = (24)$ in $\mathbb{Z}$. Describe $(\mathfrak{a} : \mathfrak{b})$. In general, describe $(n : m)$ in terms of the prime factorizations of the two integers n and m.

2.9 Let $k[x, y]$ be the polynomial ring in the variables x and y over the field k, and let $\mathfrak{m}$ be the ideal generated by x and y; that is $\mathfrak{m} = (x, y)$. Let n denote a natural number. ✲

a) Exhibit a set of generators for the power $\mathfrak{m}^n$.

b) Let μ and ν be two natural numbers. Show that $\mathfrak{m}^n \subseteq (x^\mu, y^\nu)$ for n sufficiently large. What is the smallest n for which this holds?

2.10 Let $A = \mathbb{Z}[\sqrt{2}, \sqrt{3}]$. Show that as an abelian group A free of rank four and exhibit a basis. Show that the underlying abelian groups of the principal ideals $(\sqrt{2})$ and $(\sqrt{3})$ both are of rank four. Exhibit additive bases for both. ✲

★

2.2 *Quotient rings and kernels*

In one way ideals play the same role in the category of rings as normal subgroups do in the category of groups. They are precisely the subobjects that appear as kernels of homomorphisms, and consequently, the ones that can be factored out.

Kernels of ring homomorphisms (Kjernen til en ringavbildning)

2.10 By definition the *kernel* of a ring homomorphism $\phi\colon A \to B$ is the kernel of ϕ considered a mapping between the underlying additive groups; that is, the subset of elements mapping to zero, or written in symbols one has $\ker\phi = \{\, a \in A \mid \phi(a) = 0 \,\}$. If $a \in \ker\phi$ and $b \in A$, we find

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) = 0 \cdot \phi(b) = 0,$$

and we can conclude that $ab \in \ker\phi$. Hence the kernel $\ker\phi$ is an ideal.

Quotient rings (Kvotientringer)

2.11 To see that any ideal is a kernel, one introduces the concept of *quotient rings*. An ideal $\mathfrak{a}$ in A being an additive subgroup, there is a quotient group $A/\mathfrak{a}$. It consists of the *residue classes* $[a] = a + \mathfrak{a}$ of elements in A, and the sum of two such, say $[a]$ and $[b]$, equals $[a + b]$. To put a ring structure on $A/\mathfrak{a}$ we simply define the product of two classes $[a]$ and $[b]$ as

$$[a] \cdot [b] = [a \cdot b] = a \cdot b + \mathfrak{a}.$$

Some checking is needed; the most urgent one being that the product only depends on the residue classes $[a]$ and $[b]$ and not on the representatives a and b. This is encapsulated in the formula

$$(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) = a \cdot b + a \cdot \mathfrak{a} + b \cdot \mathfrak{a} + \mathfrak{a} \cdot \mathfrak{a} \subseteq a \cdot b + \mathfrak{a}.$$

It is left to the students to verify that this product comply with the associative and the distributive laws. Finally, by definition of the ring operations in $A/\mathfrak{a}$, the quotient map $\pi\colon A \to A/\mathfrak{a}$ is a map of rings whose kernel equals the given ideal $\mathfrak{a}$.

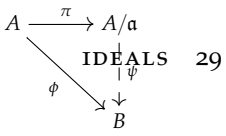
EXAMPLE 2.7 It is appropriate to mention what quotients by the two "extreme" ideals are. The quotient $A/\mathfrak{a}$ equals A if and only if $\mathfrak{a}$ is the zero-ideal, and it equals[1] the null-ring if and only if $\mathfrak{a} = A$. ☆

[1] This examplifies what purpose the null-ring serves; it allows a general existence theorem (avoiding the hypothesis $\mathfrak{a} \neq A$).

A universal property (En universell egenskap)

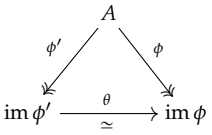
2.12 The quotient ring $A/\mathfrak{a}$ together with the quotient map $\pi\colon A \to A/\mathfrak{a}$ enjoys a so-called *universal property*—the rather pretentious notion "solves a universal problem" is also common usage—which is convenient way of characterizing many types of mathematical objects. The origin of the technique is found in category theory where objects not always have "elements" and one relies on "arrows" to express properties.

Any map of rings $\phi\colon A \to B$ that vanishes on $\mathfrak{a}$; that is, which satisfies $\mathfrak{a} \subseteq \ker\phi$, factors in a unique way through the quotient $A/\mathfrak{a}$. In other words, there is a unique ring-map $\psi\colon A/\mathfrak{a} \to B$ such that $\phi = \psi \circ \pi$. Indeed, since



$\phi(\mathfrak{a}) = 0$, the map ϕ is constant on every residue class $[a] = a + \mathfrak{a}$, and we put $\psi([a])$ equal to that constant value. This value is forced upon ψ, so ψ is unique, and it is a ring-map since ϕ is. We have proven:

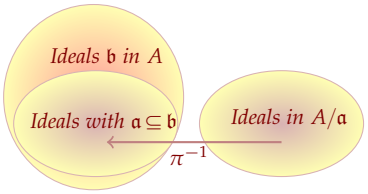
PROPOSITION 2.13 (THE FACTORIZATION THEOREM) *Given an ideal $\mathfrak{a}$ in the ring A. A map of rings $A \to B$ vanishes on $\mathfrak{a}$ if and only if it factors through the quotient map $A \to A/\mathfrak{a}$. The factorization is unique.*



If it happens that $\ker\phi = \mathfrak{a}$, the induce map ψ will be injective, and hence, *a priori* being surjective, is an isomorphism. The images of all ring-maps with the same kernel are therefore isomorphic, in the strong sense that the isomorphisms fit into diagrams like the one in the margin.

Ideals in quotients

2.14 There is a natural one-to-one correspondence between ideals in $A/\mathfrak{a}$ and ideals in A containing the ideal $\mathfrak{a}$. Indeed, if $\mathfrak{b} \subseteq A$ is an ideal with $\mathfrak{a} \subseteq \mathfrak{b}$, the image $\pi(\mathfrak{b})$ equals the additive subgroup $\mathfrak{b}/\mathfrak{a} \subseteq A/\mathfrak{a}$ and since π is surjective, this is an ideal in $A/\mathfrak{a}$. Moreover, if $\mathfrak{c} \subseteq A/\mathfrak{a}$ is an ideal, the inverse image $\pi^{-1}(\mathfrak{c})$ is an ideal in A satisfying $\pi(\pi^{-1}(\mathfrak{c})) = \mathfrak{c}$ (again because π is surjective); or in other words, $\pi^{-1}(\mathfrak{c})$ contains $\mathfrak{a}$ and $\pi^{-1}(\mathfrak{c})/\mathfrak{a} = \mathfrak{c}$.



PROPOSITION 2.15 *Let $\mathfrak{a}$ be an ideal in the ring A and $\pi\colon A \to A/\mathfrak{a}$ the quotient map. The following three statements hold true:*

- *For every ideal $\mathfrak{b}$ in A containing $\mathfrak{a}$, the quotient $\mathfrak{b}/\mathfrak{a}$ is an ideal in $A/\mathfrak{a}$. Every ideal in $\mathfrak{c} \subseteq A/\mathfrak{a}$ is of this form for a unique ideal $\mathfrak{b}$; indeed, one has $\mathfrak{c} = \pi^{-1}(\mathfrak{c})/\mathfrak{a}$.*
- *For every ideal $\mathfrak{b}$ in A it holds true that $\pi^{-1}(\pi(\mathfrak{b})) = \mathfrak{b} + \mathfrak{a}$.*
- *An ideal is mapped to the zero ideal in $A/\mathfrak{a}$ if and only if it is contained in $\mathfrak{a}$.*

PROOF: We already saw that $\pi(\mathfrak{b}) = \mathfrak{b}/\mathfrak{a}$ is an ideal. That $\mathfrak{b}$ is unique follows from the second assertion since if $\pi(\mathfrak{b}) = \pi(\mathfrak{b}')$ it ensues that $\mathfrak{b} + \mathfrak{a} = \mathfrak{b}' + \mathfrak{a}$, and hence $\mathfrak{b} = \mathfrak{b}'$ when both contain $\mathfrak{a}$. The second assertion is clear since $\mathfrak{a} = \ker\pi$. Likewise is the third for the same reason. ❑

2.16 Proposition 2.15 above may be rephrased in terms of the lattices of ideals $\mathcal{I}(A)$ and $\mathcal{I}(A/\mathfrak{a})$. The map $\pi^{-1}\colon \mathcal{I}(A/\mathfrak{a}) \to \mathcal{I}(A)$ sending an ideal $\mathfrak{c}$ to the inverse image $\pi^{-1}(\mathfrak{c})$ is injective and the image consists of the ideals in A containing $\mathfrak{a}$. The map the other way round, which sends an ideal $\mathfrak{b}$ in $\mathcal{I}(A)$ to its image $\pi(\mathfrak{b})$, serves as a section to π^{-1} over the sublattice of ideals containing $\mathfrak{a}$. The map π^{-1} preserves inclusions and respects intersections, products and sums.

2.17 The image in $A/\mathfrak{a}$ of an ideal $\mathfrak{b} \subseteq A$, which not necessarily contains $\mathfrak{a}$, is the ideal $(\mathfrak{b} + \mathfrak{a})/\mathfrak{a}$. This holds since obviously $\pi(\mathfrak{b} + \mathfrak{a}) = \pi(\mathfrak{b})$. Now,

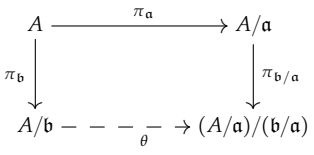
$\ker \pi|_{\mathfrak{b}} = \mathfrak{a} \cap \mathfrak{b}$ from which ensues the following isomorphism

$$\mathfrak{b}/\mathfrak{b} \cap \mathfrak{a} \simeq (\mathfrak{a} + \mathfrak{b})/\mathfrak{a}. \tag{2.1}$$

Finally, we mention that when $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals with $\mathfrak{a} \subseteq \mathfrak{b}$, there is a natural isomorphism

$$(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \simeq A/\mathfrak{b}. \tag{2.2}$$

Indeed, in the diagramme in the margin, the composition $\pi_{\mathfrak{b}/\mathfrak{a}} \circ \pi_{\mathfrak{a}}$ has the ideal $\mathfrak{b}$ as kernel, and therefore factors through $\pi_{\mathfrak{b}}$ by say θ. The map θ is surjective since the composition is and injective since the composition has $\mathfrak{b} = \pi_{\mathfrak{a}}^{-1}(\mathfrak{b}/\mathfrak{a})$ as kernel. These two formulas are often referred to as the *Isomorphisms theorems*.



THEOREM 2.18 (THE ISOMORPHISM THEOREM) *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in A. Then the following two equalities hold, where in the second is assumed that $\mathfrak{a} \subseteq \mathfrak{b}$;*

- $\mathfrak{b}/\mathfrak{b} \cap \mathfrak{a} \simeq (\mathfrak{a} + \mathfrak{b})/\mathfrak{a}$;
- $(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \simeq A/\mathfrak{b}$.

PROBLEM 2.11 Let k be a field and $\phi\colon k \to A$ a ring homomorphism. Show that ϕ is injective unless A is the null ring. ★

Examples

2.8 We promised to give examples that strict inclusion can hold in the last statement of in Paragraph 2.8 (on page 26). Here comes one. Let $B = k[X, Y, Z]/(Z - XY)$, and as usual the lower case version of a variable will stand for its class in B. Then $B = k[x, y, z]$ with $z = xy$.

We let the map $\phi\colon A \to B$ be the natural inclusion of $A = k[z]$ in $B = k[x, y, z]$; for any ideal $\mathfrak{c}$ in B the inverse image $\phi^{-1}(\mathfrak{c})$ is then nothing but the intersection $\mathfrak{c} \cap B$.

Consider the two principal ideals $\mathfrak{a} = (x)B$ and $\mathfrak{b} = (y)B$ in B. Since $z = xy$, it holds that $z \in (x)B$ and $z \in (y)B$, and since $(z)A$ is a maximal ideal in $A = k[z]$, we see that $\mathfrak{a} \cap A = \mathfrak{b} \cap A = (z)A$, and hence $(\mathfrak{a} \cap A) \cdot (\mathfrak{b} \cap A) = (z^2)A$. On the other hand $\mathfrak{ab} = (xy)B = (z)B$ so that $\mathfrak{a} \cdot \mathfrak{b} \cap A = (z)A$; hence $\phi^{-1}(\mathfrak{a}) \cdot \phi^{-1}(\mathfrak{b}) \subsetneq \phi^{-1}(\mathfrak{a} \cdot \mathfrak{b})$.

2.9 For an example of strict inclusion in the last statement Paragraph 2.9 (on page 26) let $A = k[X, Y, Z]$ and $B = k[X, Y, Z]/(ZX - ZY)$ and consider the projection map $\phi\colon A \to B$; then $\phi(\mathfrak{c}) = \mathfrak{c}B$ for any ideal $\mathfrak{c}$ in A.

Let $\mathfrak{a} = (X)$ and $\mathfrak{b} = (Y)$. Then $\mathfrak{a} \cap \mathfrak{b} = (XY)$. With the usual lower case convention, since $zx = zy$, it holds that and $zx \in \mathfrak{a}B \cap \mathfrak{b}B$, but $zx \notin (xy)B$; and hence $\phi(\mathfrak{a}) \cap \phi(\mathfrak{b}) \subsetneq \phi(\mathfrak{a} \cap \mathfrak{b})$.

☆

2.3 *Prime ideals and maximal ideals*

Two classes of ideals are infinitely more important than others. We are speaking about the *prime ideals* and the *maximal ideals*. The prime ideals are defined in terms of multiplicative properties of the ring, and are generalizations of prime numbers. They took the place of the primes in Kummer and Dedekind's world of "ideal numbers". Maximal ideals are defined in terms of inclusions. They are, as the name indicates, maximal among the *proper* ideals; that is, they are maximal elements in the partially ordered set $\mathcal{I}(A)\backslash\{A\}$.

2.19 An ideal $\mathfrak{a}$ in a ring A is a *prime ideal* if it is proper and satisfies the following requirement:

Prime ideals (*Primidealer*)

- If $ab \in \mathfrak{a}$, then either $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$.

An ideal $\mathfrak{a}$ is said to be *maximal* if it is proper and satisfies the following requirement:

Maximal ideals (*Maksimale idealer*)

- If $\mathfrak{b}$ is an ideal and $\mathfrak{a} \subseteq \mathfrak{b}$, then either $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{b} = A$.

In other words, $\mathfrak{a}$ is maximal among the proper ideals. Notice that both prime ideals and maximal ideals are proper by definition.

2.20 One has the following characterization of the two classes of ideals in terms of properties of quotients.:

PROPOSITION 2.21 *An ideal $\mathfrak{a}$ in A is a prime ideal if and only if the quotient $A/\mathfrak{a}$ is an integral domain. The ideal $\mathfrak{a}$ is maximal if and only if $A/\mathfrak{a}$ is a field.*

PROOF: It holds true that $A/\mathfrak{a}$ is an integral domain if and only if $[a][b] = 0$ implies that either $[a] = 0$ or $[b] = 0$; that is, if and only if $ab \in \mathfrak{a}$ implies that either $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$, which proves the first assertion.

Bearing in mind the relation between ideals in $A/\mathfrak{a}$ and ideals in A containing $\mathfrak{a}$ (as in Proposition 2.15 on page 29), the second assertion is pretty obvious. There is no ideal strictly between $\mathfrak{a}$ and A if and only if $A/\mathfrak{a}$ has no non-trivial proper ideal; that is, if and only if $A/\mathfrak{a}$ is a field (Proposition 2.3 on page 24). ❑

Notice that the zero ideal (0) is a prime ideal if and only if A is an integral domain, and it is maximal if and only if A is a field. When $\mathfrak{m}$ is a maximal ideal, the field $A/\mathfrak{m}$ is called *the residue class field* of A at $\mathfrak{m}$ and now and then denoted by $k(\mathfrak{m})$. Since fields are integral domains, we see immediately that maximal ideals are prime. The converse does not hold as we shortly shall see examples of (Example 2.11 below).

Residue class fields (*Restklassekropper*)

PROPOSITION 2.22 *A maximal ideal $\mathfrak{m}$ is prime.*

2.23 Not only for elements is it true that a product lies in a prime ideal only when one of the factors does, the same applies to products of ideals as well:

PROPOSITION 2.24 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in A such that $\mathfrak{ab}$ is contained in the prime ideal $\mathfrak{p}$. Then either $\mathfrak{a}$ or $\mathfrak{b}$ is contained in $\mathfrak{p}$.*

PROOF: Assume that neither $\mathfrak{a}$ nor $\mathfrak{b}$ lies in $\mathfrak{p}$ and pick elements $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ not being members of $\mathfrak{p}$. Since $\mathfrak{ab}$ is contained in $\mathfrak{p}$, the product ab belongs to $\mathfrak{p}$, and since $\mathfrak{p}$ is prime, it either holds that $a \in \mathfrak{p}$ or that $b \in \mathfrak{p}$. Contradiction. ❑

2.25 In the correspondence between ideals in A and $A/\mathfrak{a}$ described in Proposition 2.15 on page 29 prime ideals correspond to prime ideals (containing $\mathfrak{a}$) and maximal ideals to maximal ideal (containing $\mathfrak{a}$). The last statement is clear since with the notation as in Proposition 2.15 the inverse image map π^{-1} is an isomorphisms of the lattice $\mathcal{I}(A/\mathfrak{a})$ with the sublattice of $\mathcal{I}(A)$ whose members contain $\mathfrak{a}$, and hence maximal elements correspond to maximal elements. The first ensues from the general truth that prime ideals pull back along ring maps to prime ideals; indeed, assume that $\mathfrak{p}$ is a prime ideal in B and $\phi\colon A \to B$ a ring map. If the product ab lies in the inverse image $\phi^{-1}(\mathfrak{p})$, it follows that $\phi(ab) \in \mathfrak{p}$; but $\phi(ab) = \phi(a)\phi(b)$, and hence either $\phi(a)$ lies in $\mathfrak{p}$ or $\phi(b)$ lies there; that is, either $a \in \phi^{-1}(\mathfrak{p})$ or $b \in \phi^{-1}(\mathfrak{p})$.

PROPOSITION 2.26 *Let A be a ring and $\mathfrak{a}$ an ideal. The prime ideals in the quotient $A/\mathfrak{a}$ are precisely those of the form $\mathfrak{p}/\mathfrak{a}$ with $\mathfrak{p}$ a prime ideal in A containing $\mathfrak{a}$, and the maximal ideals are those shaped like $\mathfrak{m}/\alpha$ with $\mathfrak{m}$ a maximal ideal in A likewise containing $\mathfrak{a}$.*

Examples

2.10 The archetype of maximal ideals are the kernels of evaluation maps. For instance, let $a = (a_1, \ldots, a_r)$ be a point in k^r where k is any field, and consider the map $k[x_1, \ldots, x_r] \to k$ sending a polynomial f to its value $f(a)$ at a. The kernel $\mathfrak{m}$ is a maximal ideal since $k[x_1, \ldots, x_r]/\mathfrak{m}$ is the field k. The kernel may be described as $\mathfrak{m} = (x_1 - a_1, \ldots, x_r - a_r)$. This is obvious when a is the origin, and introducing fresh coordinates $x_i' = x_i - a_i$, one reduces the general case to that case.

2.11 A simple example of a prime ideal not being maximal can be the principal ideal (y) in the the polynomial ring $k[x, y]$ in the two variables x and y over a field k. One has $k[x, y]/(y) \simeq k[x]$, for instance, since the partial evaluation map $k[x, y] \to k[x]$ sending $f(x, y)$ to $f(x, 0)$ has kernel (y), and (y) is prime because $k[x]$ is an integral domain. Moreover (y) is not maximal being contained in (x, y) (or if you prefer, because $k[x]$ is not a field).

☆

Prime avoidance and a pair of twin lemmas

A lemma about prime ideals that will be useful now and then, is the so-called Prime Avoidance Lemma. It asserts that an ideal contained in a finite union of prime ideals must lie entirely in one of them. The name stems from the equivalent statement that if an ideal $\mathfrak{a}$ is not contained in any of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, it has an element not lying in any of the $\mathfrak{p}_i$'s.

2.27 As a warm up, let us do the case of two prime ideals, in which case the statement is simply a statement about abelian groups: If a subgroup B of an abelian group is contained in the union of two others, A_1 and A_2, it is contained in one of them; indeed, pick sn $x_i \in A_i \cap B$ but $x_i \notin A_j$. Then $x_1 + x_2 \in B$ but $x_1 + x_2 \notin A_1 \cup A_2$, for were it in A_1, it would follow that $x_2 \in A_1$ which is not the case. For three groups the corresponding statement is faulty as shows the vector space $\mathbb{F}_3^2$: It is the union of the three one-dimensional subspaces it has; so in general some multiplicative structure is required.

LEMMA 2.28 (PRIME AVOIDANCE LEMMA) *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be prime ideals in the ring A. If $\mathfrak{a}$ is an ideal contained in the union $\bigcup_i \mathfrak{p}_i$, then $\mathfrak{a}$ is contained in at least one of the $\mathfrak{p}_j$'s.*

PROOF: We can certainly assume that the union is *irredundant*; that is, none of the prime ideals are contained in the union of the others. Then, for each j one may pick an element y_j lying in the prime ideal $\mathfrak{p}_j$ but not in any of the others. Assume for a contrapositive argument that $\mathfrak{a}$ is not contained in any of the $\mathfrak{p}_i$'s, and chose elements x_j from $\mathfrak{a}$ not in $\mathfrak{p}_j$. Consider for each j the element $z_j = x_j \prod_{i \neq j} y_i$. It lies in $\mathfrak{p}_i$ when $i \neq j$ but not in $\mathfrak{p}_j$, and of course it belongs to $\mathfrak{a}$ since x_j does. It ensues that the sum $z_1 + \ldots + z_r$ is a member of $\mathfrak{a}$, but not of any of the $\mathfrak{p}_i$'s (each term lies in $\mathfrak{a}$ and for a given j all but one lie in $\mathfrak{p}_j$). ❑

Notice that the proof merely requires $\mathfrak{a}$ be closed under addition and multiplication, so the ideal $\mathfrak{a}$ may be replaced with a "weak subring" (a subring without a unit element).

2.29 At several later occasions we shall meet diverse unions and intersections of prime ideals. In case there are no non-trivial inclusions among the involved prime ideals, they enjoy strong uniqueness properties; in fact, the primes involved are determined by their intersection or their union, as expressed in the following twin lemmas.

LEMMA 2.30 *Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ and $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\}$ be two families of prime ideals having the same union; that is, $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r = \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_s$. Assume that there are no non-trivial inclusion relations in either family. Then the two families coincide.*

PROOF: For each index ν one has $\mathfrak{p}_\nu \subseteq \bigcup_j \mathfrak{q}_j$ and the PRIME AVOIDANCE LEMMA gives that there is an index $\alpha(\nu)$ so that the relation $\mathfrak{p}_\nu \subseteq \mathfrak{q}_{\alpha(\nu)}$ holds. By symmetry, for each μ there is a $\beta(\mu)$ such that $\mathfrak{q}_\mu \subseteq \mathfrak{p}_{\beta(\mu)}$. Now

$$\mathfrak{p}_\nu \subseteq \mathfrak{q}_{\alpha(\nu)} \subseteq \mathfrak{p}_{\beta(\alpha(\nu))}$$

and there being no non-trivial inclusion relations among the $\mathfrak{p}_i$'s we infer that $\beta(\alpha(\nu)) = \nu$. In a symmetric manner one shows that $\alpha(\beta(\mu)) = \mu$ and we can conclude that α is a bijection from $\{1, \ldots, r\}$ to $\{1, \ldots, s\}$ with $\mathfrak{p}_\nu = \mathfrak{q}_\alpha(\nu)$, and we are happy. ❑

LEMMA 2.31 *Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ and $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\}$ be two families of prime ideals having the same intersection; that is, $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$. Assume that there are no non-trivial inclusion relations in either family. Then the two families coincide.*

PROOF: For each index ν one has $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \bigcap \mathfrak{q}_j \subseteq \mathfrak{q}_\nu$ and therefore at least for one index, say $\alpha(\nu)$, the relation $\mathfrak{p}_{\alpha(\nu)} \subseteq \mathfrak{q}_v$ holds. By symmetry, for each μ there is a $\beta(\mu)$ such that $\mathfrak{q}_{\beta(\mu)} \subseteq \mathfrak{p}_\mu$. Now

$$\mathfrak{p}_{\alpha(\beta(\mu))} \subseteq \mathfrak{q}_{\beta(\mu)} \subseteq \mathfrak{p}_\mu$$

and there being no non-trivial inclusion relations among the $\mathfrak{p}_i$'s we infer that $\alpha(\beta(\mu)) = \mu$. In a symmetric manner one shows that $\beta(\alpha(v)) = \nu$ and we can conclude that α is a bijection from $\{1, \ldots, r\}$ to $\{1, \ldots, s\}$ with with $\phi_{\alpha(v)} = \mathfrak{q}_v$ ❑

Problems

2.12 Let $\mathfrak{p}$ be a prime ideal in a ring A. Show that $\mathfrak{p}A[T]$ is prime

★

2.4 *Principal ideals*

Principal ideals are among the simplest type of ideals, and being omnipresent in the theory they deserve special attention. So we offer a few basic results about them.

2.32 Different elements can generate the same principal ideal, but they will, at least in domains, be closely related, as described in the next lemma.

LEMMA 2.33 *Two non-zero divisors a and b in a ring A generate the same principal ideal precisely when they are related by a unit; that is, when $a = ub$ where $u \in A^*$.*

PROOF: When $(a) \subseteq (b)$ there is a ring element u so that $a = ub$, and when $(b) \subseteq (a)$ it holds that $b = va$, Hence $a = vua$. And a not being a zero-divisor, we conclude that $vu = 1$. ❑

In the case of the ring A possessing zero-divisors, things are more complicated. For instance, in the ring $k[x, y, z]/(z(1 - xy))$ it holds true that $(z) = (xz)$, but the two generators z and xz are not related by a unit (see Exercise 2.19 below).

Primes and irreducibles

In general rings there are two twin notions each arising from a different aspect of prime numbers.

2.34 The first of the twins is the notion of *prime elements* in a ring. The definition is verbatim the same as one of the characterizations of prime numbers: A *prime element* in a ring A is an element a which is neither zero nor a unit and is such that if a divides a product, it divides one of the factors; in other words, a relation like $bc = ya$ for some y implies $c = xa$ or $b = xb$ for some x. The property is not restricted to products with two factors, a straightforward induction proves that if a is a prime element and divides the product $b_1 \cdots b_r$, it divides one of the factors.

Prime elements (*primelementer*)

The concept of a prime ideal is also inspired by that of prime numbers, and for principal ideals the two coincide; an element a being prime is equivalent to the principal ideal (a) being a prime ideal.

PROPOSITION 2.35 *A principal ideal (a) is a prime ideal exactly when a is a prime element.*

PROOF: Recall what a being prime means: If $a|bc$ then either $a|b$ or $a|c$. Translated into a statement about ideals $x|y$ means that $y \in (x)$. Hence, $bc \in (a)$ is equivalent to $a|bc$, and $b \in (a)$ or $c \in (a)$ to $a|b$ or $a|c$. ❑

2.36 An other aspect of prime numbers (which in fact is the usual definition) is they can not be further factored; that is, their sole factors are 1 and the prime itself. Irreducible polynomials in $k[x]$ share this quality except they can be changed by non vanishing constant factors (of course $f = c^{-1} \cdot cf$ for any non-zero constant c). Generalizing these two notions, one says that a non-zero element a from the ring A is *irreducible* if it is not a unit, and if a relation $a = bc$ implies that either b or c is a unit.

irreducible elements (*irreducible elementer*)

In a domain, this can phrased in terms of ideals and a certain maximality condition.

PROPOSITION 2.37 *An element a in the domain A is irreducible if and only if (a) is maximal among the proper principal ideal.*

PROOF: A relation $a = bc$ is equivalent to an inclusion $(a) \subseteq (b)$, and when (a) enjoys the maximality property it ensues that either $(a) = (b)$ and c is a unit, or $(b) = A$ and b is a unit. ❑

PROPOSITION 2.38 *Every prime element in a domain A is irreducible.*

PROOF: Assume that a is prime element in A and that $a = bc$. Since a is prime it holds true that $b = xa$ or $c = xa$ for some $x \in A$, say $b = xa$. Substituting back yields $a = xca$ and cancelling a, which is legal since A is supposed to be a domain, we arrive at $1 = xc$ which shows that c is a unit. ❑

The converse of this proposition is not generally valid, in fact one is tempted to say that in most rings it does not hold, but we shall shortly meet classes (see Proposition 2.41 on page 36) of rings where it is true. There are simple examples of irreducibles not being prime in quadatic extensions of $\mathbb{Z}$. We give one in the ring $\mathbb{Z}[\sqrt{-5}]$ below (Example 2.14 on page 37).

Principal ideal domains

Principal ideal domains (Hovedidealområder)

Rings in which all ideals are principal, are among the easiest rings to understand. They are called *principal ideal domains*, and this being a long name the acronym PID emerges expeditiously. In a later chapter, we shall come back to these rings together with three of their cousins, but because fundamental rings like $\mathbb{Z}$ and the polynomial ring $k[x]$ are PID's, the PID's merit an entrance early in the play.

2.39 One of the particular properties enjoyed by a principal ideal domain is there is no distinction between maximal and non-zero prime ideals.

PROPOSITION 2.40 *In a principal ideal domain A, any non-zero prime ideal is maximal.*

PROOF: A non-zero prime ideal is generated by a prime element a, and as any other prime element, a is irreducible. From Proposition 2.37 above ensues that (a) then is maximal among the proper principal ideals, but all ideals being principal, (a) is maximal. ❑

Neither is there any distinction between prime and irreducible elements:

PROPOSITION 2.41 *In a principal ideal domain A an element is prime if and only if it is irreducible.*

PROOF: An irreducible element a generates according to Proposition 2.37 above an ideal maximal among the proper principal ideals, but because all ideals are principal, (a) is a maximal ideal. Hence it is a prime ideal, and a is a prime element. ❑

Euclidean rings

The classical division algorithm for integers, which also goes under the name of Euclid's algorithm (you certainly learned it in school), ensures that the ring of integers $\mathbb{Z}$ is a PID:

PROPOSITION 2.42 *The ring $\mathbb{Z}$ of integers is a principal ideal domain.*

PROOF: Let $\mathfrak{a}$ be a non-zero ideal in $\mathbb{Z}$, and let n be the smallest positive number in $\mathfrak{a}$. Any other element a from $\mathfrak{a}$ may be divided by n to give a relation $a = q \cdot n + r$ where the remainder r is of absolute value less than n. Now, $r = a - q \cdot n$ is an element of $\mathfrak{a}$, and this contradicts the minimality of n unless $r = 0$; therefore $a = q \cdot n$, and the ideal $\mathfrak{a}$ equals the principal ideal (n). ❑

2.43 The argument above is a classic but not limited to the ring of integers. It goes through once there is a function on A for which there is a Euclidian algorithm; that is, a function δ on A assuming values in $\mathbb{N}$ or $\mathbb{N}_0$ with the following property[2]:

- For any pair x and y of elements in A there are elements q and r in A so that $x = yq + r$ and $\delta(r) < \delta(y)$.

Such a function is called a *Euclidian function*, and a domain A is said to be a *Euclidean domain* if it possesses one.

The absolute value used in the proof of Proposition 2.42 above is one example, but there are many others. For instance, on the polynomial ring $k[x]$ over a fields, putting $\delta(f) = \deg f + 1$ if $f \neq 0$ and $\delta(0) = 0$ we get one; indeed, the Euclidean condition is fulfilled by the procedure of long division. The point with these Euclidian functions is that they forces a domain to be a PID as in the following proposition; whose proof is *mutatis mutandis* the same as that of Proposition 2.42.

[2] One is not confined to use functions with values in $\mathbb{N}$; functions with values in any well-ordered set will do.

Euclidian functions (*Euklidske funksjoner*)

Euclidean domain (*Euklidske områder*)

PROPOSITION 2.44 *A domain A that possesses a Euclidean function is a* PID.

PROOF: Let $\mathfrak{a}$ be a non-zero proper ideal in A, and let $a \in \mathfrak{a}$ minimize $\delta(x)$ as x runs through the non-zero elements in $\mathfrak{a}$. We contend that a generates $\mathfrak{a}$. If $f \in \mathfrak{a}$, there are elements q and r with $f = aq + r$ and $\delta(r) < \delta(a)$. Now, $r = f - aq$ lies in $\mathfrak{a}$, and consequently $r = 0$ since $\delta(a)$ is minimal among values of δ assumed on non-zero elements in $\mathfrak{a}$. ❑

COROLLARY 2.45 *Let k be a field. Then the polynomial ring $k[x]$ is a* PID.

Examples

2.12 In the polynomial $k[x]$ over a field k principal ideals $(f(x))$ with f irreducible, are maximal ideals. The quotient $K = k[x]/(f(x))$ is a field which is obtained from k by adjoining a root of f. If you wonder what that root is, it is just the residue class $[x]$ of the variable x. This illustrates the devise that what matters in modern mathematics is "what objects do, not what they are".

2.13 The quotient $\mathbb{R}[x]/(x^2 + 1)$ is isomorphic to $\mathbb{C}$ as one sees mapping x to i. In a similar vein, if p is a prime number, the polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over $\mathbb{Q}$, so that $\mathbb{Q}[x]/\Phi_p(x)$ is a field. Sending x to a primitive p-root of unity ξ , gives an isomorphism with $\mathbb{Q}(\xi)$.

2.14 Simple and concrete examples of irreducible elements that are not prime are found in the ring $\mathbb{Z}[\sqrt{-5}]$ where among others the relation

$$2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}) \tag{2.3}$$

holds. So, for instance, 2 is not a prime element since neither $1 + i\sqrt{5}$ nor

$1 - i\sqrt{5}$ is a unit (units have absolute value 1, cfr. Exercise 1.10 on page 14). The element 2 is however irreducible in $\mathbb{Z}[\sqrt{-5}]$, for if $2 = zw$, one has $2 = \|z\|\|w\|$, and as the square of the absolute value of members of $\mathbb{Z}[\sqrt{-5}]$ are natural numbers, this entails that either $\|z\| = 1$ or $\|w\| = 1$; hence, again in view of Exercise 1.10, either z or w is a unit. Of course, the three other numbers appearing in (2.3) are irreducible as well, and Exercise 2.20 below asks you to check this. For a generic example of irreducible elements not being prime, see Exercises 2.43 and 2.44 on page 52.

2.15 *(The Gaussian integers)* The absolute value works as a Euclidean function on the ring $\mathbb{Z}[i]$. Indeed, geometrically the Gaussian integers form the integral lattice in the complex plane; that is, the set of points both whose coordinates are integers. Given two Gaussian integers a and q with $q \neq 0$, the distance from a to the nearest point in the integral lattice is obviously less then half the diagonal of a lattice square; that is, there is an element $c \in \mathbb{Z}[i]$ so that $\|a/b - c\| \leqslant \sqrt{2}/2 < 1$. Putting $r = q(a/q - c)$, we have $a = cq + r$ with $\|r\| < \|q\|$.

☆

Problems

2.13 Let $p_1, \ldots, p_r$ be prime numbers and let $A = \mathbb{Z}/(p_1 \cdot \ldots \cdot p_r)$. Show that the prime ideals in A are precisely the principal ideals (p_i). Prove that A/p_iA is the field $\mathbb{F}_{p_i}$ with p_i elements. How many elements does (p_i) have? An how many are there in the principal ideal $(p_1 \cdot \ldots \cdot \hat{p_i} \cdot \ldots \cdot p_r)$ (the "hat" indicates that p_i is not included in the product).

2.14 Given two ideals (n) and (m) in $\mathbb{Z}$. Show that $(n) \subseteq (m)$ if and only if $m|n$. Conclude that the partially ordered set $\mathcal{I}(\mathbb{Z})\backslash\{(0)\}$ of non-zero ideals in $\mathbb{Z}$ is isomorphic to the the set of natural numbers ordered by *reverse* divisibility.

2.15 Let n and m be two natural numbers. Describe (n, m) and $(n) \cap (m)$.

2.16 Find an explicit isomorphism between $\mathbb{R}[x]/(x^2 + x + 1)$ and $\mathbb{C}$. ✲

2.17 Let p be a prime not congruent one modulo four. Show that the polynomial $x^2 + 1$ is irreducible over the field $\mathbb{F}_p$, and that $\mathbb{F}_p[x]/(x^2 + 1)$ is a field isomorphic to $\mathbb{F}_p(\sqrt{-1})$. How many elements does it have? ✲

2.18 Into which of the fields $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$ is there a map of rings from $\mathbb{Z}[i]$? If there is one, describe the kernel.

2.19 Show that the units in $k[x, y, z]/(z(1 - xy))$ are the constants k^*. Show that there is no unit $u \neq 1$ so that $uz = xz$. Conclude that z and xz are not ✲

related by a unit even though $(z) = (xz)$. HINT: Killing z gives a ring-map $k[x,y,z]/(z(1-xy)) \to k[x,y]$. Setting $x = 1$, gives a ring map $k[x,y,z]/(z(1-xy)) \to k[z,y]/(z(1-y))$.

2.20 Referring to Example 2.14 show that the three other involved numbers 3, $1+i\sqrt{5}$ and $1-i\sqrt{5}$ are irreducible.

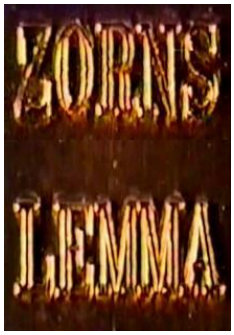
2.21 Show that $\mathbb{Z}[\sqrt{-2}]$ is principal ideal domain. HINT: Prove that A is Euclidean with the absolute value as a Euclidean function.

2.22 Let $A = \{\, n/2 + im/2\sqrt{3} \mid n, m \in \mathbb{Z} \,\}$. Prove that A is a subring of $\mathbb{C}$. Prove that A is Euclidean

★

2.5 *Existence theorems*

A useful technique for showing that ideals (and in later chapters submodules) of various kinds exist relies on the so-called Zorn's lemma. The lemma is a general result about existence of maximal elements in partially ordered sets, which for us will be the lattice $\mathcal{I}(A)$ of ideals ordered by inclusion, and it turns out to be very useful when studying rings and it will be used several times in the sequel.



Max August Zorn
(1906–1993)
German mathematician

Zorn's lemma

Zorn's lemma which is one of a few theorems that for some reason keep being called lemmas, is usually attributed to Max Zorn, but as often happens, it can be traced further back. At least Felix Hausdorff published versions of it some ten years before Zorn. Any how, "Zorns lemma" is good name (so good that an experimental and non-narrative film made by Hollis Frampton in 1970 was called "Zorns lemma").

2.46 A *maximal element* x in the partially ordered set Σ is one for which there is no strictly larger element; that is, if $y \geqslant x$ then $y = x$. One should not confuse "maximal elements" with "largest elements" the latter being elements larger than all other elements in Σ. A partially ordered set can have several maximal elements whereas a largest element, if there is one, is unique. There is of course, analogous notions of *minimal elements* and *least* elements.

Maximal elements (*Maksimale elementer*)

A partially ordered set is said to be *linearly ordered* or *totally ordered* if any two of its elements can be compared. Phrased differently, for any pair x, y of elements either $x \leqslant y$ or $y \leqslant x$ should hold. *A chain* in Σ is a linearly ordered subset of Σ. The chain is *bounded above* if for some element $x \in \Sigma$ it holds true that $y \leqslant x$ for all elements y in the chain, and then of course, x is called an *upper bound* for the chain. Similarly, the chain is said to be *bounded below* when

Linearly ordered sets (*Lineært ordnede mengder*)

Totally ordered sets (*Totalt ordnede mengder*)

Chains (*Kjeder*)

Bounded above (*Opptil begrenset*)

Upper bounds (*Øvre skranker*)

Bounded below (*Nedtil begrenset*)

having a *lower bound* in Σ; that is, an element $x \in \Sigma$ satisfying $x \leqslant y$ for all members y of the chain.

Lower bound (*Nedre skranke*)

We are now prepared to formulate Zorn's lemma, however we shall not prove it, only mention that it is equivalent to the axiom of choice (If you are interested in reading more about this, consult xxx)

THEOREM 2.47 (ZORN'S LEMMA) *Let Σ be a partially ordered set in which every chain is bounded above. Then Σ possesses a maximal element.*

2.48 A chain C in Σ is called *saturated* or *maximal* if it is not properly contained in any larger chain, or phrased differently, C is a maximal chain in Σ; that is, if C' is another chain with $C \subseteq C'$, then $C = C'$. A chain is saturated precisely when it impossible to insert any new element in-between two members of C. As an illustration of the mechanism of Zorn's lemma, let us prove the following

Saturated or maximal chains (*Mettede eller maksimale kjeder*)

PROPOSITION 2.49 *Let C be a chain in the partially ordered set Σ. Then there is a saturated chain containing C.*

PROOF: The set of chains in Σ is partially ordered by inclusion, and we intend to apply Zorn's lemma to that set.

If $\mathcal{C}$ is a chain of chains (!!) clearly the union $\bigcup_{C \in \mathcal{C}} C$ is anew a chain; indeed, suppose that x and y belong to the union so that there are chains C_x and C_y with and $x \in C_x$ and $y \in C_y$. By assumption $\mathcal{C}$ is a chain, and either $C_x \subseteq C_y$ or $C_y \subseteq C_x$ holds. In either case x and y lie in a common chain and are comparable. ❑

A basic existence result

A frequent application of Zorn's lemma in commutative algebra is to prove existence of ideals that are maximal subjected to a given condition, in many situations such maximizing ideals turn out to be prime ideals.

In this section we shall establish a basic existence result with several important applications, one being that every ring has at least one maximal ideal. We shall be interested in ideals maximal among those containing a fixed ideal and being disjoint from a fixed set S. These maximizing ideals turn out to be prime when S is multiplicatively closed; that is, if the product of any two elements from S lie in S.

THEOREM 2.50 (THE BASIC EXISTENCE THEOREM FOR IDEALS) *Assume given a ring A, an ideal $\mathfrak{a}$ in A and a subset S not meeting $\mathfrak{a}$. Then there exists an ideal $\mathfrak{b}$ maximal subjected to the two following conditions*

- $S \cap \mathfrak{b} = \varnothing$;
- $\mathfrak{a} \subseteq \mathfrak{b}$.

If S is multiplicatively closed, the ideal $\mathfrak{b}$ will be a prime ideal.

PROOF: Consider the set Σ of ideals in A satisfying the two requirements in the proposition. It is non-empty because $\mathfrak{a}$ is supposed not to meet S. Obviously, the union of the ideals belonging to a chain in Σ, will lie in Σ, and thus will be an upper bound for the chain. Zorn's lemma applies, and we can conclude that there is a maximal element in Σ.

Assume then that the set S is closed under multiplication and let a and b be elements in A such that $a \cdot b \in \mathfrak{b}$. If neither belongs to $\mathfrak{b}$, the ideals $\mathfrak{b} + (a)$ and $\mathfrak{b} + (b)$ both meet S, being strictly larger than $\mathfrak{b}$. Hence we can find elements $x + \alpha a$ and $y + \beta b$ in S with $x, y \in \mathfrak{b}$ and $\alpha, \beta \in A$, and multiplying, out we find

$$(x + \alpha a)(y + \beta b) = xy + \alpha a x + \beta b x + \alpha\beta ab.$$

The left side belongs to S as S is supposed to be multiplicatively closed, and since x, y and ab all lie in $\mathfrak{b}$, the right side belongs to $\mathfrak{b}$, which contradicts the fact that $S \cap \mathfrak{b} = \varnothing$. ❑

THEOREM 2.51 (EXISTENCE OF MAXIMAL IDEALS) *Let A be a ring different from the null-ring. Every proper ideal $\mathfrak{a}$ in a ring A is contained in a maximal ideal. In particular, there is at least one maximal ideal in every ring.*

PROOF: We apply the proposition with S merely consisting of the unit element, that is $S = \{1\}$. The maximizing ideal is proper and not contained in any other proper ideal. Hence it is maximal. To prove the second statement, apply the first to the zero ideal. ❑

The radical of an ideal

Primes frequently occur with higher multiplicities in a factorization of an integer n. It is of course interesting to get hold of the primes involved; that is, the primes p so that some power of p divides n. In the transcription of Kummer and Dedekind into the language of ideals, this leads to the notion of the *radical* of a given ideal.

The radical of an ideal (*radikalet til et ideal*)

2.52 The *radical* $\sqrt{\mathfrak{a}}$ of a given ideal $\mathfrak{a}$ in A consists of the elements a power of which lies in $\mathfrak{a}$; that is,

$$\sqrt{\mathfrak{a}} = \{\, a \in A \mid a^n \in \mathfrak{a} \text{ for some } \ n \in \mathbb{N} \,\}.$$

The elements of $\sqrt{\mathfrak{a}}$ can also be characterized as the elements in A whose residue class in $A/\mathfrak{a}$ is nilpotent. Along the same line, taking $\mathfrak{a}$ to be the zero ideal, we see that $\sqrt{(0)}$ is the set of nilpotent elements in A.

2.53 The first thing to establish is that the radical $\sqrt{\mathfrak{a}}$ in fact is an ideal.

LEMMA 2.54 *Let $\mathfrak{a}$ be an ideal in the ring A. Then the radical $\sqrt{\mathfrak{a}}$ is an ideal.*

PROOF: The radical is obviously closed under multiplication by ring elements, and we merely have to check it is closed under addition. So assume that a and b are two elements in the ring such that $a^n \in \mathfrak{a}$ and $b^m \in \mathfrak{a}$. The binomial theorem gives

$$(a+b)^N = \sum_{0 \leqslant i \leqslant N} \binom{N}{i} a^{N-i} b^i.$$

Choosing $N = n + m - 1$, we see that when $i < m$ it holds that $N - i \geqslant n$, so either a^{N-i} or b^i lies in $\mathfrak{a}$. Every term of the sum therefore lies in $\mathfrak{a}$, and by that the sum itself. ❑

Specializing $\mathfrak{a}$ to be the zero ideal yields the following.

COROLLARY 2.55 *The set of nilpotent elements in A form an ideal.*

2.56 An ideal $\mathfrak{a}$ in A is a *radical* if it equals is own radical; *i.e.* it holds true that $\sqrt{\mathfrak{a}} = \mathfrak{a}$. One easily verifies that the radical of an ideal is a radical ideal: that is, one has $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$. In the same manner with prime ideals and maximal ideals, radical ideals can be characterized in terms of quotients:

Radical ideals (*Radikale idealer*)

PROPOSITION 2.57 *An ideal $\mathfrak{a}$ in the ring A is a radical ideal if and only if the quotient $A/\mathfrak{a}$ is reduced.*

PROOF: The residue class $[a]$ in $A/\mathfrak{a}$ of an element a is nilpotent precisely when a power a^n lies in $\mathfrak{a}$, which in its turn is equivalent to $a \in \mathfrak{a}$ since $\sqrt{\mathfrak{a}} = \mathfrak{a}$ by hypothesis. ❑

2.58 The radical of an ideal $\mathfrak{a}$ must be contained in any prime ideal containing it because if $a^n \in \mathfrak{a}$ and $\mathfrak{a} \subseteq \mathfrak{p}$ with $\mathfrak{p}$ prime, it holds that $a \in \mathfrak{p}$. The converse is also true and hinges on the basic existence theorem above.

PROPOSITION 2.59 *Assume that $\mathfrak{a}$ is a proper ideal in the ring A. The radical $\sqrt{\mathfrak{a}}$ equals the intersection of the prime ideals containing $\mathfrak{a}$; that is,*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p},\ \mathfrak{p} \text{ prime}} \mathfrak{p}.$$

PROOF: We already saw that $\sqrt{\mathfrak{a}} \subseteq \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p}$, so assume that a is an element not lying in the radical $\sqrt{\mathfrak{a}}$. We shall apply Theorem 2.50 on page 40 with S being the set $\{ a^n \mid n \in \mathbb{N} \}$ of powers of a, which obviously is closed under multiplication. Since $a \notin \sqrt{\mathfrak{a}}$, it holds that $S \cap \mathfrak{a} = \varnothing$, and by the theorem we conclude that there is prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ disjoint from S; that is, $a \notin \mathfrak{p}$. ❑

The special case that $\mathfrak{a} = (0)$ merits to be pointed out:

COROLLARY 2.60 *The set of nilpotent elements in A equals the intersection of all prime ideals in A; that is*

$$\sqrt{(0)} = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}.$$

2.61 One might be tempted to discard the prime ideals not being minimal among those containing $\mathfrak{a}$ from the intersection in Proposition 2.59, and thus write

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \text{ minimal prime over } \mathfrak{a}} \mathfrak{p}. \tag{2.4}$$

Such a representation is certainly valid, but the argument is more complicated since *a priori* there could be infinitely descending chains of distinct prime ideals. However, if $\{\mathfrak{p}_i\}_{i\in I}$ is a chain of prime ideals, the intersection $\bigcap_{i\in I} \mathfrak{p}_i$ is a prime ideal, and so by Zorn's lemma, every prime containing $\mathfrak{a}$ contains a prime ideal minimal among those containing $\mathfrak{a}$; which is exactly what is need to have a representation as in (2.4). (See and do Exercise 2.23 below.)

2.62 The operation of taking the radical commutes with taking finite intersections; one has

LEMMA 2.63 *For every finite collection $\{\mathfrak{a}_i\}$ of ideals in A it holds true that $\bigcap_i \sqrt{\mathfrak{a}_i} = \sqrt{\bigcap_i \mathfrak{a}_i}$.*

PROOF: When an element a from A belongs to each of the radicals $\sqrt{\mathfrak{a}_i}$, there are integers n_i so that $a^{n_i} \in \mathfrak{a}_i$. With $n = \max n_i$, it then holds true that $a^n \in \mathfrak{a}_i$ for each i, and thus $a \in \sqrt{\bigcap_i \mathfrak{a}_i}$. This shows that one has the inclusion $\bigcap_i \sqrt{\mathfrak{a}_i} \subseteq \sqrt{\bigcap_i \mathfrak{a}_i}$. The other inclusion is straightforward. ❑

Examples

2.16 Even if a power of every element in $\sqrt{\mathfrak{a}}$ lies in $\mathfrak{a}$, no power of $\sqrt{\mathfrak{a}}$ will in general be contained in $\mathfrak{a}$. A simple but typical example being the ideal $\mathfrak{a} = (x_1, x_2^2, x_3^3, \ldots)$ generated by the powers x_i^i in the polynomial ring $k[x_1, x_2, x_3, \ldots]$ in countably many variables. The radical of $\mathfrak{a}$ is equal to the maximal ideal $\mathfrak{m} = (x_i | i \in \mathbb{N}_0)$ generated by the variables, but no power of $\mathfrak{m}$ is contained in $\mathfrak{a}$. Indeed, the exponent needed to force a power of x_i to lie in $\mathfrak{a}$, tends to infinity with i.

2.17 The operation of taking radicals respects finite intersections, but this is no more true when it comes to infinite intersections. For instance, if p is a prime number, one has $\sqrt{p^r\mathbb{Z}} = p\mathbb{Z}$ and therefore $\bigcap_r \sqrt{p^r\mathbb{Z}} = p\mathbb{Z}$, but evidently it holds true that $\bigcap_r p^r\mathbb{Z} = 0$.

☆

Problems

2.23 That minimal and maximal prime ideals exist ensues directly from Zorn's lemma as this exercise shows. Let $\{\mathfrak{p}_i\}_{i\in I}$ be a chain of prime ideals. Show that both the union $\bigcup_{i\in I} \mathfrak{p}_i$ and the intersection $\bigcap_{i\in I} \mathfrak{p}_i$ are prime ideals. ⁂

Show that every prime ideal containing a given ideal $\mathfrak{a}$ contains a a prime ideal minimal over $\mathfrak{a}$.

2.24 A multiplicatively closed set S in the ring A is said to be *saturated* if with x it contains every factor of x; that is, if $x \in S$ and $x = yz$, then $y \in S$ (and by symmetry $z \in S$). Show that S is a saturated multiplicative set if and only if the complement $A\backslash S$ is the union of prime ideals. HINT: Assume that $a \notin S$ and apply Theorem 2.50 with the ideal $\mathfrak{a}$ being the principal ideal (a).

Saturated multiplicative sets (*Meted multiplicative mengder*)

2.25 Let A be any ring. Show that the set of non-zero divisors in A form a saturated multiplicative set. Conclude that the set of zero divisors is the union of prime ideals.

2.6 *Local rings*

Rings having one single maximal ideal are called *local rings*. They occupy a central place in the theory being simpler than many other rings, and a frequently applied strategy of proof is to reduce an issue to a statement about local rings. In the analogy with rings of functions, the local rings correspond to rings of germs of functions near a point—hence the name. There is also the notion of a *semi-local ring*, which is a ring with finitely many maximal ideals.

Local rings (*Lokale ringer*)

Semi-local rings (*Semilokale ringer*)

2.64 In a local ring A with maximal ideal $\mathfrak{m}$ the complement of $\mathfrak{m}$ coincides with the group of the units; that is, every element $a \in A$ not lying in $\mathfrak{m}$ is invertible. Indeed, if it were not, the principal ideal (a) would be a proper ideal and by Theorem 2.51 on page 41 would be contained in a maximal ideal, obviously different from $\mathfrak{m}$, which would contradict that $\mathfrak{m}$ is the sole maximal ideal in A. This proves that the first statement in the following proposition implies the second.

PROPOSITION 2.65 *Let A be a ring and $\mathfrak{m}$ a proper ideal in A. The following three statements are equivalent.*

- *A is a local ring with maximal ideal $\mathfrak{m}$;*
- *The group of units and the complement of $\mathfrak{m}$ coincide; that is, $A^* = A\backslash\mathfrak{m}$;*
- *The ideal $\mathfrak{m}$ is maximal and consists of the elements a such that $1 + a$ is invertible.*

PROOF: To see the last statement ensues from the second, let a be a member of $\mathfrak{m}$. Then of course $1 + a$ is not in $\mathfrak{m}$ and hence is invertible.

Finally, let $\mathfrak{m}$ be maximal and assume that any element shaped like $1 + a$ is invertible. Let x be an element not in $\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, it holds true that $\mathfrak{m} + (x) = A$; hence $x = 1 + a$ for some $a \in \mathfrak{m}$, and x is invertible. ❑

The assumption in the last statement that $\mathfrak{m}$ be maximal, is necessary; for an example see Exercise 2.28 below.

2.66 The argument in previous paragraph partially goes through in a slightly more general situation involving the so-called *Jacobson radical* $J(A)$ of a ring A, which is the intersection of all the maximal ideals in A. In other words, $J(A) = \bigcap_{\mathfrak{m} \subseteq A \text{ maximal}} \mathfrak{m}$.

Jacobson radical (*Jacobson-radikalet*)

PROPOSITION 2.67 *Let A be a ring. The Jacobson radical of A consists of the ring elements a so that $1 + xa$ is invertible for all $x \in A$.*

PROOF: Fix an element a in A. Firstly, assume that elements of shape $1 + xa$ all are invertible. If there is a maximal ideal $\mathfrak{m}$ so that $a \notin \mathfrak{m}$, it holds true that $\mathfrak{m} + (a) = A$. Then there is a relation $1 = y + ax$ with $y \in \mathfrak{m}$. It ensues that $1 - xa$ lies in $\mathfrak{m}$, but on the other hand, $1 - ax$ is invertible by assumption; and we have the contradiction that $\mathfrak{m} = A$.

Remember, maximal ideals are proper ideals

Assume then that a lies in all maximal ideals. If $(1 + ax)$ is a proper ideal, it is by the fundamental existence theorem (Theorem 2.50 on page 40) contained in a maximal ideal $\mathfrak{n}$. Since $a \in \mathfrak{n}$, it follows that $1 \in \mathfrak{n}$, contradicting $\mathfrak{n}$ being proper. Hence $(1 + ax)$ is not proper, and $1 + ax$ is invertible. ❑

2.68 Assume that A and B are two local rings whose maximal ideals are $\mathfrak{m}_A$ and $\mathfrak{m}_B$ respectively. A map of rings $\phi\colon A \to B$ is said to be a *local homomorphism*, or a map of local rings, $\phi(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$. Equivalently, one may request that $\phi^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$.

Local homomorphism (*Lokal homomorfi*)

Examples

2.18 The set of rational functions over a field k that may be expressed as $P(x)/Q(x)$ with $P(x)$ and $Q(x)$ polynomials and $Q(0) \neq 0$, is a local ring whose maximal ideal equals the set of the functions vanishing at the origin. The evaluation map $P(x)/Q(x) \mapsto P(0)/Q(0)$ identifies the residue field with the field of complex numbers $\mathbb{C}$.

2.19 Let p be a prime number and let $\mathbb{Z}_{(p)}$ be the ring of rational numbers expressible as n/m where the denominator m is relatively prime to p. Then $\mathbb{Z}_{(p)}$ is a local ring whose maximal ideal is generated by p.

More is true, the only ideals in $\mathbb{Z}_{(p)}$ are the principal ideals (p^v); indeed, every rational number lying in $\mathbb{Z}_{(p)}$ may be written as $p^v n/m$ with $v \geqslant 0$ and neither n nor m having p as factor. And among these ideals (p) contains all the others.

2.20 In a polynomial ring $\mathbb{C}[x_1, \ldots, x_r]$ for all points $a \in \mathbb{C}^r$ the ideal of polynomials vanishing at a is a maximal ideal. It follows that the Jacobson radical f $C[x_1, \ldots, x_r]$ equals (0); i

2.21 Assume that p and q are two prime numbers. Let A be the ring of rational numbers with denominator relatively prime to pq. That is $A = \{\, n/m \mid n, m \in \mathbb{Z}, (m, pq) = 1 \,\}$. The principal ideals by (p) and (q) are the only two maximal ideals in A, and $J(A) = (p) \cap (q) = (pq)$.

☆

Problems

2.26 Show that a ring has just one prime ideal if and only if its elements are either invertible or nilpotent. Prove that this is the case if and only if $A/\sqrt{(0)}$ is a field. ✲

2.27 With reference to Exercise 1.22 on page 21, show that the ring $\mathbb{Z}_p$ of p-adic integers is a local ring whose sole maximal ideal is generated by p.

2.28 Let A be the subring of $\mathbb{Q}$ whose elements are the rational numbers a expressible as $a = m/n$ where n does have neither 2 nor 3 as factor. Show that A has two maximal ideals (2) and (3) whose intersection equals (6). What are the two residue fields? Show that $1 + a$ is invertible in A for all members $a \in (6)$.

2.29 Let $p_1, \ldots, p_r$ be distinct prime numbers and let A be the subset of $\mathbb{Q}$ whose members can be written as m/n with n relatively prime to p_i for $1 \leqslant i \leqslant r$. Show that A is a semi-local ring. Describe the maximal ideals and the residue fields. What is the Jacobson radical?

2.30 Let $k_1, \ldots, k_r$ be fields. Show that the product ring $\prod_i k_i$ is a semi-local ring. What are the maximal ideals? ✲

2.31 Let $f(x)$ be any polynomial in $k[x]$ where k is a field. Show that $k[x]/(f(x))$ is semi-local. ✲

★

2.7 *Direct products and the Chinese Remainder Theorem*

Ideals in a direct product

Let $A = \prod_{1 \leqslant i \leqslant r} A_i$ be the direct product of rings A_i. There is a simple description of ideals in A in terms of ideals in the A_i's. One produces an ideal $\mathfrak{a}$ in A from a sequence of ideals $\mathfrak{a}_i$ in the A_i's simply by putting $\mathfrak{a} = \prod_i \mathfrak{a}_i$. And, indeed, all ideals in A are of this shape.

To see this, let $\{e_i\}_{1 \leqslant i \leqslant r}$ be the orthogonal idempotents corresponding to the decomposition of A as a direct product. Then $A_i = e_i A$ and each $e_i \mathfrak{a}$ is an ideal in A_i contained in $\mathfrak{a}$, and because $\sum_i e_i = 1$, it holds true that $\mathfrak{a} = \sum_i e_i \mathfrak{a}$.

PROPOSITION 2.69 *The ideals of* $A = \prod_{1\leqslant i\leqslant r} A_i$ *are all of the form* $\prod_{1\leqslant i\leqslant r} \mathfrak{a}_i$ *where each* $\mathfrak{a}_i$ *is ideal in* A_i*. It holds true that* $A/\mathfrak{a} \simeq \prod_{1\leqslant i\leqslant r} A_i/\mathfrak{a}_i$*. The ideal* $\mathfrak{p}$ *is a prime ideal if and only if* $\mathfrak{p}_i = A_i$ *for all but one index* i*.*

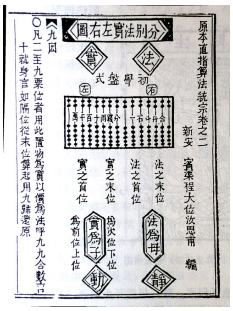
PROOF: The projection mappings $A \to A_i$, coinciding with multiplication by e_i, send $\mathfrak{a}$ to $\mathfrak{a}_i$ and induce maps $A/\mathfrak{a} \to A_i/\mathfrak{a}_i$, which in their turn give a ring-map $A/\mathfrak{a} \to \prod_i A_i/\mathfrak{a}_i$. The map is surjective since $A \to \prod_i A_i$ is, and if x in A such that $e_i x \in \mathfrak{a}_i$ for each i, the element x belongs to $\mathfrak{a}$, and the map is injective.

What remains to be seen is the statement about the prime ideals, which follows since the principal idempotents in $\prod_i A_i/\mathfrak{a}_i$ are orthogonal and so when at least two of them that are non-trivial, the product $\prod_i A_i/\mathfrak{a}_i$ is not integral domain. ❑

2.70 It is appropriate to give a comment about the zero ring at this stage. In Proposition 1.27 the idempotents e_i's are not required to be different from zero, but if $e_i = 0$, of course $e_i A$ is the zero ring, and does not contribute in a significant way to the product (it holds true that $0 \times A = A$). This is particularly pertinent for the formulation of Proposition 2.69; it might happen that $\mathfrak{a}_i = A_i$ so that $A/\mathfrak{a}_i$ is the zero ring.

The Chinese remainder theorem

A classical result that at least goes back to third century AD is the so called Chinese Remainder Theorem, a more informative name would be the Theorem of Simultaneous Congruences: As long as the moduli n_1 and n_2 are relatively prime, two congruences $x \equiv y_1 \mod n_1$ and $x \equiv y_2 \mod n_2$ have a common solution. It seems that the first written account of this result is found in the book Sunzi Suanjing by a Chinese mathematician "Master Sun"— hence the Chinese theorem.



Some old Chinese mathematics.

This can of course be generalized to any number of congruences as long as the moduli are pairwise prime, and there is a formulation for general ring with the moduli replaced by ideals. To formulate the appropriate condition on the ideals, the notion of comaximal ideals is introduced. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *comaximal* is $\mathfrak{a} + \mathfrak{b} = A$, equivalently, one may write $1 = a + b$ with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

Comaximal ideals (*Komaksimale idealer*)

Given a finite collection $\{\mathfrak{a}_i\}_{1\leqslant i\leqslant r}$ ideals in the ring A. There is an obvious map

$$A \to \prod_i A/\mathfrak{a}_i$$

sending a ring-element a to the tuple whose i-th component is the residue class of a modulo $\mathfrak{a}_i$. Its kernel consists of the elements in A lying in all the

$\mathfrak{a}_i$'s, and hence there is induced an injective map

$$\psi\colon A/\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r \hookrightarrow \prod_i A/\mathfrak{a}_i.$$

The Chinese statement is that, under certain circumstances, this map is an isomorphism.

THEOREM 2.71 (THE CHINESE REMAINDER THEOREM) *Let A be a ring and let $\{\mathfrak{a}_i\}_{1\leqslant i\leqslant r}$ be a finite collection of pairwise comaximal ideals. Then $A/\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r \simeq \prod_{1\leqslant i\leqslant r} A/\mathfrak{a}_i$.*

PROOF: It suffices to find elements a_i in A which are congruent one modulo $\mathfrak{a}_i$ and congruent zero modulo all the other ideals in the collection. Indeed, the sum $\sum_i y_i a_i$, with the y_i's being arbitrary ring-elements, will then have the same residue class as y_i modulo $\mathfrak{a}_i$.

For each pair of indices i and j with $i \neq j$ we may write $1 = c_{ij} + c_{ji}$ with $c_{ij} \in \mathfrak{a}_j$. Then c_{ij} is congruent 1 modulo $\mathfrak{a}_i$ and congruent zero modulo $\mathfrak{a}_j$. Hence the product $a_i = \prod_{j\neq i} c_{ij}$ is congruent 1 modulo $\mathfrak{a}_i$ and congruent zero modulo $\mathfrak{a}_j$ for $j \neq i$; and we are done. ❑

Problems

2.32 Let $\mathfrak{a}$ and $\mathfrak{b}$ be two comaximal ideals such that $\mathfrak{a} \cap \mathfrak{b} = 0$. If $a + b = 1$ with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$, show that a and b are idempotents.

2.33 Show that $28y - 27z$ solves the simultaneous congruences $x \equiv y \mod 9$ and $x \equiv z \mod 4$.

2.34 Let A be a semi-local ring. Show that $A/J(A)$ is a product of fields. ✲

2.35 Assume that $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are pair-wise comaximal ideals. Show that one has $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_r = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r$.

★

2.8 Graded rings and homogenous ideals

Recall that any polynomial can be written as the sum of its homogenous components. Several techniques, useful when working with polynomials, involve this decomposition; just two mention two, induction on the degree of the lowest or the highest term are powerful tools. A class of rings sharing some of these properties are the so-called *graded rings* whose elements possess a decomposition mimicking the one of polynomials into homogeneous terms.

Even more forceful techniques are available to handle graded rings which satisfy appropriate finiteness conditions. For instance, when all the homogenous components R_n are finite dimensional vector spaces over some field $k \subseteq R_0$, the so called Hilbert function $h_R(\nu) = \dim_k R_n$ is a very strong invariant of R.

A the present stage of the course we merely scratch the surface of the theory of the graded rings, but they will reappear at several later occasions.

Graded rings (*graderte ringer*)

2.72 A *graded ring* R is a ring together with a decomposition of the underlying abelian group as a direct sum

$$R = \bigoplus_{\nu \in \mathbb{Z}} R_\nu \tag{2.5}$$

of additive subgroups R_ν subjected to the rule $R_\nu \cdot R_\mu \subseteq R_{\nu+\mu}$ for any pair of indices ν, μ.

Homogenous elements (*homogene elementer*)

2.73 Elements from the subgroup R_ν are said to be *homogenous of degree* ν. Notice that the zero element 0 lies in every one of the subgroups R_ν and one can not attribute a well-defined degree to it, but it will be considered to be homogenous of any degree. From a decomposition as in (2.5) it ensues that elements a in R can be expressed as sums $a = \sum_\nu a_\nu$ whose terms a_v are homogenous of degree ν with merely finitely many being different from zero. The a_ν's are uniquely determined by a and go under the name of the *homogenous components* of a.

Homogenous components (*homogene komponenter*)

Notice that $R_0 \cdot R_0 \subseteq R_0$, so R_0 is a subring of R. Similarly, for any ν it holds true that $R_0 \cdot R_\nu \subseteq R_\nu$, and the ring R_0 of elements homogenous of degree zero acts on the group of those homogenous of degree ν. In particular, if $k \subseteq R_0$ is a field, the additive subgroups R_ν will all be vector spaces over k.

Homogenous ideals (*homogene idealer*)

2.74 If $\mathfrak{a}$ is an ideal in the graded ring R, we denote by $\mathfrak{a}_\nu$ the subgroup $\mathfrak{a}_\nu = \mathfrak{a} \cap R_\nu$ consisting of the homogenous elements of degree ν that lie in $\mathfrak{a}$. One says that $\mathfrak{a}$ is a *homogenous ideal* whenever $\mathfrak{a} = \sum_\nu \mathfrak{a}_\nu$; in other words, whenever all the homogeneous components of elements from $\mathfrak{a}$ belong to $\mathfrak{a}$ as well. Since homogenous components are unambiguously defined (or if you prefer, because $\mathfrak{a}_\nu \cap \mathfrak{a}_\mu = (0)$ whenever $\nu \neq \mu$), the sum is a direct sum, and we are entitled to write $\mathfrak{a} = \bigoplus_\nu \mathfrak{a}_\nu$.

PROPOSITION 2.75 *Let $\mathfrak{a}$ be an ideal in the graded ring R. The following three statements are equivalent.*

- *The ideal $\mathfrak{a}$ is homogenous;*
- *All homogenous components of elements in $\mathfrak{a}$ belong to $\mathfrak{a}$;*
- *The ideal $\mathfrak{a}$ may be generated by homogenous elements.*

PROOF: That the first two statements are equivalent, is just a rephrasing of how homogenous ideals were defined. So assume that $\mathfrak{a}$ is a homogenous

ideal. The homogeneous components of any set of generators of $\mathfrak{a}$ then belong to $\mathfrak{a}$, and obviously they generate $\mathfrak{a}$ (the original generators are sums of them).

The other implication is also straightforward. Let $\{a_i\}_{i\in I}$ be a set of homogeneous generators for $\mathfrak{a}$, and say a_i is of degree d_i. Any element $a \in \mathfrak{a}$ can then be expressed as $f = \sum_i f_i \cdot a_i$ with $f_i \in R$, and expanding the sum into a sum of homogenous term we find

$$f = \sum_i f_i \cdot a_i = \sum_i \big(\sum_\nu f_{i,\nu} \cdot a_i\big) = \sum_d \big(\sum_{\nu+d_i=d} f_{i,\nu} \cdot a_i\big),$$

where $f_{i,\nu}$ denotes the homogeneous component of f_i of degree ν (most of these will vanish), and where we in the last sum have recollected all terms $f_{i,\nu} \cdot a_i$ of degree d. Hence $\sum_{\nu+d_i=d} f_{i,\nu} \cdot a_i$ is the homogeneous component of f of degree d, and it belongs to $\mathfrak{a}$ since the a_i's lie there. ❑

2.76 A rich source of graded rings are the quotients of polynomial rings by homogenous ideals, or more generally the quotient of any graded ring by a homogenous ideal.

PROPOSITION 2.77 *Let R be a graded ring and $\mathfrak{a} \subseteq R$ a homogeneous ideal. Then the quotient $R/\mathfrak{a}$ is a graded ring whose homogeneous components are given as $(R/\mathfrak{a})_\nu = R_\nu/\mathfrak{a}_\nu$.*

PROOF: This follows immediately from the the direct sum decompositions $R = \bigoplus_\nu R_\nu$ and $\mathfrak{a}_\nu = \bigoplus_\nu \mathfrak{a}_\nu$. Notice first $R_i \cap \mathfrak{a} = \mathfrak{a}_i$ and it holds that $R_i/\mathfrak{a}_i \subseteq R/\mathfrak{a}$. Hence any class $[a] \in R/\mathfrak{a}$ with a decomposing as $a = \sum_i a_i$ in homogeneous terms of degree i decomposes as $[a] = \sum_i [a_i]$, where we can consider the $[a_i]$'s to be elements in $R/\mathfrak{a}$ or in $\in R_i/\mathfrak{a}_i$. Moreover, the classes $[a_i]$ are unique because is $\sum_i a_i$ and $\sum_i b_i$ were two such decompositions inducing the same element in $R/\mathfrak{a}$, it would hold true that $\sum_i (a_i - b_i) \in \mathfrak{a}$. The ideal $\mathfrak{a}$ being homogeneous and each term $a_i - b_i$ being homogeneous of degree i, it would follow that $a_i - b_i \in \mathfrak{a}$, and hence $[a_i] = [b_i]$. ❑

EXAMPLE 2.22 *(A weighted grading)* There is a way of giving polynomial rings another grading than the traditional one, which sometimes turns out to be useful. We shall illustrate this in the case two variables $R = k[x, y]$. The idea is to give each variables x and y a *weight*, that is putting $\deg x = \alpha$ and $\deg y = \beta$ where α and β can be any pair of integers. The degree of the monomial $x^i y^j$ is then defined as $\deg x^i y^j = i\alpha + j\beta$. This defines a graded structure on the polynomial ring with

$$R_\nu = \bigoplus_{i\alpha+j\beta=\nu} k \cdot x^i y^j.$$

Since already R is the direct sum $R = \bigoplus_{i,j} k \cdot x^i y^j$, one arrives at the direct sum $R = \bigoplus_\nu R_\nu$ by just recollecting terms $k \cdot x^i x^j$ with the same degree. ☆

EXAMPLE 2.23 A natural and useful condition on a graded ring is that $R_n = (0)$ for $n < 0$; that is, the degrees of any non-zero element is non-negative (it opens up for induction arguments). However, several graded rings occurring naturally are not like that. One example is the subring R of $k(x_1, \ldots, x_n)$ consisting of rational functions shaped like f/g^ν where g is a fixed homogenous polynomial, and $f \in k[x_1, \ldots, x_n]$ and $\nu \in \mathbb{N}_0$. Putting $\deg f/g^\nu = \deg f - \nu \cdot \deg g$ makes R a graded ring (check that!), and then $\deg 1/g^\nu = -\nu \cdot \deg g$. ☆

Problems

2.36 Generalise Example 2.22 above to polynomials in any number of variables by giving each variable x_i a weight α_i.

2.37 With reference to the Example 2.22 above , show that the subring R_0 of elements of degree zero in the case $\alpha = 1, \beta = -1$ is isomorphic to the polynomial ring over k in one variable. Describe R_i for all i.

2.38 *(Monomial ideals.)* An ideal $\mathfrak{a}$ in the polynomial ring $k[x_1, \ldots, x_r]$ is said to be a *monomial* if it holds true that a polynomial f belongs to $\mathfrak{a}$ if and only if every monomial occurring in f lies there. Show that this is equivalent to $\mathfrak{a}$ being generated by monomials.

Monomial ideals (*Monomiale idealer*)

2.39 Assume that k is an infinite field. The multiplicative group k^* acts on the polynomial ring $k[x_1, \ldots, x_r]$ in a natural way, the result of $t \in k^*$ acting on $f(x_1, \ldots, x_r)$ being $f^t(x_1, \ldots, x_r) = f(tx_1, \ldots, tx_r)$. Show that the polynomial f is homogeneous of degree d if and only if $f^t = t^d \cdot f$ for all t. Show that an ideal $\mathfrak{a}$ is homogeneous if and only if $\mathfrak{a}$ is invariant under this action.

2.40 Assume that k is an algebraically closed field and that $f(x, y)$ is a homogeneous polynomial in $k[x, y]$. Show that $f(x, y)$ splits as a product of linear factors. HINT: If f is of degree d, it holds that $f(x, y) = y^d f(x/y, 1)$. Consider $f(x/y, 1)$ as a polynomial in $t = x/y$.

2.41 *(Homogenization of polynomials.)* Let k be a field and let $f \in k[x_1, \ldots, x_r]$ be any non-zero polynomial. Let d be the degree of f. Define a fresh polynomial $f^H \in k[x_0, \ldots, x_r]$ in one more variable by putting $f^H(x_0, \ldots, x_r) = x_0^d f(x_1/x_0, \ldots, x_r/x_0)$. Show that f^H is *homogenous* of degree d. Show that $f^H(1, x_1, \ldots, x_r) = f(x_1, \ldots, x_r)$.

Homogenization (*homogenisering*)

2.42 *(Dehomogenization of polynomials.)* The homogenization process described in the previous exercise has a natural reverse prossess called *dehomogenization* (with respect to one of the variables, x_0 in this exercise). When $g \in k[x_0, \ldots, x_r]$ is homogenous of degree d, one puts $g^D(x_1, \ldots, x_r) = g(1, x_1, \ldots, x_r)$. Show that $(g^D)^H = x_0^s g$ for some non-negative integer $s \leqslant d$. Give examples to see that s actually can have any value between 0 and s.

Dehomogenization (*dehomogenisering*)

2.43 Assume that $A = \bigoplus_{i\geqslant 0} A_i$ is a graded integral domain with A_0 being a field. Show that any element homogenous of degree one is irreducible.
HINT: Work with components of highest degree.

2.44 Let $A = \mathbb{Z}[x, y, z, w]/(xy - wz)$ show that the class of x is irreducible but not prime.

★

2.9 *The prime spectrum and the Zariski topology*

Prime spectrum of a ring (*Primspekteret til en ring*)

Every ring has a geometric incarnation, called the *prime spectrum* Spec A of the ring A whose points are the prime ideals in A. It carries a topology called the Zariski topology after Oscar Zariski, one of the great men of algebraic geometry. This topological space depends functorially on the A, a ring map $\phi\colon A \to B$ induces a map $\tilde{\phi}\colon$ Spec $B \to$ Spec A simply by sending a prime ϕ in B to the inverse image $\phi^{-1}(\mathfrak{p})$ (which is a prime ideal in A).

The spectra of rings enter as building blocks in Alexander Grothedieck's scheme theory , which is an infinitely larger ocean with as yet huge unexplored region, and the spectra form merely the shore.

In happy marriages the spouses exert a strong mutual influence, so also in the relationship between algebra and algebraic geometry. Several geometric features of Spec A are paramount to understanding algebraic properties of the ring A, and, of course, vice versa. Even modern number theory and arithmetic are inconceivable without the geometric language along with the geometric intuition. However, in these matters we shall only superficially scratch the surface; giveing the basic definitions and a few examples.

There is another geometric construct antecedent of the schemes by about a century. Basically it goes back to René Descartes's idea of using coordinates and equations to describe geometric objects. We have all experienced parts of the menagerie of plane curves and surfaces in the space. In general, subsets of $\mathbb{C}^r$ being the common zeros of a set of polynomials, are called *varieties* and are the subjects of interest for many algebraic geometers.

Varieties (*varieteter*)

Prime spectra

2.78 Being a geometric gadget, the prime spectrum is endowed with a topology which is called the *Zariski topology*. This topology is best defined by giving the closed subsets. These are denoted $V(\mathfrak{a})$ where $\mathfrak{a}$ is any ideal A, and given as the set of prime ideals containing $\mathfrak{a}$; that is, one has

The Zariski topology (*Zariski topologien*)

$$V(\mathfrak{a}) = \{\, \mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ a prime ideal } \mathfrak{p} \supseteq \mathfrak{a} \,\}.$$

There are some axioms to be verified. First of all, $V(0) = \text{Spec } A$ and $V(A) = \varnothing$, so the empty set and the entire space are both closed. Secondly, we must check that unions of finitely many closed subsets are closed (it suffices to check it for unions of two) and that the intersection of any family of closed sets is closed. To the former, observe that $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{ab})$ since both $\mathfrak{ab} \subseteq \mathfrak{a}$ and $\mathfrak{ab} \subseteq \mathfrak{b}$ hold, and the other inclusion $V(\mathfrak{ab}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$ follows since $\mathfrak{ab} \subseteq \mathfrak{p}$ implies that either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$ according to Proposition 2.24 on page 2.24 above. Hence $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$.

To the latter, notice the trivial fact that $\sum_i \mathfrak{a}_i$ lies in $\mathfrak{p}$ if and only if each of the $\mathfrak{a}_i$'s lies in $\mathfrak{p}$. We have shown

Oscar Zariski (1899–1986) Russian-born American mathematician

LEMMA 2.79 *Let A be a ring.*

- $V(0) = \text{Spec } A$ *and* $V(1) = \varnothing$
- *For any ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A it holds true that $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$;*
- *For any family $\{\mathfrak{a}_i\}_{i\in I}$ of ideals one has $V(\sum_{i\in I} \mathfrak{a}_i) = \bigcap_{i\in I} V(\mathfrak{a}_i)$;*
- *If $\mathfrak{a} \subseteq \mathfrak{b}$, then $V(\mathfrak{b}) \subseteq V(Fa)$*
- $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.

2.80 The Zariski topology has certain peculiar features never met when working with mundane topologies like the ones of manifolds. For instance, there are lots of points in Spec A that are not closed; so in particular the prime spectra tend to be seriously non-Hausdorff. One has:

LEMMA 2.81 *The closed points in* Spec A *are the maximal ideals.*

PROOF: We saw that every proper ideal is contained in a maximal ideal (Theorem 2.51 on page 2.51); hence $V(\mathfrak{a})$ will always have a maximal ideal as member. So if $\{\mathfrak{p}\}$ is closed; that is, equal to $V(\mathfrak{a})$ for some $\mathfrak{a}$, the prime ideal $\mathfrak{p}$ must be maximal.

On the other hand whenever $\mathfrak{m}$ is maximal, obviously $V(\mathfrak{m}) = \{\mathfrak{m}\}$ since no prime ideal strictly contains $\mathfrak{m}$. ❑

Examples

We do not intend to dive deeply into a study of prime spectra, but to give an idea of what can happen, let us figure out which of the topological spaces with only two points can be a prime spectrum.

There are three non-homeomorphic topologies on a two-point set; the discrete topology with all points being close (and hence all being open as well), the trivial topology whose sole closed sets are the empty set and the entire space, and finally the so-called Sierpiński space, a two-point space with just one of the points being closed (and consequently the other being open). And two of these occur as Zariski topologies.

2.24 The direct product of two fields $A = k \times k'$ has merely the two prime ideals $(0) \times k'$ and $k \times (0)$ which both are maximal. Hence Spec $k \times k'$ consists of two points and is equipped with the discrete topology.

2.25 The ring $\mathbb{Z}_{(p)}$ of rational numbers expressible as fractions with a denominator prime to p has just two prime ideals, namely (0) and the principal ideal (p) (Example 2.19 on page 45). Hence $\{(0)\}$ is an open set being the complement of the closed point (p). Hence Spec A is the Sierpiński space.

2.26 Finally, the trivial topology having no closed point, can not be the Zariski topology of any non-empty prime spectrum; in every ring different from the null-ring there are maximal ideals, and the spectrum of the null-ring is empty.

☆

2.82 The spectrum Spec A depends functorially on the ring A. If $\phi\colon A \to B$ is a map of rings, pulling back ideals along ϕ takes prime ideals to prime ideals; indeed, let $\mathfrak{p} \subseteq B$ be prime and assume that $ab \in \phi^{-1}(\mathfrak{p})$. This means that $\phi(a)\phi(b) \in \mathfrak{p}$, and so either $\phi(a) \in \mathfrak{p}$ or $\phi(b) \in \mathfrak{p}$. In other words, either a lies in $\in \phi^{-1}(\mathfrak{p})$ or b lies there. We thus obtain a map $\tilde{\phi}\colon$ Spec $B \to$ Spec A.

PROPOSITION 2.83 *The map $\tilde{\phi}$ is continuos.*

PROOF: Let $\mathfrak{a} \subseteq A$ be an ideal. The one has $\tilde{\phi}^{-1}V(\mathfrak{a}) = V(\mathfrak{a}B)$; indeed, tautologically it holds true that $\mathfrak{a} \subseteq \phi^{-1}\mathfrak{p}$ if and only if $\phi(\mathfrak{a}) \subseteq \mathfrak{p}$. ❑

A byproduct of the proof is that the inverse image under $\tilde{\phi}$ of the closed set $V(\mathfrak{a})$ is homeomorphic to Spec $B/\mathfrak{a}B$. Indeed, the prime ideals in $B/\mathfrak{a}B$ are in a one-to-one correspondence with the prime ideals in B containing $\mathfrak{a}B$ (Theorem 2.15 on page 29) , and these are, as we saw in the proof, precisely the points in Spec B mapping to points in $V(\mathfrak{a})$. Moreover, the whole lattice of ideals $\mathcal{I}(B/\mathfrak{a}B)$ is isomorphic to the lattice of ideals in B containing $\mathfrak{a}B$. That takes care of the topology; closed sets correspond to closed sets.

PROPOSITION 2.84 *Let $\tilde{\phi}\colon$ Spec $B \to$ Spec A be induced by $\phi\colon A \to B$. Then the inverse image $\tilde{\phi}^{-1}V(\mathfrak{a})$ is homeomorphic to* Spec $B/\mathfrak{a}B$. *In particular, for any point $\mathfrak{p} \in$ Spec A the fibre over $\mathfrak{p}$ equals* Spec $B/\mathfrak{p}B$.

2.85 The Zariski topology has a particular basis of open sets called the *distinguished open sets*. For each element $f \in A$ there is one such open set $D(f)$ whose members are the prime ideals not containing f; that is, $D(f) = \{\mathfrak{p} \mid f \notin \mathfrak{p}\}$. This is an open set since the complement is the closed set $V(f)$.

The distinguished open sets (*Særskilte åpne mengder*)

LEMMA 2.86 *The distinguished open sets form a basis for the topology on* Spec A.

PROOF: A typical open subset U is the complement of a set shaped like $V(\mathfrak{a})$. Now, a prime $\mathfrak{p}$ does not contain $\mathfrak{a}$ if and only if there is an element f lying in $\mathfrak{a}$ but not in $\mathfrak{p}$. Hence $U = \bigcup_{f \in \mathfrak{a}} D(f)$, and we are through. ❑

PROBLEM 2.45 Let A and B be two rings. Show that Spec $(A \times B)$ is the disjoint union of Spec A and Spec B. ★

PROBLEM 2.46 Show that $V(\sqrt{\mathfrak{a}}) = V(\mathfrak{a})$. ★

Complex Varieties

For any $S \subseteq \mathbb{C}[x_1, \ldots, x_r]$ of polynomials, the zero set $V(S)$ is defined as the set in $\mathbb{C}^r$ of simultaneous zeros of the polynomials in S; that is,

$$V(S) = \{\, x \in \mathbb{C}^r \mid f(x) = 0 \text{ for all } f \in S \,\}.$$

Curves in plane and surfaces in the space, as we know them fro earlier course are most often of this type with S just containing one element, the equation of the gadget under consideration. There is one difference however, we consider points with complex coordinates not only reals.

EXAMPLE 2.27 The good old parabola equals $V(y - x^2)$ in $\mathbb{C}^2$, or more precisely the old chap consists of the real points (those with both coordinates being real) of $V(y - x^2)$. ☆

2.87 One easily convinces oneself that the ideal $\mathfrak{a}$ generated by S has the same zero-set as S (sums of functions vanishing at point vanish there too, and even more, multiples of one vanishing vanishes), so without loss one may confine the study to sets shaped like $V(\mathfrak{a})$. One has the following formulas, where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathbb{C}[x_1, \ldots, x_r]$:

- If $\mathfrak{a} \subseteq \mathfrak{b}$ then $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$;
- $V(\mathfrak{a} + \mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b})$;
- $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$
- $V(\sqrt{\mathfrak{a}}) = V(\mathfrak{a})$
- $V((1)) = \varnothing$ and $V((0))) = \mathbb{C}^r$

We have seen that to any point in $\mathbb{C}^r$ there corresponds a maximal ideal $\mathfrak{m}_a$ in $\mathbb{C}[x_1, \ldots, x_r]$, namely the one whose members are the polynomials vanishing at a. It is generated by the linear polynomials $x_i - a_i$. There is a famous theorem of David Hilbert's called the Hilbert Nullstellensatz asserting, in one of its guises, that all maximal ideal in $C[x_1, \ldots, x_r]$ are of this shape. So anticipating that result we conclude that the points in $V(\mathfrak{a})$ are in natural one-one correspondence with the maximal ideals in $\mathbb{C}[x_1, \ldots, x_r]$ containing $\mathfrak{a}$; hence with the closed points in Spec $\mathbb{C}[x_1, \ldots, x_r]/\mathfrak{a}$.

History:
2018-08-21: Added examples 2.1, 2.2, 2.3 and 2.4. Corrected misprints and improved the language a few places.
23/08/2018 Added example 2.4;

24/08/2018 Corrected many misspellings in section 2.9

27/08/2018 Moved examples in paragraphs 2.8 and 2.9 to after quotients have been treated. Expanded paragraph 2.56. Added a small paragraph 2.25 about prime- and max- ideals in quotients.

30/08/2018 Expanded example 2.4. Added exercise 2.13.

06/09/2018 Corrected the definition of irreducible and prime elements. Added example 2.20;

07/09/2018 Have rewritten the section about principal ideals. Taken out the section abpout UFD's which has become a chapter of its own.

17/09/2018 Minor changes; discarded exercise 2.25

21/10/2018 Added Lemma 2.28 on page 33

26/10/2018 Have two more lemmas. Needed in chapter 8, but Their natural place is here

Lecture 3

Unique factorization domains I

Preliminary version 0.1 as of 2018-09-13 at 14:13 (typeset 3rd December 2018 at 10:03am)—Prone to misprints and errors and will change. 2018-09-13 Corrected proof of Prop 3.11.
13/09/2018 Added hypothesis that Rbe a doamain in Proposition 3.20.

When working with integers the Fundamental Theorem of Arithmetic is a most valuable tool used all the time. In general is does not hold and we have to do without it, and the birth of algebraic number theory and by that beginning of commutative algebra, came as a response to this "defect". However in certain nice rings the fundamental theorem persists, and these rings are called *unique factorization domains* or *factorial ring*, and out of the inherent human laziness comes the acronym UFD which is in widespread use.

Unique factorization domains (*Entydig faktoriseringsområder*)
Factorial rings
UFD's

3.1 *Unique factorization domains*

3.1 To be precise a UFD is a domain where every non-zero element which is not a unit, can be expressed in an essentially unique way as a product

$$a = p_1 \cdot \ldots \cdot p_r$$

of irreducible elements p_i. The qualifyer "essentially unique" must be understood in the large sense; the order of the factors can of course be changed at will, and replacing a factor p_i with up_i, where u is a unit, can be compensated by multiplying another factor by the inverse u^{-1}. So "essentially unique" means that the factors are unique up to order and multiplication by units.

In the definition there are two separate conditions which are of quite different flavour, and we shall take a closer look at each.

3.2 The first is the requirement that any element can be expressed as a finite product of irreducibles. This is in essence a finiteness condition on A and is fulfilled *e.g.* in Noetherian rings, but it does certainly not hold in general. An example can be the ring of entire functions in $\mathbb{C}$. The irreducibles in this ring are of the form $u(z)(z-a)$ where $u(z)$ is a unit (*i.e.* a non-vanishing entire function) and $a \in \mathbb{C}$ any point, so any entire function with infinitely many zeros—like our good old friend $\sin z$—can not be a finite product of irreducibles.

One can always attempt a recursive attack. Any ring element a which is not irreducible, is a product $a = a_1a_2$ of non-units. These being irreducible makes us happy, but if they are not, they are in their turn products $a_1 = a_{11}a_{12}$ and $a_2 = a_{21}a_{22}$. If some of the fresh factors are not irreducible, we split them into products of non-units. Continuing like this we establish a recursive process which, if it terminates, yields a finite factorization of a into irreducibles.

However, the process may go onfor every—like it will for *e.g.* $a = \sin z$—but in many cases there are limiting condition making it end. For instance, in the case of $\mathbb{Z}$, the number of steps is limited by the absolute value $\|a\|$, and in the case of polynomials in $k[x]$ by the degree of a.

3.3 The second condition is the uniqueness requirement which is much more of an algebraic nature, and hinges on the condition that irreducible elements be prime. In fact, in any ring the uniqueness condition holds automatically for finite factorizations into prime elements:

LEMMA 3.4 *Let A be a ring. Assume that $\{p_i\}_{1\leqslant i\leqslant r}$ and $\{q_i\}_{1\leqslant i\leqslant s}$ are two collection of prime elements from A whose products agree; that is it holds true that*

$$p_1 \cdots p_r = q_1 \cdots q_s.$$

Then the p_i's and the q_i's coincide up to order and unit factors.

PROOF: The proof goes by induction on r. Since p_1 is prime, it divides one of the q_i's, and after reordering the q_i's and adjusting q_1 by a unit, we may assume that $p_1 = q_1$. Cancelling p_1 gives $p_2 \cdots p_r = q_2 \cdots q_s$, and we finish the proof by induction. ❑

Since irreducibles are prime in $\mathbb{Z}$ and $k[x]$ (both are principal ideal domains), we immediately conclude that $\mathbb{Z}$ and $k[x]$ are factorial rings.

Examples

The main examples of factorial rings are principal ideal domains and polynomial rings over those, as we shortly shall see, and producing other examples demands some technology not available to us for the moment. So we confine ourselves to examples of non-factorial rings.

3.1 The classical example of a ring which is not factorial, which is ubiquitous in texts, is the ring $\mathbb{Z}[i\sqrt{5}]$. In it 6 has two distinct factorizations in irreducibles (see Example2.14 on page 37)

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

3.2 The standard example from algebraic geometry is the quotient ring[1] $A = k[X, Y, Z, W]/(XY - ZW)$. Indicating the class of a variable by a lowercase version of the name; the relation

$$xy = zw \tag{3.1}$$

[1] A geometer would call it "the cone over a quadratic surface in projective 3-space

holds in A. We saw in Example 3.5 on page 64 that A is a domain and its graded since the polynomial $XY - ZW$ is homogenous. It is not to challenging to see that the class of any non-zero linear form is irreducible in A (see Exercise 2.43 on page 52). Hence the relation (3.1) shows that A is not factorial.

This also gives an easy example of the intersection of two principal ideals being non-principal; *i.e.* distinct from their product, in that $(x) \cap (z) = (xy, xz)$.

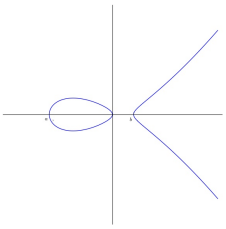


Figure 3.1: The real points of a cubic curve $y^2 = x(x-a)(x-b)$ with $a \neq b$ and $ab \neq 0$.

3.3 Another famous example from algebraic geometry can be $B = \mathbb{C}[X,Y]/(Y^2 - X(X-a)(X-a))$ where a and b are elements in $\mathbb{C}$. The relation

$$y^2 = x(x-a)(x-b),$$

where x and y denotes the classes of X and Y in B, prevails in B and gives two different decompositions of an element into irreducibles; of course one must verify that the involved linear factors are irreducible (see exercise xxx). Plane curves given by equations like

$$y^2 - x(x-a)(x-b)$$

with $a, b \in \mathbb{C}$ are called *elliptic curves* and have been at the centre-stage of algebraic geometry since its beginning. They are closely related to the so-called *elliptic functions*, and in fact, they were the very starting point for the development of algebraic geometry.

3.4 The polynomial $y^2 - x(x-a)(x-b)$ is irreducible in $k[x,y]$ for any field k. Indeed, if it were not, it would have a linear factor, and one could write

$$y^2 - x(x-a)(x-b) = (\alpha x + \beta y + \gamma)Q(x,y) \tag{3.2}$$

with α, β and γ constants from k and not both α and β being zero.

If $\beta \neq 0$, one may substitute $y = -\beta^{-1}(\alpha x + \gamma)$ into this equation. The right side then vanishes, and we obtain the polynomial identity

$$\beta^{-2}(\alpha x + \gamma)^2 - x(x-a)(x-b) = 0,$$

which is impossible since the left side is a monic cubic polynomial.

If $\beta = 0$, it holds true that $\alpha \neq 0$, and we may substitute $x = -\alpha^{-1}\gamma$ which makes the right side of (3.2) vanish. The leftside will then be a monic quadratic polynomial in y which is identically zero; absurd!

☆

Irreducibles in a UFD

3.5 As we saw (Proposition 2.38 on page 35), in a domain prime elements are always irreducible, but if the domain is factorial, the converse holds as well. Among domains with an appropriate finiteness condition—like the Noetherian domains we shall come to—this even characterises the factorial domains (Lemma 3.4 above).

PROPOSITION 3.6 *For members of a* UFD *being prime is equivalent to being irreducible.*

PROOF: Assume that a is irreducible, and that $a|xy$. Let $x = p_1 \cdots p_s$ and $y = q_1 \cdots q_t$ be decompositions into irreduicbles. Then of course

$$xy = p_1 \cdots p_s \cdot q_1 \cdots q_r$$

is a factorization into irreducibles as well. On the other hand, xy/a is an element in A and has a factorization $xy/a = r_1 \cdots r_m$ into irreducibles, so that

$$a \cdot r_1 \cdots r_m = p_1 \cdots p_s \cdot q_1 \cdots q_r$$

are two equal products of irreducibles. Irreducible factors coinciding up to order and units, this means that, up to a unit, a is either one of the p_i's or one of the q_i's, or phrased differently, a divides either x or y. ❑

Greatest common divisors and least common multiples

3.7 In a UFD any two elements have a *greatest common divisor*; that is an element d so that the principal ideal (d) is minimal among the principal ideals containing both principal ideals (a) and (b) where a and b are the two elements under consideration. Expressed in terms of divisibility, there is a d so that $d|a$ and $d|b$ and any other x dividing both a and b divides d; that is $x|a$ and $x|b$ implies that $x|d$. The greatest common divisor of a and b is not unique, but only determined up to an invertible factor; however the *principal ideal* (d) is unambiguously defined.

The greatest common divisor (*Største felles divisor*)

3.8 The two elements also have a *least common multiple*. This is an element m in A so that the principal ideal (m) is maximal among the principal ideals contained in (a) and (b); or phrased in terms of divisibility, it holds that $a|m$ and $b|m$, and for any other member x of A it ensues from $a|x$ and $b|x$ that $m|x$. Again, merely the principal ideal (m) is unambiguously defined.

The least common multiple (*Minste felles multiplum*)

PROPOSITION 3.9 *In a* UDF *any two elements have a greatest common divisor and a least common multiple.*

PROOF: Let a and b be the elements. Proceed to write down factorizations say $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$ into irreducibles, and pick up the "common factors": Reordering the factors, we find a non-negative integer t so that $(p_i) = (q_i)$ for $i \leqslant t$ and $(p_i) \neq (q_i)$ for $t > i$. Then $d = p_1 \cdots p_t$ is a greatest common divisor. It might of course happen that no (p_i) equals any (q_j), in which case $t = 0$, and the greatest common divisor equals one.

To lay hands on a least common multiple, make the product of all the ideals (p_i) and all the ideals (q_j) not found among the (p_i)'s. This product is a principal ideal, and any generator serves as a least common multiple. ❑

Kaplansky's criterion

3.10 I am especially found of the formulation[2] in the following criterion due to Irving Kaplansky whose proof is an elegant application of the Basic Existence Theorem.

[2] The slogan is: "A is a UFD if and only if every prime contains a prime".

PROPOSITION 3.11 *A domain A is a* UFD *if and only if every non-zero prime ideal contains a prime element.*

PROOF: The implication one way is clear. Let $\mathfrak{p}$ be a non-zero prime ideal and consider any of its non-zero elements. It factors as a product of primes, and one of the factors must lie in $\mathfrak{p}$.

To prove the other implication it suffices, in view of Lemma 3.4 on page 58, to show that any non-zero member of A is either a unit or a finite product of prime elements, so let Σ be the set of elements in A that can be expressed as a finite product of one or more prime elements. It is certainly multiplicative closed, and A having at least one maximal ideal it is not empty (maximal ideals are prime and contain prime elements by assumption). We contend that Σ coincides with the set of non-zero non-units of A.

Irving Kaplansky (19171–2006) Canadian mathematician

Assume this is not true; that is, there is a member x of A, neither zero nor a unit, that does not lie in Σ. Then $(x) \cap S = \varnothing$ since if $xy = p_1 \cdots p_r$ with the p_i's being prime elements and y not being a unit, it follows by an easy induction on r that x belongs to S. By the Basic Existence Theorem (Theorem 2.50 on page 40), there is a prime ideal in A maximal subjected to not meeting S and containing x. That prime ideal is not the zero ideal, and by assumption there is therefore a prime element lying in $\mathfrak{p}$, which is a contradiction since all primes lie in Σ. Hence Σ fills up the entire set of non-zero non-units in A. ❑

An immediate corollary is the following (which also can be proved in several other ways):

COROLLARY 3.12 *Every* PID *is a* UFD.

PROOF: Prime ideals are generated by prime elements. ❑

Gauss' lemma and polynomials over UDF*'s*

Every domain A is contained in a canonically determined field called the *fraction field* of A. The elements are fractions of shape a/b with a and b elements from A and, of course, $b \neq 0$. The arithmetic of these fractions is governed by the usual rules for rational fractions. For the moment we have not shown such field exist, but shall assume it. Later on they will be constructed as particular cases of a general "localization process".

Several of the domains we have seen are *a priori* contained in a field, like $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{d}]$ which are subrings of $\mathbb{C}$, and a polynomial ring $\mathbb{C}[x_1, \ldots, x_r]$

Johann Carl Friedrich Gauss
(1777–1855)
German mathematician

of over the complex numbers is contained in the rational function field $\mathbb{C}(x_1, \ldots, x_r)$. And these fields obviously have a fraction field *a priori*.

The objective of the current section is to establish the result that the polynomial rings over UFD's are UDF's. That result hinges on a key concept of a primitive polynomial and a key lemma, the so-called Gauss lemma. We begin with that before attacking the main assertion.

Primitive polynomials (*Primitive polynomer*)

3.13 For a moment image a polynomial $f(x) = a_0 + a_1 x + \ldots + a_r x^r$ with coefficient from the UDF A. Extracting the greatest common divisor d of the coefficient a_i one may write write $f = d \cdot g$ where $g \in A[x]$ is a polynomial whose coefficients are without a common divisor. This naturally leads to the concept of a primitive polynomial: A polynomial is called *primitive* if the greatest common divisor of the coefficients equals 1.

Content of a polynomial (*innehold*)

With a splitting $f(x) = c_f \cdot g(x)$ like above with g primitive and $c_f \in A$, it is widespread usage to call the element c_f the *content* of f. It is not unambiguously associated with f, but like a greatest common divisor, unique up to an invertible factor.

LEMMA 3.14 (GAUSS' LEMMA) *Assume that A is a UFD. Let f and g be primitive polynomials in $A[x]$. Then the product fg is primitive.*

It ensues immediately from the lemma that for any two polynomials f and g it holds true that $c_{fg} = uc_f c_g$ with $u \in A^*$; in other words, the content depends up to units on the polynomial in a multiplicative manner

PROOF: Write $f = \sum_{0 \leqslant i \leqslant n} a_i x^i$ and $g = \sum_{0 \leqslant i \leqslant m} b_i x^i$. Let d be a non-unit in A. The polynomial f being primitive, there is a least i_0 so that d does not divide a_{i_0} and ditto a least j_0 so that d does not divide b_{j_0}. Consider the coefficient of $x^{i_0+j_0}$ in the product fg; that is, the sum

$$\sum_{i+j=i_0+j_0} a_i b_j.$$

If $i \neq i_0$ and $j \neq j_0$, either $i < i_0$ or $j < j_0$; in the former case $d | a_i$ and in the latter $d | b_j$, so in both cases $d | a_i b_j$. Hence all terms of the sum are divisible by d except $a_{i_0} b_{j_0}$ and the sum is not divisible by d. ❑

3.15 So to our main objective

THEOREM 3.16 *If A is a UFD, then the polynomial ring $A[x]$ is a UFD. The irreducible elements in $A[x]$ are the irreducibles in A and the primitive, irreducible polynomials.*

Induction and the fact that $k[x]$ is a UFD immediately give the corollary that polynomial rings over fields are UFD's. Ot is also worth while mentioning that the same applies to polynomials rings over the integers.

COROLLARY 3.17 *If k is a field $k[x_1, \ldots, x_r]$ is a UFD.*

COROLLARY 3.18 *The ring $\mathbb{Z}[x_1, \ldots, x_r]$ are factorial.*

PROOF OF 3.16: We let K be the fraction field of A. Given a polynomial $p \in A[x]$ which we to begin with assume is primitive. It can be factored as $p = f_1 \cdots f_r$ with the f_i's being irreducible polynomials in $K[x]$. Multiplying through with an element from A on gets rid of the denominators of the coefficients of the f_i's and subsequently recollecting in one product the common divisors of the coefficients of each the f_i's, one arrives at a relation

$$a \cdot p = b \cdot g_1 \cdots g_r$$

where a and b are members of A and the g_i's are primitive polynomials in $A[x]$. By Gauss' lemma, the product $g_1 \cdots g_r$ is primitive, and since the content is unique up to a unit, it follows that $b = ua$ with $u \in A^*$. This takes care of the existence.

To the unicity, assume that $f_1 \cdots f_r = g_1 \cdots g_s$ in $A[x]$. Then $f_i = u_i g_i$ with $u_i \in K$, so clearing denominators we arrive at

$$a_i f_i = b_i g_i$$

hence $a_i = v_i b_i$ with $v_i \in A^*$ ❑

3.19 Factoring a polynomial into a product of irreducibles, or for that matter, showing a polynomial is irreducible, is often an unpleasant task. That the polynomial is homogenous might sometimes be helpful because then one knows *a priori* that the irreducible components are homogeneous; indeed, one has the following proposition.

PROPOSITION 3.20 *Let R be a graded factorial domain satisfying $R_n = 0$ for $n < 0$. Then the irreducible factors of a homogeneous element a are homogeneous.*

PROOF: Let a_i be the irreducible factors of a and develop each a_i as the sum $a_i = \sum_\nu a_{i,\nu}$ of the homogeneous components. Denote by a_{i,ν_i} the non-zero component of a_i of lowest degree. Since the degree of every element is non-negative, it holds true that

$$a = \prod_i a_i = \prod_i a_{i,\nu_i} + \text{ terms of higher degree,}$$

and $\prod_i a_i$ is non-zero as R is assumed to be a domain. But now, homogeneous components are unambiguously defined, and a is homogenous. Hence the sum of the high degree terms vanishes, and we have expressed a as a product of homogeneous elements

$$a = \prod_i a_{i,\nu_i}.$$

By induction on the degree, each a_{i,ν_i} has only homogeneous irreducible components, and the same applies therefore to a. ❑

EXAMPLE 3.5 The polynomial $f = xy - wz$ is irreducible. If f were the product of two linear terms, each variable would occur in precisely one of them since no term of f is a square, hence cross-terms like xw or xz would appear in f. ☆

EXAMPLE 3.6 The polynomial $y^p - x^q$ are irreducible when p and q are relatively prime. To see this give $k[x, y]$ the grading for which $\deg x = p$ and $\deg y = q$. An irreducible polynomial has both non-zero terms of the form $\alpha \cdot y^n$ and of the form $\beta \cdot x^m$, unless it equals x or y. If it additionally it is homogeneous, it holds true that $nq = mp$ and $n = ap$ and $m = bq$ for some natural numbers a and b. It follows that $y^p - x^q$ is irreducible since any irreducible factor is not reduced to x or y. ☆

âĂć

PROBLEM 3.1 Assume that $p(x)$ is a monic polynomial in $\mathbb{Z}[x]$ wich factors as $p(x) = r(x)s(x)$ in $\mathbb{Q}[x]$. Show that $r(x)$ and $s(x)$ both lie in $\mathbb{Z}[x]$ and are monic. HINT: multiply by the least common multiples of denominators of coefficents and appeal to Gauss's lemma. ★

PROBLEM 3.2 Let $d = 2k$ be an even integer and consider the ring $\mathbb{Z}[i\sqrt{2k}]$ with k an odd natural number. Show that $\mathfrak{p} = (2, i\sqrt{2k})$ is not a principal ideal but that $\mathfrak{p}^2 = (2)$. Prove that $\mathbb{Z}[i\sqrt{2k}]$ is not a UDF ✳ ★

PROBLEM 3.3 Consider the ring $\mathbb{Z}[i\sqrt{14}]$. Prove that ✳

$$3^4 = (5 + 2i\sqrt{14})(5 - 2i\sqrt{14})$$

and show that the involved elements all are irreducible elements of $\mathbb{Z}[i\sqrt{14}]$. ★

Lecture 4

Modules

Preliminary version 1.05 as of 2018-10-02 at 14:37 (typeset 3rd December 2018 at 10:03am)—To be completed. Prone to misprints and errors and will change.
2018-08-21: Rewritten paragraph 4.23 Proposition 4.26 corrected; added exercise 4.20
27/08/2018 Finished the paragraph 4.48 on page 87 about split exact sequences;
29/08/2018 Reworked section 4.5 about exact sequences.
15/09/2018 Reworked the snake section. Added exercise 4.15. Added examples 4.12, 4.13 and 4.14.
17/09/2018 Added example 4.18 exercises 4.25 and 4.26.
18/09/2018 Added example 4.24 on page 93; Added exercise 4.38 on page 95;
25/09/2018 Rewritten proof of Splitting Criterion, Prop 4.51; Corrected misprints; changed exercise 4.38 slightly. Added a new exercise 4.16.
26/09/2018 Added an exercise about elliptic curves and free modules, ex 4.27 on page 84. Added exercise 4.34 on page 89.
27/09/2018 Corrected several minors misprints.
Extended problem 4.34 about additive functors. Several minor improvements.
02/10/2018 Added exercise 4.5. Added example 4.17 Added a simple lemma snake-section (lemma 4.65).

Along with every ring comes a swarm of objects called modules; they are the additive groups on which the ring acts. The axioms for modules resemble the axioms for a vector spaces, and modules over fields are in fact just vector spaces. Over general rings however, they are much more diverse and seriously more complicated than vector spaces. Ideals for instance, are modules, and any over-ring is a module over any subring to mention two instances. An abelian group is nothing but a $\mathbb{Z}$-module and a module over the polynomial ring $k[t]$ over a field k is just a vector space over k endowed with an endomorphism; so the module theory encompasses all abelian groups and the entire linear algebra!

4.1 The axioms

4.1 A *module* M over the ring A, or an *A-module* as one also says, has two layers of structures. It is endowed with an underlying structure as an abelian group, which will be written additively, on top of which lies a linear action of the ring A. Such an action is specified by a map $A \times M \to M$, whose value at (a, m) will be denoted by $a \cdot m$ or simply by am. It is subjected to the following

Modules (*Moduler*)

four conditions:

- $a(m + m') = am + am'$;
- $(a + a')m = am + a'm$;
- $1 \cdot m = m$;
- $a \cdot (a' \cdot m) = (aa') \cdot m$.

where $a, a' \in A$ and $m, m' \in M$ are arbitrary elements. The first condition expresses that the action is A-linear; that is, the map $A \to \mathrm{Hom}_{\mathsf{Sets}}(M, M)$ sending a to the "multiplication-by-a-map" $m \mapsto am$ takes values in the ring $\mathrm{Hom}_{\mathsf{Ab}}(M, M)$ of group-homomorphism. The last three requirements express that this map is a ring homomorphism; in other words, it is the *ring* A that acts.

4.2 One recognizes these conditions from linear algebra; they are word for word the vector space axioms, the sole difference being that A is not required to be a field but can be any ring. In case A is a field k, there is nothing new; a k-module is just a vector space over k. One should not draw this analogy to far however, general modules are creatures that behave very differently than vector spaces.

Examples

4.1 The primordial examples of modules over a ring A are the ideals $\mathfrak{a}$ in A and the quotients $A/\mathfrak{a}$. Already here, the difference from the case of vector spaces surfaces; fields have no non-zero and proper ideals. There are also the "subquotients" $\mathfrak{b}/\mathfrak{a}$ of two nested ideals. Of course, these examples include the ring itself; every ring is a module over itself.

4.2 Another examples more in the flavour of vector spaces are the direct sums of copies of A. The underlying additive group is just the direct sum $A \oplus A \oplus \ldots \oplus A$ of a certain finite number, say r, copies of A. The elements are r-tuples $(a_1, \ldots, a_r)$, and addition is performed component-wise. The action of A is also defined component-wise: $a \cdot (a_1, \ldots, a_r) = (a \cdot a_1, \ldots, a \cdot a_r)$. We insist on this being an additive[1] construction and shall write rA for this module, not A^r as is common usage in linear algebra.

[1] The direct sum plays an additive role in the category of A-modules, the multiplicative role is taken by another construct, the tensor product. But that's for a later chapter.

4.3 Another familiar class of modules are the abelian groups. They are nothing but modules over the ring $\mathbb{Z}$ of integers. An integer n acts on an element from the module by just adding up the appropriate number of copies of the element and then correcting the sign.

4.4 Over-rings form an abundant source of examples—when A is a subring of B, multiplication by elements from A makes B into an A-module. So for

instance, $k[x,y]$ is a $k[x]$-module as is $k[x,x^{-1}]$. And $k[x]$ will be a module over the subring $k[x^2,x^3]$.

If m and n are two natural numbers the ring $\mathbb{Z}[\sqrt{m}/n]$ is a $\mathbb{Z}[\sqrt{m}]$-module (and, of course, it is a $\mathbb{Z}$-module, and also $\mathbb{Z}[1/n]$-module for that matter).

More generally, any ring homomorphism $\phi\colon A \to B$ induces an A-module structure on B through the action $a \cdot b = \phi(a)b$ of an element $a \in A$ on $b \in B$. One says that B is an *A-algebra*.

Algebras (Algebraer)

4.5 Suppose that k is a field. Giving a $k[t]$-module is the same as giving a k-vector space M and an endomorphism of M; that is, a linear map $\tau\colon M \to M$. A polynomial $p(t)$ in $k[t]$ acts on M as $p(t) \cdot m = p(\tau)(m)$.

☆

PROBLEM 4.1 Let A and B be two rings and assume that B has an A-module structure compatible with the ring structure; *i.e.* $a \cdot bb' = b(a \cdot b')$. Show that there is ring homomorphism $A \to B$ inducing the module structure. ★

✲

Homomorphisms between modules

A new concept in mathematics is always followed by a fresh class of relevant maps; so also in our present case of modules. An *A-module homomorphism* $\phi\colon M \to N$ between two A-modules M and N is a homomorphism of the underlying abelian groups that respects the action of A; that is, $\phi(am) = a\phi(m)$ for all a's in A and all m's in M. Simply said, a module homomorphism is just *an A-linear map* from M to N. With this notion of morphisms, the A-modules form a category Mod_A.

Module homomorphisms (Modulhomomorfier)

4.3 The set $\mathrm{Hom}_A(M,N)$ is naturally contained in the set $\mathrm{Hom}_{\mathbb{Z}}(M,N)$ of group homomorphism from M to N (which are just the additive maps) and consists of those commuting with the action of A on both M and N. It is well-known that the sum of two additive maps is additive (left for the zealous students to check), and when both commute with the actions of A, the sum does so as well. Therefore $\mathrm{Hom}_A(M,N)$ is an abelian group, and defining $a \cdot \phi$ as the map sending m to $a\phi(m)$ gives it an A-module structure. One must of course verify that $a \cdot \phi$ is A-linear, but this is easy: If $b \in A$ is another element, one finds

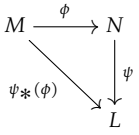
$$a \cdot \phi(bm) = a(b\phi(m)) = b(a\phi(m)),$$

where the first equality holds since ϕ is A-linear and the second because A is commutative[2].

[2] For non-commutative rings A the set $\mathrm{Hom}_A(M,N)$ is merely an abelian group in general. It does not carry an A-module structure unless further hypotheses are imposed on A.

4.4 The module $\mathrm{Hom}_A(M,N)$ depends functorially on both the variables M and N, and historically, it was one of the very first functors to be studied. The dependence on the first variable is contravariant—the direction of arrows are reversed— whereas the dependence on the second is covariant—directions

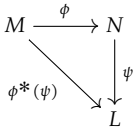
are kept. The induced maps are just given by composition. Of course, such constructions are feasible in all categories, what is special in Mod_A is that $\mathrm{Hom}_A(M,N)$ is an A-module and the induced maps are A-linear. The technical name is that category Mod_A has *internal homs*—the set of maps stay within the family!



To be presice let M, N and L be three A-modules and $\psi\colon N \to L$ an A-linear map. Sending ϕ to $\psi \circ \phi$ yields an associated map

$$\psi_*\colon \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,L).$$

It is A-linear, and if $\psi\colon L \to L'$ is another A-linear map, one has $(\psi' \circ \psi)_* = \psi'_* \circ \psi_*$.



In a similar fashion, the contravariant upper-star version

$$\phi^*\colon \mathrm{Hom}_A(N,L) \to \mathrm{Hom}_A(M,L),$$

which sends ψ to $\psi \circ \phi$, is A-linear as well, and it is functorial; *i.e.* $(\phi' \circ \phi)^* = \phi^* \circ \phi'^*$ for composable maps ϕ and ϕ'.

4.5 It follows readily from the involved maps being A-linear that the composition of composable maps is an A-bilinear operation. That is, one has

$$\phi \circ (a\psi + a'\psi') = a\phi \circ \psi + a'\phi \circ \psi' \text{ and } (a\phi + a'\phi') \circ \psi = a\phi \circ \psi + a'\phi' \circ \psi$$

where the maps are composable[3] and a and a' denote ring elements.

[3] That is, ϕ and ϕ' are maps from M to N and ψ and ψ' from N to L.

Problems

4.2 Show that there is a canonical isomorphism $\mathrm{Hom}_A(A,M) \simeq M$. ✳

4.3 Let A be an integral domain and $\mathfrak{a} \subseteq A$ a non-zero ideal. Show that $\mathrm{Hom}_A(A/\mathfrak{a}, A) = 0$. ✳

4.4 Let p and q be two prime numbers. Show that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) = 0$ if $p \neq q$, and that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$. ✳

4.5 Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in the ring A. Show that there is a canonical isomorphism $\mathrm{Hom}_A(A/\mathfrak{a}, A/\mathfrak{b}) \simeq (\mathfrak{a} : \mathfrak{b})/\mathfrak{b}$.

★

Submodules

4.6 A *submodule* N of an A-module M is a subgroup closed under the action of A; in other words, for arbitrary elements $a \in A$ and $n \in N$ it holds true that $an \in N$, and of course, N being a subgroup the sum and the difference of two elements from N belong to N.

Submodules (*Undermoduler*)

Examples

4.6 Ideals in the ring A are good examples of submodules, and by definition they constitute all submodules of A.

4.7 If $\mathfrak{a} \subseteq A$ is an ideal and M an A-module, the subset $\mathfrak{a}M$ of M formed by all multiples am with $a \in \mathfrak{a}$ and $m \in M$ is a submodule.

4.8 Given an ideal $\mathfrak{a}$ in A. The set $(0 : \mathfrak{a})_M$ of elements in M annihilated by all members of $\mathfrak{a}$ form a submodule. It holds true that $\mathrm{Hom}_A(A/\mathfrak{a}, M) = (0 : \mathfrak{a})_M$.

☆

The lattice of submodules

4.7 Just like the ideals in A the submodules of a given A-module M form a partially ordered set[4] denoted $\mathcal{I}(\mathcal{M})$ under inclusion.

The intersection $\bigcap_{i\in I} N_i$ of a collection $\{N_i\}_{i\in I}$ of submodules of M is a submodule. It is the largest submodule of M contained in all the submodules from the collection. In the similar way, the smallest submodule containing all the modules in the collection is the sum $\sum_{i\in I} N_i$ whose elements are finite A-linear combinations of elements from the N_i's; that is, elements shaped like

$$\sum a_i m_i, \tag{4.1}$$

where $m_i \in N_i$, and the a_i's are elements from A only finitely many of which are non-zero. More generally, for any set $S \subseteq M$ there is a smallest submodule of M containing S; it is called *the submodule generated* by S and consists of elements like in (4.1) but with the m_i's from S.

[4] The set $\mathcal{I}(M)$ forms what is called a *complete lattice*. A partially ordered set is called a *lattice* when every pair of elements possesses a least upper bound and a greatest lower bound, and it is said to be *complete* if the same is true for any subset. In our case the greatest lower bound is the intersection and the least upper bound the sum.

Submodules generated by elements (*Undermoduler generert av elementer*)

Kernels and images

4.8 An A-module homomorphism $\phi\colon M \to N$ is in particular a group homomorphism and as such has a kernel and an image. Both these subgroups are submodules as well; this ensues from the equality $a\phi(m) = \phi(am)$ satisfied by A-linear maps. Indeed, one immediately sees that the image is closed under multiplication by elements from A, and if $\phi(m) = 0$, it follows that $\phi(am) = a\phi(m) = 0$ as well.

PROBLEM 4.6 Let M and N be A-modules and $\phi\colon M \to N$ an A-linear map. Show that for every submodule $L \subseteq N$ the inverse image $\phi^{-1}(L)$ is a submodules of M. ★

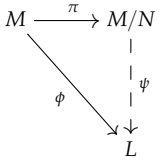
Quotients

4.9 Just as with ideals in a ring, one can form quotient of a module by a submodule.

Let M be the module and N the submodule. From the theory of abelian groups we already know that the two underlying additive groups have a quotient group M/N, which is formed by the cosets $[m] = m + N$. Endowing M/N with an A-module structure amounts to telling how elements $a \in A$ act on M/N, and one does this simply by putting $a \cdot [m] = [am]$. Of course, some verifications are needed. Routinely one checks that the class $[am]$ does not depend on the representative m, which is the case since $a(m + N) = am + aN = am + N$. Secondly, the module axioms in paragraph 4.1 must be verified; this is straightforward and left to the zealous students.

4.10 By definition the canonical map $\pi\colon M \to M/N$ that sends m to the class $[m]$ is A-linear, and characterized by the universal property that any A-linear map vanishing on N factors through it:

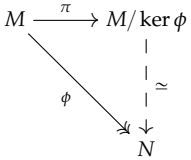
Proposition 4.11 (Universal propety of quotients) *Let N be a submodule of the A-module M. The quotient map $\pi\colon M \to M/N$ enjoys the following universal property. For every A-module homomorphism $\phi\colon M \to L$ with $N \subseteq \ker\phi$ there exists a unique A-linear map $\psi\colon M/N \to L$ so that $\phi = \psi \circ \pi$.*



Proof: The proof is *mutatis mutandis* the same as for (abelian) groups. The map ϕ is constant on the residue classes $[m] = m + N$, and $\psi([m])$ is defined as (and compelled to be) that constant value. Since ϕ is A-linear, the constant value on $[m + m'] = m + m' + N$ equals $\phi(m) + \phi(m')$, and on $[am] = am + N$ it is $a\phi(m)$. Hence ψ is A-linear. ❑

Corollary 4.12 (The first ismorphism theorem) *A surjective A-linear map $\phi\colon M \to N$ induces an isomorphism $M/\ker\phi \simeq N$.*

Proof: By the universal property ϕ factors through a map $\psi\colon M/\ker\phi \to N$. This is surjective since ϕ is, and injective since it kills the kernel. (That a class $[x]$ goes to zero, implies that $\phi(x) = 0$, hence $x \in \ker\phi$). ❑



One easily establishes the two following results. The analogue assertions for abelian groups are well known, and the proofs persist being valid for modules as well.

Proposition 4.13 *Let $\pi\colon M \to M/N$ be the quotient map. The "inverse-image-map" $\pi^{-1}\colon \mathcal{I}(M/N) \to \mathcal{I}(\mathcal{M})$ is a one-to-one correspondence between submodules of M containing N and submodules of M/N. It respect inclusions, arbitrary intersections and arbitrary sums.*

Proof: Routine. ❑

Proposition 4.14 (The second ismorphism theorem) *If N and N' are two submodules of M, there are canonical isomorphisms where in the second one assumes that $N' \subseteq N$:*

❑ $(N + N')/N' \simeq N/N \cap N'$;

❑ $(M/N')/(N/N') \simeq M/N$.

PROOF: Routine. ❑

4.15 In a famous paper Grothendieck introduced axiomatically the notion of an *abelian category*. The axioms reflect the main categorical properties of the module category Mod_A. Among the requirements is that all hom-sets be abelian groups and all compositions be bilinear (like we discussed in paragraph 4.4) and all maps have kernels and a cokernels. Moreover, there is an axiom which fabulously can be formulated as "the kernel of the cokernel equals the cokernel of the kernel".

Abelian category (*Abelske kategorier*)

Let us also mention that a category whose hom-sets are abelian groups and whose compositions are bilinear is called an *additive category*. When, as is true of Mod_A, the hom-sets are A-modules and the compositions A-bilinear, it is said to an *A-linear category*.

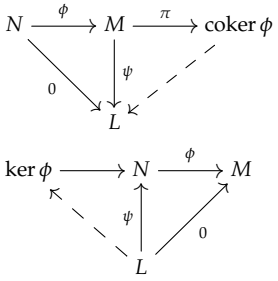
Additive categories (*Additive kategorier*)

A-linear category (*A-lineære kategorier*)

4.16 The definition of the *cokernel* in a categorical vernacular must be formulated exclusively in terms of arrows and therefore given as a universal property. The cokernel of an A-linear map $\phi\colon N \to M$ is an A-linear map $\pi\colon M \to \operatorname{coker}\phi$ such that $\pi \circ \phi = 0$, and which is universal with respect to that property. By The First Isomorphism Theorem (Theorem 4.12) the quotient $M/\operatorname{im}\phi$ fulfils that requirement, and hence serves as the cokernel of ϕ.

The cokernel (*Kokjernen*)

The two stablemates kernel and cokernel are from a categorical viewpoint dual concepts, and a definition of the kernel just in terms of arrows is indicated with a diagram in the margin.



PROPOSITION 4.17 *Every A-module homomorphism $\phi\colon M \to N$ has a kernel, an image and a cokernel.*

PROOF: As mentioned above, the quotient $N/\operatorname{im}\phi$ serves as the cokernel. The kernel is the usual tangible subset of M consisting of the elements sent to zero. ❑

EXAMPLE 4.9 In Mod_A the fabulous axiom cited above boils down to the obvious: The kernel of the cokernel and the cokernel of the kernel both equal the image. (If you find this rather cryptical than obvious, think twice!!) ☆

EXAMPLE 4.10 The submodules $\mathfrak{a}M$ where $\mathfrak{a}$ is an ideal in A form a particular important class of submodules of M. A quotient $M/\mathfrak{a}M$ inherits a natural structure of module over the quotient ring $A/\mathfrak{a}$; indeed, the product $x \cdot m$ between elements $x \in A$ and $m \in M/\mathfrak{a}M$ only depends on the residue class $[x]$ of x modulo $\mathfrak{a}$ since $(x + a)m = xm + am = xm$ for any $a \in \mathfrak{a}$.

So for instance, the module M itself is in a canonical way a module over $A/\operatorname{Ann} M$; or for that matter, over $A/\mathfrak{a}$ for any $\mathfrak{a}$ that kills M. ☆

EXAMPLE 4.11 Given a ring map $\phi\colon A \to B$ between two rings A and B. This allows one to consider any B-module M as an A-module just by letting members a of A act on elements $m \in M$ as $\phi(a) \cdot m$, and in this ways one obtains a natural functor from Mod_B to Mod_A. Sometimes one sees the notation M_ϕ or M_A for this module, but to avoid symbols looking like overdecorated Christmas trees, letting the A-module structure be tacitly understood and simply writing M is to prefer in most instances. ☆

4.2 *Direct sums and direct products*

There are two important and closely related constructions one can make in the category Mod_A of A-modules namely the direct product and the direct sum. There is no restriction on the cardinality of the involved families, but during practical work in algebraic geometry or number theory one mostly meets finite families, and in that case the two constructs agree.

Direct products

4.18 In this section we work with a collection $\{M_i\}_{i\in I}$ of modules over the ring A. From earlier courses direct product of a collection of groups is well known, and here we consider *the direct product* $\prod_{i\in I} M_i$ of the underlying additive groups of the M_i's. The elements are *strings* or *tuples* $(m_i)_{i\in I}$ indexed by the set I, and the addition is performed component-wise; *i.e.* $(m_i) + (m_i') = (m_i + m_i')$. In case I is finite, say $I = \{1, \dots, r\}$, an alternative notation for a tuple is $(m_1, \dots, m_r)$. The actions of A on the different M_i's induce an action on $\prod_{i\in I} M_i$, likewise defined component for component; a ring element a acts like $a \cdot (m_i) = (a \cdot m_i)$. The module axioms in paragraph (4.1) are cheap to verify, and we have an A-module structure on $\prod_{i\in I} M_i$.

Direct products of modules (*Direkte produkter av moduler*)

The projections $\pi_i\colon \prod_{i\in I} M_i \to M_i$ are A-linear since the module operations of the product are performed component-wise.

Direct sums

4.19 The *direct sum* of the module collection $\{M_i\}$ is denoted $\bigoplus_{i\in I} M_i$, and is defined as the submodule of the direct product consisting of strings $m = (m_i)_{i\in I}$ with all but a finite number of the m_i's vanishing—or so to say, there is an i_0 (that depends on m) such that $m_i = 0$ for $i \geqslant i_0$. Obviously this is a submodule, and again, the projections are A-linear.

Direct sums of modules (*Direkte summer av moduler*)

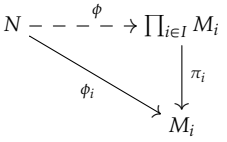
When the index set I is finite requiring strings to merely have finitely many non-zero components imposes no constraint, so in that case the direct sum and the direct product coincide. However, when the index set I is infinite, they are certainly not isomorphic; they are not even of the same cardinality. For instance, the direct sum of countably many copies of $\mathbb{Z}/2\mathbb{Z}$ is countable (being

the set of finite sequences of zeros and ones) whereas the direct product of countably many copies of $\mathbb{Z}/2\mathbb{Z}$ has the cardinality of the continuum (every real number has a 2-adic expansion).

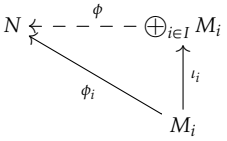
Universal properties

4.20 Both the product and the direct sum are characterised by *universal properties*. It is noticeable that these properties are dual to each other; reversing all arrows in one, yields the other. For this reason the direct sum is frequently called the *co-product* in the parlance of category theory.

We proceed to describe the two universal properties and begin with the direct product. In that case, the set-up is formed by an A-module N and a collection of A-linear maps $\phi_i\colon N \to M_i$. The conclusion is there exists a unique A-linear map $N\colon N \to \prod_{i\in I} M_i$ such that $\pi_i \circ \phi = \phi_i$. Indeed, this amounts to the map $\phi(n) = (\phi_i(n))_{i\in I}$ being A-linear.



In the case of the direct sum the universal property does not involve the projections, but rather the natural inclusions $\iota_j\colon M_j \to \bigoplus_{i\in I} M_i$ that send an $m \in M_j$ to the string having all entries equal to zero but the one in slot j which equals m. The given maps are maps $\phi_i\colon M_i \to N$, and the conclusion is that there exists a unique map $\bigoplus_{i\in I} M_i \to N$ so that $\phi \circ \iota_j = \phi_j$. The map ϕ is compelled to be defined as



$$\phi\big((m_i)_{i\in I}\big) = \sum_{i\in I} \phi_i(m_i),$$

and this is a legitimate definition since merely finitely many of the m_i's are non-zero.

PROBLEM 4.7 Work out all the details in the above reasoning. ★

4.21 With the stage rigged as in the previous paragraphs we round off the discussion of the universal properties of direct products and direct sums by offering equivalent formulations in terms of the hom-modules:

PROPOSITION 4.22 *There are canonical isomorphisms*

- $\mathrm{Hom}_A(\bigoplus_{i\in I} M_i, N) \simeq \prod_{i\in I} \mathrm{Hom}_A(M_i, N)$;
- $\mathrm{Hom}_A(N, \prod_{i\in I} M_i) \simeq \prod_{i\in I} \mathrm{Hom}_A(N, M_i)$.

Notice that in the first isomorphism, which involves the contravariant slot, the direct sum is transformed into a direct product. It further warrants a special comment that when the index set is finite, the direct product coincides with the direct sum, and the proposition may be summarized by saying that the hom-functor commutes with finite direct sums. In the vernacular of category theory one says that it is *additive* in both variables.

PROBLEM 4.8 Figure out the precise definitions of the isomorphisms in Proposition 4.22 above. HINT: The key word is universal properties. ★

4.23 We shall identify each module M_j with the image $\iota_j(M_j)$ in $\bigoplus_{i\in I} M_i$ under the natural inclusion ι_j; that is, with the submodule of elements having all entries zero except at slot j.

Fix one the indices say ν. Forgetting the ν-th entry in string $(m_i)_{i\in I}$ gives a string $(m_i)_{i\in I\setminus\{\nu\}}$ indexed by the subset $I\setminus\{\nu\}$ of indices different from ν. The operations in direct sums being performed component-wise, this is clearly an A-linear assignment; hence gives an A-linear map

$$\bigoplus_{i\in I} M_i \longrightarrow \bigoplus_{i\in I\setminus\{\nu\}} M_i$$

The kernel is obviously equal to M_ν (identified with the submodule of the direct sum wher merely the ν-th entry is non-zero), and the Isomorphism theorem (Theorem 4.12 on page 70) yields an isomorphism

$$\Big(\bigoplus_{i\in I} M_i\Big)/M_\nu \simeq \bigoplus_{i\in I\setminus\{\nu\}} M_i$$

The slogan is: Killing one addend of a direct sum yields the sum of the others.

PROBLEM 4.9 Generalize the slogan above to any sub-collection: Let $J \subseteq I$ be a subset. Prove that there is a canonical isomorphism

$$\bigoplus_{i\in I}(M_i)/\bigoplus_{j\in J} M_J \simeq \bigoplus_{i\in I\setminus J} M_i$$

★

Split submodules, direct sums and idempotent maps

It is of interest to have criteria for a submodule to be a direct summand of the surrounding module. We know every subvector space is a direct summand (bases can be extended to the containing space), but for general rings most submodules are not.

4.24 A synonym for a submodule $N \subseteq M$ to be a direct summand, is that N *lies split* in M—this of course means that there is another submodule N' so that $M = N \oplus N'$— and just as in linear algebra, the submodule N' is called a *complement* to N. Equivalently, every element m from M can be unambiguously expressed as a sum $m = n + n'$ with $n \in N$ and $n' \in N$; or phrased differently, the two conditions $N \cap N' = 0$ and $N + N' = M$ are satisfied.

Split submodules (*Splitt undermoduler*)

Complementary submodules (*Komplementære undermoduler*)

EXAMPLE 4.12 A principal ideal (n) i $\mathbb{Z}$, with n neither being zero nor plus-minus one, is not a direct summand of $\mathbb{Z}$ since every other ideal contains multiples of n. ☆

EXAMPLE 4.13 Cheap but omnipresent examples of non-split submodules are ideals $\mathfrak{a}$ in domains A. By paragraph 4.23 , any complement of $\mathfrak{a}$ would be isomorphic to $A/\mathfrak{a}$. If $\mathfrak{a}$ is a non-zero proper ideal, the quotient A/α contains non-zero elements killed by $\mathfrak{a}$ which is absurd since A was assumed to be a domain. ☆

EXAMPLE 4.14 A ring that is not a domain, may possess non-zero proper ideals lying split. The simples example is the direct product $A = k \times k$ of two fields. The subspaces $k \times (0)$ and $(0) \times k$ are both ideals. ☆

4.25 When we treated rings that were direct products of other rings, the notion of idempotent elements turned out to be quite useful. This notion can be generalizations in several directions and in various contexts, the virtue of idempotents always being that they express some kind of "direct decomposition". In our present context of modules over a ring A, an A-linear map $\epsilon\colon M \to M$ is said to be *idempotent* if $\epsilon^2 = \mathrm{id}_M$.

Idempotent map of modules (*Idempotent modulavbildning*)

PROPOSITION 4.26 *Let M be an A-module. If ϵ is an idempotent endomorphism of M, the map $M \to \ker\epsilon \oplus \operatorname{im}\epsilon$ sending m to $(m - \epsilon(m), \epsilon(m))$ is an isomorphism. A submodule N of M lies split if and only if there is an idempotent endomorphism $\epsilon\colon M \to M$ with $\operatorname{im}\epsilon = N$.*

PROOF: Suppose to begin with that ϵ is an idempotent endomorphism of M. We contend that $M = \operatorname{im}\epsilon \oplus \ker\epsilon$. Indeed, it holds true that $m = (m - \epsilon(m)) + \epsilon(m)$. Obviously $\epsilon(m)$ lies in $\operatorname{im}\epsilon$ and $m - \epsilon(m)$ lies in the kernel $\ker\epsilon$ because ϵ is idempotent:

$$\epsilon(m - \epsilon(m)) = \epsilon(m) - \epsilon^2(m) = \epsilon(m) - \epsilon(m) = 0.$$

On the other hand, $\operatorname{im}\epsilon \cap \ker\epsilon = 0$ since if $x = \epsilon(y)$ lies in $\ker\epsilon$, it holds that $\epsilon(x) = \epsilon^2(y) = \epsilon(y) = x$, and hence $x = 0$. This takes care of one implication.

Suppose then that $M = N \oplus N'$ and let $\pi\colon M \to N$ and $\iota\colon N \to M$ respectively be the projection and the inclusion map, then $\iota \circ \pi = \mathrm{id}_N$. Put $\epsilon = \pi \circ \iota$. Then

$$\epsilon^2 = (\iota \circ \pi) \circ (\iota \circ \pi) = \iota \circ (\pi \circ \iota) \circ \pi = \iota \circ \pi = \epsilon.$$

❑

Problems

4.10 Assume that for each $i \in I$ there is given a submodule $N_i \subseteq M_i$. Prove that $\bigoplus_{i\in I} N_i$ is a submodule of $\bigoplus_{i\in I} M_i$ in a natural way and that there is a natural isomorphism $\bigoplus_{i\in I} M_i/N_i \simeq (\bigoplus_{i\in I} M_i)/(\bigoplus_{i\in I} N_i)$.

4.11 Let M_1 and M_2 be two submodules of the A-module M whose intersection vanishes; that is, $M_1 \cap M_2 = (0)$. Prove that $M_1 + M_2$ is naturally isomorphic with the direct sum $M_1 \oplus M_2$. HINT: Establish that any $m \in M_1 + M_2$ can ✳

be expressed as $m = m_1 + m_2$ with m_1 and m_2 unambiguously defined elements in respectively M_1 and M_2.

4.12 Let $\{M_i\}_{i\in I}$ be a family of submodules of the A-module N. Assume that they comply to the following rule: For any index $\nu \in I$ and any finite subset $J \subseteq I$ not containing ν, the intersection of M_ν and $\sum_{j\in J} M_j$ vanishes; that is, $M_i \cap \sum_{i\in J} M_j = (0)$. Prove that $\sum_{i\in I} M_i$ is isomorphic with the direct sum $\bigoplus_{i\in I} M_i$.

4.13 Generalise Proposition 4.26 in the following way. Assume that $\epsilon_1, \ldots, \epsilon_r$ are mutually orthogonal idempotent endomorphisms of the A-module M. Suppose they satisfy $\sum \epsilon_i = 1$. Show that putting $M_i = \epsilon_i(M)$ one obtains a decomposition $M = \bigoplus_i M_i$. Prove the converse: If such a decomposition exists, exhibit a collection of idempotents inducing it.

4.14 Extend Proposition 4.27 to an arbitrary direct product $A = \prod_{i\in I} A_i$: Prove that any A module M is isomorphic to a product $\prod_{i\in I} M_i$ where M_i is an A_i-module unambiguously associated with M.

★

Modules over direct products

Consider a direct product $A = A_1 \times \ldots \times A_r$ of a collection $\{A_i\}_{1\leqslant i\leqslant r}$ of rings. We aim at describing all modules over A in terms of modules over the factors A_i. The crucial construction being the following. Suppose given an A-module M_i for each i. The additive group $\bigoplus_i M_i$ has a natural A-module structure and a string $a = (a_i)_{i\in I}$ of ring elements acts on a string $m = (m_i)_{i\in I}$ of module elements according to the rule $a \cdot m = (a_i \cdot m_i)$ (once more the axioms come for free the action being defined component-wise). We contend that all A-modules are shaped like this.

PROPOSITION 4.27 *Let $A_1, \ldots, A_r$ be rings and put $A = A_1 \times \ldots \times A_r$. Assume that M is an A-module. Then there are canonically defined submodules M_i of M that are A_i-modules and are such that $M \simeq \bigoplus_i M_i$.*

PROOF: Let $e_1, \ldots, e_r$ be the idempotents arising from the decomposition of A as a product; in other words they are the "basis elements" $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with the 1 located in slot i. Let $\mathfrak{a}_i$ be the kernel of the projection $A \to A_i$; that is, $\mathfrak{a}_i$ is the ideal generated by the idempotents e_j other than e_i. The set $M_i = e_i M$ is an A-submodule of M killed by $\mathfrak{a}_i$; hence it is an A_i-module. Since $\sum_i e_i = 1$, it follows that $M = \bigoplus_i M_i$. ❑

4.28 Let us take closer look at the case when A is a direct product of finitely many fields; say $A = k_1 \times \ldots \times k_r$. Then Proposition 4.27 above tells us that all modules over A are shaped like direct sums $V_1 \oplus \ldots \oplus V_r$ with each V_i a vector space over k_i.

Unions of submodules

There is no reason that the union of a collection of submodules in general should be a submodule; no more than the union of two lines through the origin in space is a plane! This an additive issue (unions of submodules are obvious closed under multiplication by ring elements) and takes place in most abelian groups: If H_1 and H_2 are two subgroups of an abelian group H, neither containing the other, their union cannot be a subgroup. Indeed, if x_1 lies in H_1 but not in H_2 and x_2 in H_2 but not in H_1, the sum $x_1 + x_2$ cannot belong to $H_1 \cup H_2$. Suppose for instance it belonged to H_1, then x_2 would lie there too which it was chosen not to.

4.29 However, there is one natural condition that ensures the union to be a submodule. One says that the collection is *directed* if for any two modules in the collection there is a third containing both; that is—if $\{M_i\}_{i\in I}$ is the collection—for any pair M_i and M_j there should be an index k so that $M_i \subseteq M_k$ and $M_j \subseteq M_k$. The union $\bigcup_{i\in I} M_i$ will then be closed under addition (and as multiplication poses no problem, will thence be a submodule); indeed, let x and y be two members of the union. This entails there are indices i and j so that $x \in M_i$ and $y \in M_j$, and the collection being directed, one may find an index k so that $M_i \cup M_j \subseteq M_k$. Both elements x and y then lies in M_k, and hence their sum does as well. So the sum belongs to the union. We have proven:

Directed collection of submodules (*Rettet samling av undermoduler*)

PROPOSITION 4.30 *Let $\{M_i\}_{i\in I}$ be a directed collection of submodules of the A-module M. Then the union $\bigcup_{i\in I} M_i$ is a submodule.*

4.3 *Finitely generated modules*

A particular class of modules are the finitely generated ones for which he theory is riche. But be aware that many modules arising for instance in algebraic geometry are not finitely generated.

4.31 A particularly class of modules are *the finitely generated modules* as the name indicates, they are modules M for which there is a finite set of elements that generate M. In other words, one may find elements $m_1, \ldots, m_r$ from M such that any $m \in M$ can be expressed as a linear combination $m = \sum_i a_i m_i$ with the a_i's being elements from A.

Finitely generated modules (*Endelig genererte moduler*)

EXAMPLE 4.15 Several important and natural modules are non finitely generated. One example can be the $\mathbb{Z}$-module $B = \mathbb{Z}[p^{-1}]$ where p is a natural number. For each non-negative integer i we consider the submodule $B_i = \mathbb{Z} \cdot p^{-i}$. Because $p^{-i} = p \cdot p^{-i-1}$, it holds true that $B_i \subseteq B_{i+1}$, and the B_i's form an ascending chain of submodules. Now, every element in B is of the form $a \cdot p^{-n}$ for some n, in other words one has $B = \bigcup_i B_i$. Any finite set of elements from B is contained in some B_N for N sufficiently large (just take N larger than all exponents of p appearing in the denominators), so if if finitely

many elements generate B it would hold true that $B_N = B$ for some N. This is obviously absurd, as p can appear in a denominator with any exponent. ☆

Cyclic modules

4.32 Modules requiring only a single generator are said to be *cyclic* or *monogenic*, and they are omnipresent. Among the ideals, the principal ideals are precisely the cyclic ones, and more generally, if M is any module and $m \in M$ an element[5], the submodule $Am = \{ a \cdot m \mid a \in A \}$ is cyclic.

Cyclic modules (*Sykliske moduler*)
Monogenic modules (*Monogene moduler*)

[5] The zero module is counted among the cyclic ones, so $m = 0$ is admitted.

Now, assume that M is a cyclic A-module and let $m \in M$ be a generator. Multiplication induces an A-linear map $\phi\colon A \to M$ that sends a to am, and this map is surjective since m was chosen as a generator. The kernel consists by definition of those a's that kill m, or which amounts to the same, that kill M. Hence $\ker\phi = \operatorname{Ann} M$, and by Corollary 4.12 on page 70, we arrive at an isomorphism $M \simeq A/\operatorname{Ann} M$.

LEMMA 4.33 *Every cyclic A-module M is isomorphic to $A/\operatorname{Ann} M$.*

So the cyclic modules are up to isomorphism precisely the quotient $A/\mathfrak{a}$ of A by an ideal $\mathfrak{a}$; notice that A itself is cyclic, corresponding to $\mathfrak{a} = 0$. The name cyclic is inherited from the theory of groups; the cyclic groups being those generated by a single element, in other words, those shaped like $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}$. The ideal $\mathfrak{a}$ is of course uniquely determined by the isomorphism class of M as an A-module (it equals the annihilator $\operatorname{Ann} M$ of M), but different ideals may give rise to quotient that are isomorphic as rings (but of course not as modules). For instance, the quotients $\mathbb{C}[x]/(x-a)$ with $a \in \mathbb{C}$ are all isomorphic to $\mathbb{C}$.

Simple modules

4.34 The simplest modules one can envisage are the ones without other submodules than the two all modules have, and they are simply called simple: A non-zero A-module M is said to be *simple* if it has no non-zero proper submodule. Simple modules are cyclic and any non-zero element generates; indeed, if $m \neq 0$, the submodule Am is non-zero (as m lies in it) and hence equals M since M has no proper non-zero submodules. Lemma 4.33 above gives that M is of the form $A/\operatorname{Ann} M$. Moreover, the annihilator ideal $\operatorname{Ann} M$ must be a maximal ideal since if $\operatorname{Ann} M \subseteq \mathfrak{a}$, the quotient $\mathfrak{a}/\operatorname{Ann} M$ is a submodule of M which either equals 0 or M. In the former case $\operatorname{Ann} M = \mathfrak{a}$, and in the latter it holds that $\mathfrak{a} = A$. Thus all simple A-modules are characterized:

Simple modules (*Simple moduler*)

PROPOSITION 4.35 *An A-module M is simple if and only if it is cyclic and its annihilator $\operatorname{Ann} M$ is a maximal ideal; i.e. M is simple if and only if M is isomorphic to $A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.*

Problems

4.15 Let N be a submodule of M. Show that if N and M/N both are finitely generated, then M is finitely generated as well. Give an example of modules M and N so that M and M/N are finitely generated but N is not. ⁂

4.16 Let N and L be submodules of the A-module M. If $N \cap L$ and $N + L$ are finitely generated, show that both N and L are finitely generated. ⁂

4.17 Show that $k[x, x^{-1}]$ is not a finitely generated module over $k[x]$. ⁂

4.18 Show that $k[x]/k[x^2, x^3]$ is a cyclic module over $k[x^2, x^3]$. What is the annihilator? What can you say about $k[x]/k[x^2, x^p]$ where p is an odd prime? ⁂

4.19 Assume that k is a field. Consider the polynomial ring $k[x]$ as a module over the subring $k[x^3, x^7]$. Prove it is finitely generated by exhibiting a set of generators. Determine the annihilator of the quotient $k[x]/k[x^3, x^5]$. ⁂

4.20 *(Schur's lemma.)* Assume that if M and N are two simple A-module that are not isomorphic. Prove that $\operatorname{Hom}_A(M, N) = 0$. Prove that $\operatorname{Hom}_A(M, M) = A/\operatorname{Ann} M$. ⁂

★

4.4 *Bases and free modules*

Just like for vector spaces one says that a set of generators $\{m_i\}_{i \in I}$ (not necessarily finite) is a *basis* for M if every element from M can be written as linear combination of the m_i's in only one way; that is, the coefficients a_i in an expression $m = \sum_i a_i m_i$ are unambiguously determined by m. But be aware that unlike what is the case for vector spaces, most modules do not have a basis.

Bases for modules (*Basis for en modul*)

EXAMPLE 4.16 The two elements x and y generate the ideal (x, y) in the polynomial ring $k[x, y]$, but do not form a basis since the element xy can be expressed as two different linear combinations, namely[6] one has $xy = x \cdot y = y \cdot x$. And of course, x and y form a minimal set of generators in the sense that one can not do without either, so even minimal generator sets are not necessarily bases. The natural question then arises: Can the ideal (x, y) be generated by one element? The answer is no! A generator would divide both x and y which is absurd.

[6] In the first expression x is the coefficient and y the generator, where as in the second it is the other way around; y is the coefficient and x the generator.

PROBLEM 4.21 Show that the property, familiar from the theory of vector spaces, that $\sum_i a_i m_i = 0$ implies that $a_i = 0$ is sufficient for a generating set $m_1, \ldots, m_r$ to be a basis. HINT: Consider the difference of two equal linear combinations of the m_i's. ★

The gist of this example is that x and y commute, and this indicates that the phenomenon is inherent in commutative rings. Any set of generators for an ideal consisting of at least two elements can never be a basis simply because the generators commute. ☆

Free modules

4.36 The lack of bases for most modules, leads to a special status of those that have one. One says that an A-module F is *free* if it has a basis. The reason behind the suggestive name "free" is that one may freely prescribe the values a linear map takes on the basis elements—a principle that goes under the name of the *Universal Mapping Principle*:

Free modules (*Fri moduler*)

Proposition 4.37 (The Universal Mapping Principle) *Suppose that F is a free A-module with a basis $\{f_i\}_{i\in I}$, and let M be another A-module. For any subset $\{m_i\}_{i\in I}$ of M indexed by I, there is a unique A-linear map $\phi\colon F \to M$ such that $\phi(f_i) = m_i$.*

Proof: Every element $x \in F$ is expressible as $x = \sum_{i\in I} a_i f_i$ with the coefficients a_i's from A, merely finitely many of which are non-zero, and most importantly, they are uniquely determined by x. Hence sending x to $\sum_{i\in I} a_i m_i$ gives a well defined map $\phi\colon F \to M$. We leave the task of checking it is A-linear to the zealous student. (This amounts to checking that the coefficients of a linear combination is the corresponding linear combination of the coefficients which ensues from the coefficients being uniquely determined.) ❑

4.38 We retrun to Example 4.16 about when ideals are free, and give a precise statement:

Proposition 4.39 *An ideal $\mathfrak{a}$ in the ring A is a free A-module if and only if it is principal and generated by a non-zero divisor.*

Proof: We saw in Example 4.16 above that when $\mathfrak{a}$ requires at least two generators, it has no basis and therefore is not free. Nor can principal ideals generated by a zero divisor be free since if $af = 0$ with $a \neq 0$, the relation $af = 0f$ gives two representations of 0. The other way around, if the non-zero divisor f is a generator for $\mathfrak{a}$, it is basis; indeed f being a non-zero divisor it can be cancelled from an equality like $af = bf$. ❑

4.40 Archetypes of free modules are the direct sums $nA = A \oplus \ldots \oplus A$ of n copies of the ring A which we already met in Example 4.2 on page 4.2. They come equipped with the so-called *standard basis* familiar from courses in linear algebra. The basis elements e_i are given as $e_i = (0, \ldots, 0, 1, 0, \ldots 0)$ with the one sitting in slot number i.

There is no reason to confine these considerations to direct sums of finitely many copies of A. For any set I, the direct sum $\bigoplus_{i\in I} A$ has a *standard basis*

$\{e_i\}_{i\in I}$ and is a free module; the basis element e_i is the string with a one in slot i and zeros everywhere else.

PROPOSITION 4.41 *Assume that F is a free A-module with basis $\{f_i\}_{i\in I}$. Then there is an isomorphism between F and the direct sum $\bigoplus_{i\in I} A$ that sends each basis vector f_i to the standard basis vector e_i.*

PROOF: By Proposition 4.37 above, we may define a map $\phi\colon F \to \bigoplus_{i\in I} A$ by sending f_i to the standard basis vector e_i; conversely, since $\bigoplus_{i\in I} A$ is free, sending e_i to f_i sets up a map $\psi\colon \bigoplus_{i\in I} A \to F$. These two maps are obviously mutual inverses. ❑

COROLLARY 4.42 *Any two bases of a free module have the same cardinality. Two free modules are isomorphic if and only if they possess bases of the same cardinality.*

Rank of a free module
(Rangen til en fri modul)

The common cardinality of the bases for a free module is called the *rank* of the module, and the rank is the sole invariant of free modules; up to isomorphism it determines the module. When the module is a vector space over a field and the rank is finite, the rank is just the dimension of the vector space.
PROOF: After Proposition 4.41 above we need merely to verify that when two direct sums $\bigoplus_{i\in I} A$ and $\bigoplus_{j\in J} A$ are isomorphic as A-module, the index sets I and J are of the same cardinality. This is well known from the theory of vector spaces when A is a field, so take any maximal ideal in A and consider the isomorphic vector spaces $\bigoplus_{i\in I} A/\mathfrak{m}$ and $\bigoplus_{j\in J} A/\mathfrak{m}$ over $A/\mathfrak{m}$ (isomorphic in view of exercise 4.10 on page 75). One has a basis of the same cardinality as I, the other one of cardinality that of J; hence I and J are equipotent. ❑

EXAMPLE 4.17 *(Free modules with given basis)* From time to time it will be convenient to operate with free A-modules with a given set S as basis. There is no constraint on the set S, it can be whatever one finds useful. The formal way to construct A^S is as the set of maps $\alpha\colon S \to A$ of finite support; that is the maps such that $\alpha(s) \neq 0$ for at most finitely many members s of S; in symbols

$$A^S = \{\, \alpha\colon S \to A \mid \alpha \text{ of finite support } \}.$$

The module structure of A^S is given point-wise: $(\alpha + \alpha')(s) = \alpha(s) + \alpha'(s)$ and $(a \cdot \alpha)(s) = a\alpha(s)$.

There is a collection of function termed generalized *Kronecker-δ's* that constitute a natural basis for A^S. These are in a one-to-one correspondence with the set S: There is one such function δ_s for each member $s \in S$ and it is defined as

$$\delta_s(t) = \begin{cases} 0 & \text{when } s \neq t \\ 1 & \text{when } t = s\,. \end{cases}$$

It is a trivial matter to verify they form a basis: They generate A^S because any α can be expressed as $\alpha = \sum_{s\in S} \alpha(s)\delta_s$, and if $\sum a_s\delta_s = 0$ is a dependence relation, one just plugs in any t from S to find that $a_t = 0$.

A suggestive way of denoting elements from the module A^S is as linear combinations $\sum_s a_s \cdot s$ of elements from S, which merely amounts to writing s for the function δ_s.

The module A^S depends functorially on S. Indeed, given any map $\phi\colon S \to S'$. Because the δ_s's form a basis for A^S, we obtain according to the Universal Mapping Principle for free modules, a map $\phi_*\colon A^S \to A^{S'}$ by sending each basis element δ_s to the element $\delta_{\phi(s)}$ of $A^{S'}$. In the alternative notation, the map ϕ_* takes the form $\phi_*(\sum_s a_s \cdot s) = \sum_s a_s \cdot \phi(s)$, and it is pretty obvious that $(\psi \circ \phi)_* = \psi_* \circ \phi_*$ when ψ is another map which is composable with ϕ. So, A^S is a covariant functor from the category Sets of sets to the category Mod_A of A-modules. ☆

PROBLEM 4.22 Let M be an A-module and let $F_M = A^M$ be the free module with elements from M as a basis. Then M is a quotient of F_M in a canonical way: Define a map $\theta_M\colon F_M \to M$ by sending δ_m to m (in the alternative notation it takes the hypertautological form $m \mapsto m$). Show that θ_M is surjective and that $\phi \circ \theta_M = \theta_N \circ \phi_*$ whenever $\phi\colon M \to N$ is an A-linear map. ★

$$\begin{array}{ccc} F_M & \xrightarrow{\phi_*} & F_N \\ {\scriptstyle\theta_M}\downarrow & & \downarrow{\scriptstyle\theta_N} \\ M & \xrightarrow[\phi]{} & N \end{array}$$

Matrices and maps of free modules

Just like linear maps between two vector spaces of finite dimension, A-linear maps between two *free* A-modules can be described by matrices, and the mechanism works exactly in the same way. Be aware however, that the task of describing maps between modules that are not free, is substantially more complicated, if a good description at all is accessible.

4.43 The representation of a map by a matrix depends on the choice of bases for each module. So let E and F two finitely generated and free A-module and let $\{e_j\}$ and $\{f_i\}$ be the two bases. When each $\phi(e_j)$ is expressed in terms of the basis $\{f_i\}$, the coefficients in the expressions make up the matrix. If E is of rank n and F of rank M the matrix is the $m \times n$-matrix given[7] as $M(\phi) = (a_{ij})_{ij}$ where $\phi(e_j) = \sum_i a_{ij} f_i$.

4.44 The familiar property that compositions of maps correspond to products of matrices still holds true, and the verification is *mutatis mutandis* the same as for linear maps between vector spaces (and we leave it to students needing to fresh up their knowledge of linear algebra); that is, if ψ is A-linear map from F to a third free module G, one has

$$M(\psi \circ \phi) = M(\psi) \cdot M(\phi).$$

Likewise, associating a matrix to a map persists being a linear operation in that

$$M(\alpha\phi + \beta\phi') = \alpha M(\phi) + \beta M(\phi'),$$

whenever $\phi'\colon E \to F$ is A-linear and α and β are two elements from the ring A.

[7] The notation $M^{\mathcal{E}}_{\mathcal{F}}(\phi)$ i cumbersome, but sometimes helpful. Then the rule for composition takes the form $M^{\mathcal{E}}_{\mathcal{F}}(\phi) \cdot M^{\mathcal{F}}_{\mathcal{G}}(\psi) = M^{\mathcal{E}}_{\mathcal{G}}(\phi \cdot \psi)$

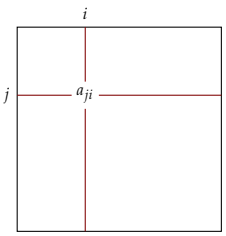
4.45 The all important construction of determinants of linear maps generalizes word for word to A-linear maps bewteen free modules, and all the basic properis of determinants continue to hold; like multiplicativity, alteration in rows and columns, expantions along rows or columns.

In particular, we would like to point out the formula

$$A \cdot A^\dagger = \det A \cdot I \tag{4.2}$$

valid for a square matrix A, where $A^\dagger$ is the so-called *cofactor-matrix* of A and I is the identity matrix. The ij-th entry of $A^\dagger$ is the sub-determinant of A with the j-th row and i-column struck out adjusted with the sign $(-1)^{i+j}$. The formula (4.2) follows from the rules for expanding a determinant along a row. Contrary to the case of vector spaces, it does not suffice that $\det A$ be non-zero for A to be invertible, the determinant must be invertible in A, but in that case it ensues from 4.2 that the inverse is given as

The cofactor-matrix (Kofaktormatrisen)



$$A^{-1} = (\det A)^{-1} \cdot A^\dagger.$$

4.46 Observer that an *endomorphism* ϕ of a free module E has a canonically defined determinant. Indeed, let M be a matrix for ϕ in some basis for E and M' in another. If N is the base-change matrix, it holds true that $M' = NMN^{-1}$ and consequently

$$\det M' = \det N \cdot \det M \cdot \det N^{-1} = \det M.$$

This makes $\det \phi = \det M$ a legitimate definition as the determinant $\det M$ of ϕ does not depend on which basis is used.

This allows the definition of *the characterstic polynomial* of an endomorphism ϕ of a free module E of finite rank, namely as $P_\phi(t) = \det(t \cdot \mathrm{id}_E - \phi)$. It is an element of the polynomial ring $A[t]$.

The characterstic polynomial of an endomorphism (Det karakteristiske polynomet til en endomorfi)

Ours is a pedestrian approach to determinants—there is also a Formula 1 way based on so-called exterior powers. It has the disadvantage of requiring more advanced machinery and being rather opaque for beginners, but has the great advantage of being completely functorial. It also open up for defining determinants of endomorphisms of a wider class of modules than the free ones.

EXAMPLE 4.18 *(The norm)* An indispensable tool in algebtaic number theory is the norm. We have already come across it at occations, *e.g.* when showing that 2 and 3 were irreducible eements in $\mathbb{Z}[i\sqrt{5}]$, butin the guise of the ordinary absolute value of compelx numbers.

The setting is as follows. We are given an algebra B over a ring A which is free of finite rank n as A-module. Every element b in B defines an A-linear "multiplication-by-b" map[8] $[b]\colon B \to B$ that sends x to $b \cdot x$. Its determinant $\det[b]$ is called the *norm* of b and denoted $N_{B/A}(b)$. Clearly $[bb'] = [b] \circ [b']$

[8] Not to be confused with the residue class notation.

The norm of an element (Normen til et element)

and the determinant of a composition being equal to the product of the determinants, we infer that $N_{B/A}(bb') = N_{B/A}(b)N_{B/A}(b')$. The norm is therefore a *multiplicative* functions on B with values in A. Moreover, for elements $a \in A$ one has $N_{B/A}(a) = a^n$. This follows because the map $[a]$ is just $a \cdot \mathrm{id}_B$ and $\det(a \cdot \mathrm{id}_B) = a^n$ (the map $[a]$ is represented as a scalar matrix in any basis). ☆

Problems

4.23 Prove that any finitely generated A-module is the quotient of a free module of finite rank. ⁎

4.24 Show that any A-module is the quotient of a free module. HINT: let $F_M = \bigoplus_{m\in M} A$ be the direct sum of copies of A, one for each element $m \in M$. ⁎

4.25 Let $A = \mathbb{Z}[\sqrt{d}]$. Show that A is a free $\mathbb{Z}$-module with basis $1, \sqrt{d}$. Use this to show that $N_{A/\mathbb{Z}}(x + y\sqrt{d}) = x^2 - dy^2$. ⁎

4.26 Assume that d is an innteger such $d \equiv 1 \mod 4$. Let $\alpha = (1 + \sqrt{d})/2$. Show that $\alpha^2 = \alpha + (d-1)/4$. Prove that $A = \mathbb{Z}[\alpha]$ is free $\mathbb{Z}$-module of rank 2 with $1, \alpha$ as a basis. Determine the matrix of the map $x \mapsto \alpha x$ in this basis and compute the characteristic polynomial. ⁎

4.27 Let $A = k[X, Y]/(Y^2 - X(X-a)(X-b))$ be the coordinate ring of an elliptic curve and as usual let x be the class of X and y that of Y. ⁎

a) Show that $k[x]$ is isomorphic with the polynomial ring $k[X]$ and that A is a free $k[x]$-module of rank 2.

b) Show that $k[y]$ is isomorphic to the polynomial ring $k[Y]$ and that A is a free $k[y]$ module of rank 3.

c) Show that x and y are irreducible elements in A and conclude that A is not a UDF. ★

The next series of exercises, which culiminate with problem 4.30, are aimed at giving an example that countable products of free modules are not neceras-saryli free

4.28 Show that in a free $\mathbb{Z}$-module every element is divisible by at most finitely many integers.

4.29 Show that the direct sum of countably many copies of $\mathbb{Z}$ is countable, whereas the direct product of countably many copies is not (it has the cardinality of the continuum).

4.30 *(Infinite products are not always free.)* The task is to show that the direct product $P = \prod_{i\in\mathbb{N}} \mathbb{Z}$ of a countable number of copies of $\mathbb{Z}$ is not a free $\mathbb{Z}$-module. Aiming for a contradiction, suppose that the product has a basis $\{f_i\}_{i\in I}$. The direct sum $Q = \bigoplus_{i\in\mathbb{N}} \mathbb{Z}$ lies in P and has the standard basis

elements e_i (with a one in slot i as sole non-zero component). Each e_i can be developed as $e_i = \sum_j a_{ij} f_j$ with $a_{ij} \in \mathbb{Z}$ in terms of the basis elements f_j.

a) Prove that I cannot be countable.

b) Prove that there is a countable subset $J \subseteq I$ so that the module Q generated by the f_j's with $j \in J$ contains the direct sum $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}$. HINT: Let j be in J when the coefficient $a_{ij} \neq 0$ for at least one i.

c) For any element $x = (n_1, n_2, \ldots)$ in P and any $i \in \mathbb{N}$ prove that the element $y = (0, 0, \ldots, 0, n_i, n_{i+1}, \ldots)$ has the same image in P/Q as x.

d) Show that there are strictly increasing sequences $\{n_k\}$ of natural numbers with $n_k | n_{k+1}$ and so that $a = (n_1, n_2, \ldots)$ does not lie in Q. HINT: Q is countable.

e) Show that the image of a in P/Q is divisible by infinitely many numbers and hence P/Q cannot be free.

★

4.5 *Exact sequences*

Let ϕ and ϕ be two composable A-linear maps and write them they down in a sequence

$$M \xrightarrow{\phi} N \xrightarrow{\psi} L.$$

Exact sequences (*Eksakte følger*)

This sequence is said two be *exact* if $\ker \psi = \operatorname{im} \psi$. It frequently happens that such a sequence is part of a longer sequence of maps, extending to the left or to the right, and then the extended sequence is said to be *exact at* N as well. A sequence exact at all places, is simply said to be *exact*.

4.47 Two special cases warrant mentioning; the first being when $M = 0$:

$$0 \longrightarrow N \xrightarrow{\psi} L.$$

The image of the zero map being the zero submodule (0), exactness boils down in this case to ψ being injective. Similarily, when $L = 0$, the sequence is shaped like

$$M \xrightarrow{\phi} N \xrightarrow{\psi} 0,$$

and it being exact is equivalent to ϕ being surjective.

EXAMPLE 4.19 Any map $\alpha \colon M' \to M$ lives in the exact sequnece

$$0 \longrightarrow \ker \alpha \longrightarrow M' \longrightarrow M \longrightarrow \operatorname{coker} \alpha \longrightarrow 0.$$

☆

Short exact sequences

By far the most often met exact sequences, are the so-called short exact sequences; and they are a valuable tool when one tries to study a module by breaking it down into smaller (and presumptive simpler) pieces.

4.48 A three-term sequence (or a five-term sequence if you count the zeros)

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0 \tag{4.3}$$

is called a *short exact sequence* when it is exact. This means that α is injective, that β surjective and that $\operatorname{im}\alpha = \ker\beta$. Of course, the term "short" in the name implies there are long exact sequence as well, and indeed there are, as we shall see later on.

Short exact sequence (*Korteksakte følger*)

It ensues from the First Isomorphism Theorem (Corollary 4.12 on page 70) that there is a unique isomorphism $\theta\colon M'' \simeq M/\alpha(M')$ shaped in a way that β corresponds to the quotient map. In other words, θ enters in the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha|_{M'}} & & \| & & \downarrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & \alpha(M') & \longrightarrow & M & \longrightarrow & M/\alpha(M') & \longrightarrow & 0 \end{array} \tag{4.4}$$

where the maps in the bottom row are respectively the inclusion of $\operatorname{im} M'$ into M and the quotient map. In short, up to isomorphisms all short exact sequence appear as

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0,$$

where $N \subseteq M$ is a submodule, and the two maps are respectively the inclusion and the quotient map.

Example 4.20 *(Direct sums)* The direct sum $M \oplus N$ of two A-modules fits naturally into the short exact sequence

$$0 \longrightarrow N \longrightarrow N \oplus M \longrightarrow M \longrightarrow 0$$

where the left-hand map is the natural inclusion sending x to $(x, 0)$ and the one to the right is the projection onto M, which maps (x, y) to y. If N and N' are two submodules of the A-module M, then there is a short exact sequence

$$0 \longrightarrow N \cap N' \xrightarrow{\iota} N \oplus N' \xrightarrow{\sigma} N + N' \longrightarrow 0$$

where ι is the inclusion map and $\sigma(x, y) = x - y$. ☆

Example 4.21 *(A Chinese squence)* The Chinese remainder theorem (Theo-

rem 2.71 on page 48) for two ideals may be generalized by saying that the sequence

$$0 \longrightarrow \mathfrak{a} \cap \mathfrak{b} \longrightarrow A \longrightarrow A/\mathfrak{a} \oplus A/\mathfrak{b}\mathfrak{b} \longrightarrow A/\mathfrak{a} + \mathfrak{b} \longrightarrow 0, \tag{4.5}$$

where the two maps in the middle are given by the following two assignments $x \mapsto ([x]_{\mathfrak{a}}, [x]_{\mathfrak{b}})$ and $([x]_{\mathfrak{a}}, [y]_{\mathfrak{b}}) \mapsto [x]_{\mathfrak{a}+\mathfrak{b}} - [y]_{\mathfrak{a}+\mathfrak{b}}$. Having four non-zero terms it is to long to be called short exact, but it may be obtained by splicing the two short exact sequences

$$0 \longrightarrow \mathfrak{a} \cap \mathfrak{b} \longrightarrow A \longrightarrow A/\mathfrak{a} \cap \mathfrak{b} \longrightarrow 0$$

and

$$0 \longrightarrow A/\mathfrak{a} \cap \mathfrak{b} \longrightarrow A/\mathfrak{a} \oplus A/\mathfrak{b} \longrightarrow A/\mathfrak{a} + \mathfrak{b} \longrightarrow 0$$

☆

Problem 4.31 Verify that the two maps defined in the example above are well defined and that the sequence is exact. Deduce the Chinese Remainder Theorem from it. ★

Problem 4.32 Write down a "Chinese sequence" involving three ideals that generalizes the sequence (4.5) above. Prove it is exact and deduce the Chinese Remainder Theorem for three ideals from it. Hint: It will have six non-zero terms. ★

Split exact sequences

Some short exact sequence stand out from all the crowd, to wit, the so-called split exact sequences. A short exact sequence

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0. \tag{4.6}$$

Split exact sequences (*Splitteksakte følger*)

is *split exact* when being isomorphic to the standard sequence of Example 4.20 on page 86. This not only requires that M be isomorphic to the direct sum $M' \oplus M''$, but the somehow stronger requirement that there be an isomorphism inducing the identity on M' and pairing β with the projection, must be met: that is, the isomorphism must fit into the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \longrightarrow & 0 \\ & & \| & & \downarrow\simeq & & \| & & \\ 0 & \longrightarrow & M' & \longrightarrow & M' \oplus M'' & \longrightarrow & M'' & \longrightarrow & 0. \end{array}$$

where the maps in the bottom sequence are the projection and the inclusion.

4.49 Of course all sequences are not split exact, and even if the two extreme modules are the same the middle modules need not be isomorphic. The

easiest example is found among abelian group: Both $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ appear in the midst of short exact sequences with both extreme modules being $\mathbb{Z}/p\mathbb{Z}$. In general, it is an unsurmountable challenge to classify all possible middle modules given the two extreme ones.

4.50 There is nice criterion for a short exact sequence to be split involving only one of the maps α or β; to formulate it we need two new concepts. A *right section* for β is an A-linear map $\sigma\colon N \to M$ such that $\beta \circ \sigma = \mathrm{id}_N$, and a *left section* for α is one $\tau\colon M \to M'$ with the property that $\tau \circ \alpha = \mathrm{id}_{M'}$.

Right sections (*Høyresek-sjoner*)

Left sections (*Venstresek-sjoner*)

PROPOSITION 4.51 (SPLITTING CRITERION) *Let the short exact sequence*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

of A-modules be given. Then the following three statements are equivalent

- *The sequence is split;*
- *The map α has a left section;*
- *The map β has a right section.*

Before starting with the proof we observe that a map $\beta\colon M \to M''$ that possesses a right section σ is automatically surjective since if $x \in M''$ it holds true that $\beta(\sigma(x)) = x$. Thus, once the map β has a right section its source M will be isomorphic to $M'' \oplus \ker\beta$. Moreover, the restriction of β to the image $\sigma(M'')$ is easily seen to be an isomorphism so that M is the direct sum of the two submodules $\ker\beta$ and $\sigma(M'')$.

PROOF: We start out by assuming that the sequence is split and that $\theta\colon M \to M' \oplus M''$ is an isomorphism of the right type. Then one easily verifies that the maps given by $m'' \mapsto \theta^{-1}(0, m'')$ and $m' \mapsto \theta^{-1}(m', 0)$ are sections for respectively β and α of the right variance and hence the first assertion implies each of the two others.

Assume then that the map β has a right section σ and define a map $\Phi\colon M' \oplus M'' \to M$ simply by the assignment $(x, y) \mapsto \alpha(x) + \sigma(y)$. This map is clearly A-linear and it lives in the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \longrightarrow & 0 \\
 & & \| & & \uparrow{\scriptstyle \Phi} & & \| & & \\
0 & \longrightarrow & M' & \xrightarrow[\iota]{} & M' \oplus M'' & \xrightarrow[\pi]{} & M'' & \longrightarrow & 0
\end{array}$$

whose rows are exact, and where ι and π are respectively the canonical inclusion and projection. The left square commutes since $\Phi(\iota(x)) = \alpha(x) + \sigma(0) = \alpha(x)$, and that the right does, ensues from the following little calulation

$$\beta(\Phi(x, y)) = \beta(\alpha(x) + \sigma(y)) = \beta(\sigma(y)) = y = \pi(x, y).$$

where we use that σ is a right section for β. Now, there is a general fact (called THE FIVE LEMMA, see Exercise **??** on page **??** below) that a map in the midst of two isomorphisms as in the diagram above is an isomorphism; but it is also easily checked *ad hoc*: If $0 = \Phi(x,y) = \alpha(x) + \sigma(y)$, it follows that $y = 0$ since the right square above is commutative, hence $\alpha(x) = 0$, and consequently $x = 0$ because α is injective. To prove surjectivity of Φ, observe that for $z \in M$, the difference $z - \sigma(\beta(z))$ is killed by β, and because $\ker\beta = \operatorname{im}\alpha$, one has $z - \sigma(\beta(z)) = \alpha(y)$ for some y so that $z = \alpha(y) + \sigma(\phi(z))$.

Finally, let us treat the case that α has a left section. The map $\Psi\colon M \to M' \oplus M''$ defined by $\Psi(z) = (\tau(z), \beta(z))$ fits in the following diagram analogue to the one above

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle\Psi} & & \| & & \\ 0 & \longrightarrow & M' & \xrightarrow[\iota]{} & M' \oplus M'' & \xrightarrow[\pi]{} & M'' & \longrightarrow & 0 \end{array}$$

The right square commutes trivially, and the left coomutes since one has

$$\Psi(\alpha(z)) = (\tau(\alpha(z)), \beta(\alpha(z))) = (z, 0) = \iota(z).$$

From there on one proceedes in an *ad hoc* manner as above, or resort to the general principle of the five lemma. ❑

When σ is a right section for β, the isomorphism Φ gives a decomposition $M = \alpha(M') \oplus \sigma(M'') = \ker\beta \oplus \sigma(M)$ into a direct sum of two *submodules* (hence the equalities are genuine), and in a similar fashion, when α has a left section τ, the module M decomposes as $M = \alpha(M') \oplus \ker\tau$, also a sum of two submodules.

PROBLEM 4.33 In this exercise the setting is as in the proposition, and the point is to connect up with the splitting criterion formulated in terms of idempotents we gave when discussing direct sums and products (Proposition 4.26 on page 75).

a) Assume that σ is a right section for β. Prove that $\sigma \circ \beta$ is an idempotent endomorphism of M, and that the corresponding decomposition in a direct sum is the one in remark abovef; that is $M = \ker\beta \oplus \sigma(M'')$.

b) Assume that τ is a left section for α. Prove that $\alpha \circ \tau$ is idempotent, and that the corresponding decomposition is $M = \alpha(M'') \oplus \ker\tau$. ★

PROBLEM 4.34 *(Aditive functors.)* A functor F between two module categories[9] $\mathsf{Mod}_A \to \mathsf{Mod}_B$ is said to be *additive* if it takes sums of maps to sums of maps; that is $F(\phi + \psi) = F(\phi) + F(\psi)$ whenever ϕ and ψ are A-linear maps between two A-modules. The functors $\mathrm{Hom}_A(-, N)$ and $\mathrm{Hom}_A(N, -)$ are examples of such animals.

[9] To make things simple, we contend ourselves to module categories. There is however a notion of *additive categories* (where hom-sets are abelian groups and compositions bilinear), and between such categories the term *additive functor* is meaningful.

Additive functors (*Additive funktorer*)

a) Let F be any covariant functor $F\colon \mathsf{Mod}_A \to \mathsf{Mod}_B$ and let $\beta\colon M \to N$ be an A-linear map having a right section σ. Prove that $F(\sigma)$ is a right section of $F(\beta)$.

b) Assume additionally that F is additive. Show that if the sequence

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

is split exact, then the sequence

$$0 \longrightarrow F(M') \xrightarrow{F(\alpha)} F(M) \xrightarrow{F(\beta)} F(M'') \longrightarrow 0$$

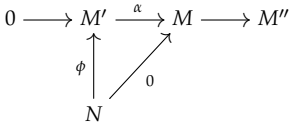
is split exact as well. In particular, the functor F transforms finite direct sums into finite direct sums. HINT: If σ and τ are sections of respectively β and α, then $F(\sigma)$ and $F(\tau)$ will be sections of respectively $F(\beta)$ and $F(\alpha)$. ★

Left exactness of hom-functors

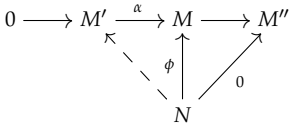
4.52 Suppose given a short exact sequence like (4.3) above and let N be an A-module. Applying the covariant hom-functor $\mathrm{Hom}_A(N,-)$ to the sequence, we obtain an induced sequence which is shaped like

$$0 \longrightarrow \mathrm{Hom}_A(N,M') \xrightarrow{\alpha_*} \mathrm{Hom}_A(N,M) \xrightarrow{\beta_*} \mathrm{Hom}_A(N,M'')\ . \tag{4.7}$$

The maps are simply given by composition; *i.e.* $\alpha_*\phi = \alpha\circ\phi$ and $\beta_*\phi = \beta\circ\phi$, and since $\beta_*\circ\alpha_* = (\beta\circ\alpha)_*$ and $\beta\circ\alpha = 0$, it holds true that $\beta_*\circ\alpha_* = 0$. More is true, the induced sequence will in fact be exact.



To understand why this is true, there are two spots where exactness is to be checked; the first being that α_* is injective. But $\alpha_*(\phi) = \phi\circ\alpha$, and since α is assumed to be injective, α_* is injective as well; indeed $\alpha\circ\phi = 0$ means that the image $\mathrm{im}\,\phi$ lies in the kernel of α. Secondly, to verify the sequence (4.7) is exact at the middle spot, assume that $\beta\circ\phi = 0$ for a map $\phi\colon N \to M$. Then ϕ factors through the image $\alpha(M')$, and α being injective, ϕ can be represented as $\alpha\circ\phi'$ for a map $\phi'\colon N \to M'$ which is precisely what we desire.



4.53 In a similar vein, the contravariant version $\mathrm{Hom}_A(-,N)$ applied to (4.3) yields the sequence where the arrows are reversed

$$0 \longrightarrow \mathrm{Hom}_A(M'',N) \xrightarrow{\beta^*} \mathrm{Hom}_A(M,N) \xrightarrow{\alpha^*} \mathrm{Hom}_A(M',N)\ , \tag{4.8}$$

and an argument like above shows that this also is an exact sequence.

PROBLEM 4.35 Give the argument referred to in the previous paragraph in detail. ★

4.54 It is common usage to refer to the phenomena described above as saying that $\mathrm{Hom}_A(N,-)$ and $\mathrm{Hom}_A(-,N)$ are *left exact functors*. There are crowds of

Left exact functors (*Venstre-eksakte funktorer*)

examples that β_* and α^* are not surjective, so $\mathrm{Hom}_A(N,-)$ and $\mathrm{Hom}_A(-,N)$ are seldom *exact functors* in the sense that they take short exact sequences to short exact sequences.

Exact functors (Eksakte funktorer)

A large part of homological algebra was developed just to describe the "missing cokernels" $\operatorname{coker}\beta_*$ and $\operatorname{coker}\alpha^*$. In general the only answer to this challenge is that the two sequences can be extended *ad infinitum* to the right to yield long exact sequences that involve so-called Ext-modules. These modules do not depend on the original short exact sequence only on the modules involved and N of course (but the maps in the long exact sequence do), and in some cases these long exact sequences can be controlled.

Two classes of modules stand out namely the ones with the property that either the functor $\mathrm{Hom}_A(N,-)$ or the functor $\mathrm{Hom}_A(-,N)$ exact. The former are called *projective modules* (they are ubiquitous in commutative algebra, and we shall come back to them) and the latter are the so-called *injective modules*.

Projective modules (Projektive moduler)
Injective modules (Injektive moduler)

4.55 In paragraph 4.52 above we proved the "only-if-part" of the following proposition (although we worked with short exact sequences like in (4.3) we never used that β was surjective).

Proposition 4.56 (Left exactness I) *Let the sequence*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \tag{4.9}$$

be given and assume that $\beta \circ \alpha = 0$. The sequence is exact if and only if for all A-modules N the sequence

$$0 \longrightarrow \mathrm{Hom}_A(N,M') \longrightarrow \mathrm{Hom}_A(N,M) \longrightarrow \mathrm{Hom}_A(N,M'') \tag{4.10}$$

is exact.

Proof: To attack the "if-part" assume that (4.10) is exact for all A-modules N.

If α is not injective, take $N = \ker\alpha$, which is non-zero, and let ι be the inclusion of $\ker\alpha$ in M'. Then $\alpha\circ\iota = 0$, but ι is non-zero so α_* is not injective.

In a similar vein, if the image $\operatorname{im}\alpha$ is strictly smaller than the kernel $\ker\beta$, take $N = \ker\beta$ and consider the inclusion map ι of N in M. By choice it holds that $\beta\circ\iota = 0$, but ι cannot factor though α since $\operatorname{im}\alpha$ is strictly contained in $\operatorname{im}\iota$. ❑

4.57 As alluded to in Paragraph 4.54 above, even if the map β is surjective, the induced map β_* will in most cases not be surjective. An easy example is given below. That β_* surjective means that any A-linear map $\phi\colon N \to M''$ can be lifted to an A-linear map into M, as illustrated in the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \longrightarrow & 0 \\ & & & & & \nwarrow & \uparrow{\scriptstyle \phi} & & \\ & & & & & & N & & \end{array}$$

PROPOSITION 4.58 *If F is a free A-module, the functor $\mathrm{Hom}_A(F,-)$ is exact; in other words, free modules are projective.*

PROOF: Let $\{f_i\}$ be a basis for F. Since β is surjective, there are elements $\{m_i\}_{i\in I}$ such that $\beta(m_i) = \phi(f_i)$. By the Universal Mapping Property of free modules (Proposition 4.37 on page 80), there is a map $\Phi\colon F \to M$ with $\Phi(f_i) = m_i$. Then $\beta\circ\Phi = \phi$ since $\beta(\Phi(f_i)) = \beta(m_i) = \phi(f_i)$, and two maps agreeing on a basis are equal. ❑

PROPOSITION 4.59 *An A-module is projective if and only if it is a direct summand in a free module.*

PROOF: Let P be the module. And assume first that P is projective. Let $\{p_i\}_{i\in I}$ be a generating set for P (finite or not, we do not care about the size. One could *e.g.* use the canonical free module F_P from Example 4.17 on page 81) and consider the exact sequence

$$0 \longrightarrow K \longrightarrow \bigoplus_{i\in I} A \xrightarrow{\phi} P \longrightarrow 0,$$

where a string $(a_i)_{i\in I}$ is sent to $\sum_i a_i p_i$ (the string lives in the direct sum so merely finitely many of the a_i's are non-zero). Since the p_i generate P, this map is surjective. Now, since P is projective, the identity map $\mathrm{id}_P\colon P \to P$ can be lifted to a $\sigma\colon P \to \bigoplus_{i\in I} A$. This means that $\phi\circ\sigma = \mathrm{id}_P$, and the lifting σ is a section of ϕ . Hence P lies split in $\bigoplus_{i\in I} A$ by the Splitting Criterion (Proposition 4.51 on page 88).

To prove the other implication, let $\phi\colon P \to M''$ be given assume that $P\oplus P'$ is free. Consider the map $P\oplus P' \to M''$ sending (x,y) to $\phi(x)$. This map can be lifted as $P\oplus P'$ is free, and restricting the lifted map to P yields a lifting of ϕ. ❑

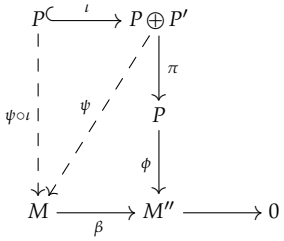


Diagram illustrating the last part of the proof; π is the projection and ι the inclusion. Notice that $\pi\circ\iota = \mathrm{id}_P$.

4.60 There is also an assertion dual to the one of Proposition 4.56 above. The proof of the two being quit similar, we leave all the checking to the zealous and not so zealous students; it is a good training for these diagram-arguments. The assertion reads as follows:

PROPOSITION 4.61 (LEFT EXACTNESS II) *Let the sequence*

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0 \tag{4.11}$$

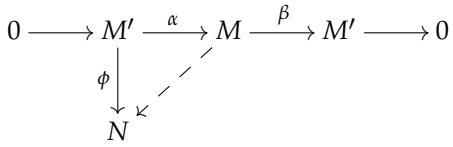
be given and assume that $\beta\circ\alpha = 0$. The sequence is exact if and only if for all A-modules N the sequence

$$0 \longrightarrow \mathrm{Hom}_A(M'',N) \longrightarrow \mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_A(M',N) \tag{4.12}$$

is exact.

4.62 In most cases the map α^* will not be surjective even if α is. Surjectivity means that any map $\phi\colon M \to N$ can be extended to a map $M \to N$, like in the

diagram below



Examples

4.22 Consider the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0 \tag{4.13}$$

where p is a prime number. No non-zero map from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}$ exists (all elements in $\mathbb{Z}/p\mathbb{Z}$ are killed by p, but none in $\mathbb{Z}$ apart from 0), so the identity $\mathrm{id}_{\mathbb{Z}/p\mathbb{Z}}$ can not be lifted to a map $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}$. Since it holds true that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}) = 0$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$, applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, -)$ yields the sequence

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z}/p\mathbb{Z},$$

and of course a map $0 \to \mathbb{Z}/p\mathbb{Z}$ cannot be surjective!

4.23 We observe that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$, so the functor $\mathrm{Hom}_{\mathbb{Z}}(-, Z/p\mathbb{Z})$ when applied to the sequence (4.13) in example 4.22 above, yields the exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{p^*} \mathbb{Z}/p\mathbb{Z}.$$

The map p^* is just multiplication by p which on $\mathbb{Z}/p\mathbb{Z}$ is the zero map; hence the rightmost arrow is zero. The left arrow is therefore an isomorphism; this ensues from exactness of the sequence, but neither is it hard to verify *ad hoc* that it equals the identity map.

☆

Example 4.24 *(A projective module that is not free)* The prime ideals one meets in number theory which are not principal are in most cases projective, and later on we shall prove this for ideals in the so-called Dedekind rings. For the moment we content ourself with giving just one example illustrating this phenomenon.

The example will be the ideal $\mathfrak{a} = (2, 1 + i\sqrt{5})$ in the ring $A = \mathbb{Z}[i\sqrt{5}]$, which turns out to be a projective but not a free A-module. Indeed, we shall with an explicit construction see that $\mathfrak{a}$ is a direct summand in the free module $A \oplus A$ and hence it will be projective (Proposition 4.59 on page 92), and since it is not principal, it is not free.

Showing that $\mathfrak{a}$ is a summand in $A \oplus A$ amounts to finding an isomorphism $A \oplus A \simeq \mathfrak{a} \oplus M$, for some module M. In fact, one may show that the complement M is forced to be isomorphic with $\mathfrak{a}$, so that $A \oplus A \simeq \mathfrak{a} \oplus \mathfrak{a}$, but that will be for some other time. This also provides an example of two direct sums that are isomorphic without the summands being isomorphic.

The free module $A \oplus A$ has the usual basis $e_1 = (1,0)$ and $e_2 = (0,1)$ The gist of the construction is the map

$$\phi\colon A \oplus A \to \mathfrak{a} \subseteq A$$

defined by the assignments $e_1 \mapsto 2$ and $e_2 \mapsto 1 + i\sqrt{5}$. We shall identify a submodule M inside $A \oplus A$ that ϕ maps isomorphically onto $\mathfrak{a}$ and thereby proving that $\mathfrak{a}$ lies split in $A \oplus A$. The submodule M in question is generated by the two elements $a_1 = -2e_1 + (1 - i\sqrt{5})e_2$ and $a_2 = -(1 + i\sqrt{5})e_{t1} + 3e_2$

We begin with checking that the restriction $\phi|_M$ is surjective. This ensues from the very definition of ϕ as the following little calculations show:

$$\begin{aligned}\phi(a_1) &= -2 \cdot 2 + (1 - i\sqrt{5}) \cdot (1 + i\sqrt{5}) = -4 + 6 = 2,\\ \phi(a_2) &= -(1 + i\sqrt{5}) \cdot 2 + 3 \cdot (1 + i\sqrt{5}) = (1 + i\sqrt{5}).\end{aligned}$$

To prove that ϕ is injective on M, pick an element $a = xa_1 + ya_2$ in M that maps to zero. This means that $2x + (1 + i\sqrt{5})y = 0$ in A. Now, one has

$$xa_1 + ya_2 = -\big(2x + (1 + i\sqrt{5})y\big)e_1 + ((1 - i\sqrt{5})x + 3y)e_2 = \big((1 - i\sqrt{5})x + 3y\big)e_2,$$

and since

$$2\big((1 - i\sqrt{5})x + 3y\big) = \big(-(1 + i\sqrt{5})(1 - i\sqrt{5}) + 6\big)y = 0,$$

it follows that $(1 - i\sqrt{5})x + 3y = 0$ as well. Hence $a = 0$, and we are through. ☆

Problems

4.36 Let A be a ring and suppose that B is an A-algebra. Assume given an exact sequence ⁂

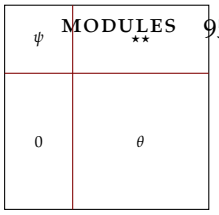
$$0 \longrightarrow E \longrightarrow F \longrightarrow G \longrightarrow 0$$

of B-modules that regarded as A-modules are free of finite rank. Prove that $\operatorname{rk}_A F = \operatorname{rk}_k E + \operatorname{rk}_A G$.

In the following exercise we let $P_\phi(t) = \det(t \cdot \mathrm{id}_E - \phi)$ be the characteristic polynomial of an endomorphism $\phi\colon E \to E$ of a free A-module of finite rank.

4.37 *(Multiplicativity of the characteristic polynomial.)* Assume given a commutative diagram ⁂

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & E & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 0 \end{array}$$



where the rows are exact and the involved modules are free of finite rank. Prove that $\det\phi = \det\psi \cdot \det\theta$. Show that $P_\phi(t) = P_\psi(t) \cdot P_\theta(t)$. HINT: Exhibit a basis for F in which the matrix of ϕ has an appropriate block decomposition (as in the margin). Conclude that $\det\phi = \det\theta \cdot \det\psi$ and that $\operatorname{tr}\phi = \operatorname{tr}\theta + \operatorname{tr}\psi$.

4.38 With reference to Example 4.24 above, let $A = \mathbb{Z}[i\sqrt{5}]$ and $\mathfrak{a} = (2, 1 + i5)$. Let $\Psi\colon 2A \to 2A$ be the A-linear map given by the matrix

$$\Psi = \begin{pmatrix} -3 & 1 + i\sqrt{5} \\ 1 - i\sqrt{5} & -2 \end{pmatrix}$$

a) Show that there is an exact sequence

$$2A \xrightarrow{\Psi} 2A \xrightarrow{\phi} \mathfrak{a} \longrightarrow 0,$$

where ϕ is the map from Example 4.24, and hence that $\operatorname{coker}\Psi \simeq \mathfrak{a}$.

b) Show that $\operatorname{Hom}_A(\mathfrak{a}, A) \simeq \mathfrak{a}$.

c) Let $\Phi\colon 2A \to 2A$ be the map given the matrix

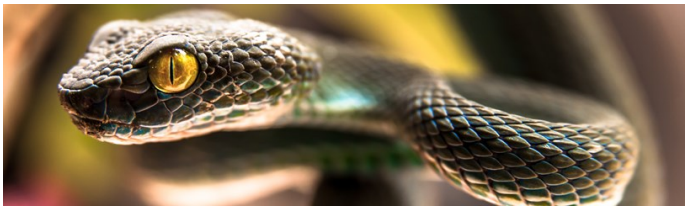
$$\Phi = \begin{pmatrix} 2 & 1 + i\sqrt{5} \\ 1 - i\sqrt{5} & 3 \end{pmatrix}$$

Show that $\Phi \circ \Psi = \Psi \circ \Phi = 0$, and that there is an exact sequence

$$\ldots \xrightarrow{\Phi} 2A \xrightarrow{\Psi} 2A \xrightarrow{\Phi} 2A \xrightarrow{\Psi} 2A \xrightarrow{\Phi} \ldots$$

that extends infinitely in both directions.

d) Show that $\operatorname{coker}\Phi \simeq \mathfrak{a}$, and conclude that $2A \simeq 2\mathfrak{a}$.



4.6 *Snakes and alike*

4.63 An all important feature in homological algebra are the so-called *connecting maps* which relate homology groups of complexes in various ways. A simple but very useful instance of this feature is described in the Snake Lemma. The name is of "bourbakistic origin", and mnemotechnical efficient. See the next section below for a reason for the name.

Lemma 4.64 (The snake lemma) *Given a diagram*

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\phi_1} & M_2 & \xrightarrow{\phi_2} & M_3 & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow[\psi_1]{} & N_2 & \xrightarrow[\psi_2]{} & N_3 \end{array} \tag{4.14}$$

where the rows are exact and the squares are commutative. There exists a map $\delta\colon \ker \alpha_3 \to \operatorname{coker} \alpha_1$ *rendering the following sequence exact*

$$\ker \alpha_2 \longrightarrow \ker \alpha_3 \xrightarrow{\delta} \operatorname{coker} \alpha_1 \longrightarrow \operatorname{coker} \alpha_2, \tag{4.15}$$

where the two extremal maps from left to right are induced by and ϕ_2 *and* ψ_1*.*

Proof: The proof of the Snake Lemma is an example of a sport called *diagram chasing* which was extensively practised among homological algebraists. We have two missions to complete, firstly the map δ must be constructed and secondly, we must verify that the sequence (4.15) is exact.

We begin with the first and most interesting one: A short and dirty mnemotechnical definition of δ is $\psi_1^{-1} \circ \alpha_2 \circ \phi_2^{-1}$ which of course is meaningless as it stands since neither ϕ_2 nor ψ_1 is invertible, but it gives a hint of how to construct δ.

Now the fun is starting: Pick an element $x \in M_3$ so that $\alpha_3(x) = 0$ and lift it to an element y in M_2; that is, pick an element $y \in M_2$ with $\phi_2(y) = x$. The rightmost square of (4.14) being commutative, we infer that $\psi_2(\alpha_2(y)) = 0$; the bottom line of 4.14 being exact, there is thence a z in N_1 with $\psi_1(z) = \alpha_2(y)$. And that is it; the image of z in $\operatorname{coker} \alpha_1$ is the wanted guy $\delta(x)$.

$$\begin{array}{ccccc} y & \longmapsto & x & & \\ \downarrow & & \downarrow & & \\ z & \longmapsto & \alpha_2(y) & \longmapsto & 0 \\ \downarrow & & & & \\ \delta(x) & & & & \end{array}$$

We have done a choice on the way—the choice of a lift of x to M_2—and for the definition of δ to be legitimate the trapped z must be independent of that choice. So assume that y' is another element of M_3 that maps to x; then we may write $y' = y + w$ with $\phi_2(w) = 0$. Since the line on top of 4.14 is exact it holds that $w = \phi_1(u)$ for some u, and we find

$$\alpha_2(y') = \alpha_2(y) + \alpha_2(\phi_1(w)) = \alpha_2(y) + \psi_1(\alpha_1(u))$$

Luckily, ψ_1 is injective (the bottom line of 4.14 is exact), so if $z' \in N_1$ is such that $\psi_1(z') = y'$ one has

$$z' = z + \alpha_1(u)$$

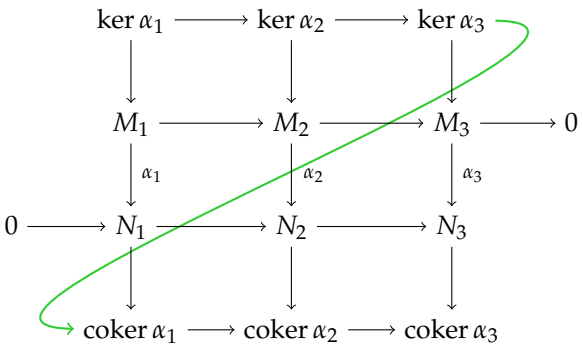
and finally, this means the images of z and z' in $\operatorname{coker} \alpha_1$ agree, and δ is well defined!

The big game has been snared, and it remains only to check exactness of 4.15: We shall do half of the job and check exactness at $\ker \alpha_3$, letting the zealous students have the fun of checking the other half. So assume that $\delta(x) = 0$. This means that $z = \alpha_1(v)$ for some $v \in M_1$; hence $\alpha_2(y) = \psi_1(z) = \psi_1(\alpha_1(v)) = \alpha_2(\phi_1(v))$. It follows that $y = \phi_1(v) + t$ with $t \in \ker \alpha_2$ and consequently $x = \phi_2(y) = \phi_2(t)$, which is what we need. ❑

Why snake?

The reason for the name "Snake Lemma" is apparent when one considers the diagram below.

There the map δ connecting $\ker \alpha_3$ to $\operatorname{coker} \alpha_1$ we constructed in the Snake Lemma, zig-zags like a green snake through the diagram.



In applications of the Snake Lemma one frequently happens that the maps $\phi_1 \colon M_1 \to M_2$ is injective and one $\psi_2 \colon N_2 \to N_3$ is surjective. The diagram we start with thus is shaped like

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\phi_1} & M_2 & \xrightarrow{\phi_2} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow[\psi_1]{} & N_2 & \xrightarrow[\psi_2]{} & N_3 & \longrightarrow & 0 \end{array} \tag{4.16}$$

Such a diagram induces two three term exact sequences, one formed by the kernels of the α_i's and one by their cokernels, and point is that the snake map δ connects these two sequences. In other words, we have a six term exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker \alpha_1 & \longrightarrow & \ker \alpha_2 & \longrightarrow & \ker \alpha_3 & & \\ & & & & & \overset{\delta}{\searrow} & & & \\ & & \operatorname{coker} \alpha_1 & \longrightarrow & \operatorname{coker} \alpha_2 & \longrightarrow & \operatorname{coker} \alpha_3 & \longrightarrow & 0. \end{array} \tag{4.17}$$

LEMMA 4.65 (SNAKE LEMMA II) *Assume given a commutative diagram with exact row as in (4.16). Then the six term sequence (4.17) above is exact.*

PROOF: The sequence is trivially exact at the two extreme slots $\ker \alpha_1$ and $\operatorname{coker} \alpha_3$, and that the snake-part is exact, is just the Snake Lemma, so what remains to be done is checking exactness at $\ker \alpha_2$ and $\operatorname{coker} \alpha_2$, and this

follows by two simple hunts in the diagram. We shall check exactness at $\ker \alpha_2$, but shall leave exactness at $\operatorname{coker} \alpha_2$ for the students to practise diagram chasing. So assume that $x \in \ker \alpha_2$ is such that $\phi_2(x) = 0$. Then $x = \phi_1(y)$ for some $y \in M_1$, and $\psi_1(\alpha_1(y)) = \alpha_2(\phi_1(y)) = \alpha_2(x) = 0$. Since ψ_1 is assumed to be injective, it follows that $y \in \ker \alpha_1$ and we are through. ❑

Problems

4.39 *(The five lemma I.)* Use the Snake Lemma to prove the following abbreviated and preliminary version of the five lemma in the next exercise. Assume given a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

with exact rows. If two of the α_i's are isomorphisms, then the third one is as well.

4.40 *(The five lemma II.)* Given a commutative diagram

$$\begin{array}{ccccccccc} M_0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 \\ \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} \\ M_0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 \end{array}$$

of A-modules with exact rows. Show that α_2 is an isomorphism whenever the four other α_i's are.

There is a slightly stronger assertion namely that if α_1 and α_3 are isomorphisms, α_0 surjective and α_4 injective, then α_2 is an isomorphism. Prove this.

There is a plethora of small results like this involving diagrams of different geometric shapes and with suggestive names like the star lemma and the diamond lemma. Once you have grasped the essence of diagram chasing and remember the Snake Lemma you should be safe in that corner of the territory of homological algebra. The most important use of connecting homomorphisms is when constructing long exact sequences of homology associated with a complexes; but that will be for a later occasion.

In the next two exercises one take the following statement for granted:

PROPOSITION 4.66 *Assume that A is a* PID *and that $\phi\colon E \to E$ is an endomorphism of a finitely generated free A-module E. Then ϕ lives in a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F & \longrightarrow & E & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \phi} & & \downarrow & & \\ 0 & \longrightarrow & F & \longrightarrow & E & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

where the rows are exact and where F is free of rank $n-1$.

4.41 Infer from the previous exercise that if $A = \mathbb{Z}$ and ϕ has non-vanishing determinant, it holds true that the cokernel $\operatorname{coker}\phi$ is finite and that $\|\det\phi\| = \#\operatorname{coker}\phi$. HINT: Use the Snake Lemma. ✲

4.42 In the same vein as in exercise 4.41 above, assume that $A = k[t]$ is the polynomial ring over the field k and that ϕ has non-vanishing determinant. Prove that $\operatorname{coker}\phi$ is of finite dimension over k and that $\deg\det\phi = \dim_k \operatorname{coker}\phi$ HINT: Again, the snake is the solution. ✲

4.43 *(Modules of finite presentation.)* One says that a module M is of *finite presentation* if it sits in an exact sequence ✲

Modules of finite presentation (*Moduler av endelig presentasjon*)

$$A^n \longrightarrow A^m \longrightarrow M \longrightarrow 0$$

where A^n and A^m are finitely generated free modules. Let $N \subseteq M$ be a submodule. In general this is a more restrictive condition on a module than being finitely generated, however over Noetherian rings the two are equivalent. Prove that if both N and M/N are of finite presentation, then the same holds for M. HINT: Establish a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & A^r & \longrightarrow & A^{r+s} & \longrightarrow & A^s & \longrightarrow & 0 \end{array}$$

with exact rows and all three vertical map being surjective. Then apply the Snake Lemma and Proposition 4.15 on page 79.

★

Lecture 5

Tensor products

Version 2.1 as of 2018-10-18 at 09:53 (typeset 3rd December 2018 at 10:03am). Prone to misprints and errors and will change.

The term "tensor" appeared for the first time with a meaning resembling the current one in 1898. The German physicists Woldemar Voigt used the word in a paper about crystals. Tensors are these days extensively used in physics, and may be the most prominent example is the so-called "stress-energy-tensor" of Einstein. It governs the general theory of relativity and thereby our lives in the (very) large!

A slightly less influential occurrence took place in 1938 when the American mathematician Hassler Whitney when working on the universal coefficient theorem in algebraic topology introduced the tensor product of two abelian groups. Certain isolated cases had been known prior to Whitney's work, but Whitneys construct was general, and it is the one we shall give (although subsequently polished by several mathematicians, in particular Nicolas Bourbaki, and generalized to modules).

How far apart stress in crystals and the universal coefficient theorem may appear, the concept of tensors is basically the same—the key word being bilinearity.

Woldemar Kummer
(1850–1919)
German physicist

5.1 Introducing the tensor product

First of all, let us recall what a *bilinear map* $M \times N \to L$ is where M, N and L are three modules over a ring A.

It is simply what the name says, a map β which is linear in each of the two variables; that is, when one of the variables is kept fixed, it dependents linearly on the other. For instance, when the second variable is kept constant, it holds true that

$$\beta(ax + by, z) = a\beta(x, z) + b\beta(y, z),$$

where a and b belong to the ring A and x and y are elements in M (and ditto when the first variable is fixed). Frequently, when several rings are around, one says *A-bilinear* to be reminded which ring is considered the base ring.

Hassler Whitney
(1907–1989)
American mathematician

Bilinear maps (*Bilineære avbildninger*)

A typical example from the world of vector spaces over a field k, would be a scalar product on a vector space V, and within the realm of commutative algebra, the products of an A-algebra B is a good example; the multiplication map $(a, b) \mapsto ab$ is an A-bilinear map $B \times B \to B$.

Multilinear maps (*Multilineære avbildninger*)

5.1 There is naturally also the notion of *multilinear maps*, which involves more than two modules. In that case, the source of the map is a product $\prod_i M_i$ of finitely many A-modules M_i and its target is another A-module L. The constituting property is *mutatis mutandis* the same as for bilinear ones: When all but one of the variables are kept constant, the resulting map is A-linear.

The universal property

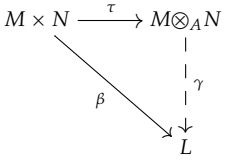
5.2 The tensor product captures in some sense all possible bilinear maps defined on the product of two A-modules M and N, or at least makes them linear. This rather vague formulation becomes precise when phrased as a universal property.

The tensor product (*Tensorproduktet*)

5.3 The *tensor product* is a pair consisting of an A-module $M \otimes_A N$ together with an A-bilinear map $\tau \colon M \times N \to M \otimes_A N$ that abide by the following rule:

- For any bilinear map $\beta \colon M \times N \to L$, there is a unique A-linear map $\gamma \colon N \otimes M \to L$ suct that $\beta = \gamma \circ \tau$.

In other words, every A-bilinear β factors linearly via τ, as expressed by the commutative diagramme in the margin. And as ususal with objects satisfying a universal property, the pair τ and $M \otimes_A N$ is unique up to a unique isomorphism.



Exsistence

The construction of the tensor product is rather abstract and serves the sole purpose of establishing the existence. It will seldom be referred to in the sequel, if at all. To ease getting a grasp on the tensor product remember the mantra, so true in moderen mathematics: "Judge things by what they do, not by what they are".

5.4 The construction starts out with the free A module $F = A^{M \times N}$ on the set $M \times N$. The elements of F are finite, formal linear combinations $\sum_i a_i \cdot (x_i, y_i)$ with $x_i \in M$, $y_i \in M$ and $a_i \in A$. In particular, every pair (x, y) is an element of F, and by definition these pairs form a basis for F. We proceede by letting G be the submodule of F generated by all expressions either of the form

$$(ax + a'x', y) - a(x, y) - a'(x', y), \tag{5.1}$$

or of the form

$$(x, ay + a'y') - a(x, y) - a'(x, y'), \tag{5.2}$$

where a and a' are elements from A while x and x' lie in M and y and y' in N.

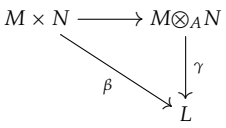
The tensor product $N\otimes_A M$ is defined as the quotient F/G, and the residue class of a pair (x,y) will be denoted by $x\otimes y$. Having forced the two expressions (5.1) and (5.2) above to be zero by factoring out the submodule G, we have made $x\otimes y$ a bilinear function of x and y; that is, the following two relations hold true in $M\otimes_A N$:

$$\begin{aligned}(ax+a'x')\otimes y &= a(x\otimes y)+a'(x'\otimes y),\\ x\otimes(ay+ay') &= a(x\otimes y)+a'(x\otimes y').\end{aligned} \tag{5.3}$$

In other words, the map $\tau\colon M\times N\to M\otimes_A N$ sending (x,y) to $x\otimes y$ is A-bilinear.

PROPOSITION 5.5 *The pair τ and $M\otimes_A N$ as constructed above satisfy the universal property in paragraph 5.3; in other words, they are the tensor product of M and N.*

PROOF: We already saw that τ is bilinear, so we merely have to check the factorization property. To that end, let $\beta\colon M\times N\to L$ be bilinear. Since $F=A^{M\times N}$ is a free module on $M\times N$, we may , according to the Universal Mapping Principle for free modules (Proposition 4.37 on page 80), define an A-linear map $\bar\beta\colon F\to L$ by sending a the basis-elements (x,y) to the values $\beta(x,y)$. Since β is bilinear, this map vanishes on the submodule G. Consequently it factors through the quotient $F/G=M\otimes_A N$ and thus gives the wanted map $\gamma\colon M\otimes_A N\to L$.



Elements shaped like $x\otimes y$ generate the tensor product, and because the value at $x\otimes y$ of any factorization of β is compelled to be $\beta(x,y)$, the uniqueness of γ comes for free. ❑

5.2 *Basic working formulas*

In this section we present a few principles and properties of the tensor products which together with some basic formulas hopefully should help students grasp "the spirit of the tensor product" and make it easier to work with it. We also discuss some particular classes of modules, like cyclic modules and free modules, which behave particularly well when exposed to a tensor product.

Decomposable tensors.

5.6 For several reasons, tensors of the form $x\otimes y$ deserve a special name; they are dubbed *decomposable tensors*. Only in a very few highly special cases all elements in a tensor product will be decomposable; the usual situation is that most are not (A simple example is discussed in Problem 5.13 on page 113 below. See also Example 5.6 on page 120). A general element in $M\otimes_A N$ may however, be expressed as a finite linear combination $\sum_i a_i\cdot x_i\otimes y_i$ of decomposable tensors since this is already true in the free module $F=A^{M\times N}$.

Decomposable tensors (*Dekomponerbare tensorer*)

Consequently, if $\{x_i\}$ is a set of generators of M and $\{y_j\}$ one for N, the decomposable tensors $\{x_i \otimes y_j\}$ form a set of generators for $M \otimes_A N$; in particular, if both factors are finitely generated, the same holds for the tensor product $M \otimes_A N$.

5.7 To define a map ϕ from $M \otimes_A N$ into any module, it suffices to give the values of ϕ on decomposable tensors $x \otimes y$, provided these values depend bilinearily on x and y. This is an informal and convenient reformulation of the universal property from Paragraph 5.3, certainly more suggestive than working with pairs (x, y).

5.8 Another useful property of decomposable tensors is subsumed in the slogan "scalars can be moved past the tensor product"; or in precise terms, for every element $a \in A$ it holds true that

$$(ax) \otimes y = x \otimes (ay).$$

This is a simple consquence of the fundamental bilinear relations (5.3) on page 103; with the notation of (5.3), just set $x' = y' = 0$.

Functoriality

Linear maps between A-modules are fundamental tools in algebra, and and it comes as no surprise that exploring how maps behave when exposed to tensor products occupies a large of the theory. As a modest start we shall observe that the tensor product construct is functorial, in the precise meaning that when considered a function of either variable, it gives a functor $\mathsf{Mod}_A \to \mathsf{Mod}_A$; so we have to tell how to tensorize maps.

5.9 Any A-linear map $\phi\colon M \to M'$ gives rise to an A-linear map $M \otimes_A N \to M' \otimes_A N$ that on decomposable tensors acts as $x \otimes y \mapsto \phi(x) \otimes y$: The expression $\phi(x) \otimes y$ depending bilinearily on x and y, this is a viable definition, and the resulting map is naturally babtized $\phi \otimes \mathrm{id}_N$.

Obviously, it holds true that $\psi \otimes \mathrm{id}_N \circ \phi \otimes \mathrm{id}_N = (\psi \circ \phi) \otimes \mathrm{id}_N$ when ψ and ϕ are two composable maps (the identity holds for decomposable tensors), and clearly $\mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes_A N}$. This means that the pair of assignments

$$M \mapsto M \otimes_A N \quad \text{and} \quad \phi \mapsto \phi \otimes \mathrm{id}_N$$

define a functor $- \otimes_A N\colon \mathsf{Mod}_A \to \mathsf{Mod}_A$.

PROPOSITION 5.10 *The functor $- \otimes_A N$ is an A-linear functor. In particular, it transforms direct sums into direct sums.*

A formal consequence of a functor being additive is that it preserves direct sums (as we established in Problem 4.34 on page 89), however we shall come back to the matter below and sketch an *ad hoc* proof when discussing Proposition 5.13 below.

PROOF: Recall that in Exercise 4.34 on page 89 we introduced the notion of additive functors: Saying the functor is *additive* is saying it transforms sums of maps to sums of maps, and it is *A-linear* if it additionally respects products with scalars; expressed in symbols this reads

additive functors (*Additive funktorer*)
A-linear functors (*Lineære fuktorer*)

$$(a\phi + b\psi)\otimes \mathrm{id}_N = a\cdot\phi\otimes\mathrm{id}_N + b\cdot\psi\otimes\mathrm{id}_N. \tag{5.4}$$

This follows easily from how $-\otimes_A N$ acts on maps together with the basic bilinear relations in (5.3) on page 103. Indeed, one finds

$$\begin{aligned}(a\phi + b\psi)\otimes\mathrm{id}_N\ (x\otimes y) =&((a\phi(x) + b\psi(x))\otimes y =\\ =\ a\phi(x)\otimes y + b\psi(x)\otimes y =&\big(a\cdot\phi\otimes\mathrm{id}_N + b\cdot\psi\otimes\mathrm{id}_N\big)x\otimes y,\end{aligned}$$

and the two sides of (5.4) agree on decomposable tensors. Hence they are equal since the decomposable tensors generate $M\otimes_A N$.

5.11 The situation is completely symmetric in the two variables, so if $\psi\colon N\to N'$ is a map, there is a map $\mathrm{id}_M\otimes\psi$ from $M\otimes N$ to $M\otimes N'$ that sends $x\otimes y$ to $x\otimes\psi(y)$, and naturally, on sets $\phi\otimes\psi = (\phi\otimes\mathrm{id}_N)\circ(\mathrm{id}_{M'}\otimes\psi)$.

Some formulas

5.12 When working with tensor products a series of formulas are invaluable. Here we given the most basic ones revealing the multiplicative nature of the tensor product; together with the direct sum it behaves in a way resembling the product in a ring.

PROPOSITION 5.13 *Suppose that M, N and L are modules over the ring A. Then we have the following four canonical isomorphisms.*

- *Neutrality:* $M\otimes_A A\simeq M$;
- *Symmetry:* $M\otimes_A N\simeq N\otimes_A M$;
- *Associativity:* $(M\otimes_A N)\otimes_A L\simeq M\otimes_A(N\otimes_A L)$;
- *Distributivity:* $(M\oplus N)\otimes_A L\simeq(M\otimes_A L)\oplus(N\otimes_A L)$.

There are some comments to be made. Firstly, these isomorphisms are so natural that for all practical purposes they may be consider as identities. Secondly, the general mechanism that extends associativity from products with three factors to products with arbitrary many factors applies to tensor products, so that any number of parentheses placed in any way in a tensor product with any number of factors can be resolved. And finally, an easy induction establishes the fourth property for any number of summands; with a somehow subtler argument, one may even show it holds for infinitely many.
PROOF: In each case we indicate how a pair of mutual inverses A-linear maps acts on decomposable tensors; this will basically suffice in the two first cases, but in particular the case of associativity, requires some more work.

Neutrality: For the first formula the actions on decomposables are $x\otimes a \to xa$ and $x \mapsto x\otimes 1$. The product xa is bilinear in x and a and therefore the map $x\otimes a \to xa$ descends to an A-linear map $M\otimes_A A \to M$ which obviously have $x \mapsto x\otimes 1$ as inverse.
Symmetry: In this case the short hand assignments are $x\otimes y \leftrightarrow y\otimes x$. In both directions the assignments are bilinear in view of the fundamental relations (5.3), and obviously they define inverse maps.

Associativity: This case is more subtle than one should believe at first sight; the (very short) shorthand definition would be $(x\otimes y)\otimes z \leftrightarrow x\otimes(y\otimes z)$, but this is not viable since $x\otimes y$ is not a general member of $M\otimes_A N$. To salvage the situation one introduces some auxiliary maps, one for each $z \in L$.

So, fix an element z from L and define an A-linear map $\eta_z\colon M\otimes_A N \to M\otimes_A(N\otimes_A L)$ by the assignment $x\otimes y \mapsto x\otimes(y\otimes z)$, which is legitimate since the expression $x\otimes(y\otimes z)$ is bilinear in x and y (the third variable z is kept fixed).

Obviously the map $\eta_z(t)$ is linear in z and *a priori* being linear in t, it depends bilinearily on t and z. We infer that sending $t\otimes z$ to $\eta_t(z)$ induces a map $(M\otimes_A N)\otimes_A L \to M\otimes_A(N\otimes_A L)$. On decomposable tensors this map behaves as wanted; that is, it sends $(x\otimes y)\otimes z$ to $x\otimes(y\otimes z)$.

A symmetric construction yields a map the other way which sends a decomposable tensor $x\otimes(y\otimes z)$ to $(x\otimes y)\otimes z$. Finally, these two maps are mutually inverses since they act as inverse maps on the decomposables, and the decomposables generate the tensor products.

Distributivity: Another way of phrasing this is to say at the tensor product respects directs sums, and this we already established in Proposition 5.10 above. However to at least halfway fulfil our promise, we vaguely indicate the beginning of an *ad hoc* proof in the flavour of the three preceding parts of the proof. It is based on the short hand version $(x, y)\otimes z \leftrightarrow (x\otimes z, y\otimes z)$, and the salient point is to extend these to maps defined on the entire tensor products using bilinearity; but, of course, details are left to the benefit of the zealous students. ❑

5.14 It is worth while to dwell a little on the associativity. Since the parentheses are irrelevant, we may as well skip them and write $M\otimes_A N\otimes_A L$ for $M\otimes(N\otimes_A L)$ (or for that matter for $(M\otimes_A N)\otimes_A L$). According to the universal property of the tensor product bilinearity is the clue for defining maps having source $M\otimes_A N$, and there is a similar trilinearity principle for defining maps sourced in a triple tensor product $M\otimes_A N\otimes_A L$. It suffices to specify ϕ on decomposable tensors $x\otimes y\otimes z$ as long as the specifying expression is trilinear in x, y and z; the precise statement is a as follows:

LEMMA 5.15 (TRILINEARITY PRINCIPLE) *Let A be a ring and M N, K and L four A-modules. Assume given a map $\phi\colon M \times N \times K \to L$ such that $\phi(x, y, z)$ depends in a trilinear manner on the variables. Then there is unique A-linear map*

$\phi\colon M\otimes_A N\otimes_A K \to L$ such that $\phi(x\otimes y\otimes z) = \phi(x,y,z)$.

PROOF: The argument is *mutatis mutandis* the same as we gave in the proof of Proposition 5.13 concerning the associative law: Fix an element $z \in K$ and consider $\phi(x,y,z)$; it depends in a bilinear manner on x and y and hence gives rise to a linear map $\eta_z\colon M\otimes_A N \to L$. The dependence of η_z on z obviously being linear, assigning $\eta_z(t)$ to $t\otimes z$ for $t \in M\otimes_A N$ and $z \in K$ is a bilinear in z and t and therefore yields the desired map $(M\otimes_A N)\otimes_A K \to L$.

And again, the map is unambiguously determined since its values are prearranged on the decomposable tensors which generate $(M\otimes_A N)\otimes_A K$. ❑

As a final comment, there is nothing special about the number three in this context. A similar statement—that is, a *principle of multi-linearity*—holds true for tensor products with any number of factors, but we leave that to the imagination of the reader.

PROBLEM 5.1 Consider the four isomorphisms in Proposition 5.13 on page 105. Be explicit about what it means that they are functorial (in every variable involved) and prove your assertions. ★

The case of cyclic modules

We now turn to discuss two situation which are frequently met when working with tensor products. Hopefully they will illuminate the working mechanism of the tensor product, but anyhow, they are illustrate some of the different phenomena that can occur.

5.16 Our first example is about the tensor product of two cyclic module and reads as follows:

PROPOSITION 5.17 *Let A be a ring. For any two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A it holds true that $A/\mathfrak{a}\otimes_A A/\mathfrak{b} \simeq A/(\mathfrak{a}+\mathfrak{b})$. In particular, one has $A/\mathfrak{a}\otimes_A A/\mathfrak{b} = 0$ if and only if the two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal.*

PROOF: Sending a pair $([x]_\mathfrak{a},[y]_\mathfrak{b})$ from $A/\mathfrak{a}\times A/\mathfrak{b}$ to the element $[xy]_{\mathfrak{a}+\mathfrak{b}}$ in $A/\mathfrak{a}+\mathfrak{b}$ is well defined and bilinear; indeed, changing x (resp. y) by a member of $\mathfrak{a}$ (resp. $\mathfrak{b}$) changes xy by a member of $\mathfrak{a}$ (resp. $\mathfrak{b}$) as well, so the map is well defined, and a product clearly depends bilinearily on the factors. This induces a map $A/\mathfrak{a}\otimes_A A/\mathfrak{b} \to A/\mathfrak{a}+\mathfrak{b}$.

One the other hand, the tensor product $A/\mathfrak{a}\otimes_A A/\mathfrak{b}$ is a cyclic A-module generated by $1\otimes 1$ because $[a]_\mathfrak{a}\otimes[b]_\mathfrak{b} = ab\cdot 1\otimes 1$, and clearly elements from both the ideals $\mathfrak{a}$ and $\mathfrak{b}$ kill it since

$$x\cdot 1\otimes 1 = (x\cdot 1)\otimes 1 = 1\otimes(x\cdot 1).$$

So $A/\mathfrak{a}\otimes_A A/\mathfrak{b}$ is a quotient of $A/\mathfrak{a}+\mathfrak{b}$ and consequently it is squeezed between two copies of $A/\mathfrak{a}+\mathfrak{b}$, by two maps both sendig 1 to 1, and hence all three must coincide. ❑

The proposition shows that the tensor product of two non-zero modules very well may vanish, and for cyclic modules this happens precisely when the respective annihilators are comaximal. We also observe that taking $\mathfrak{b} = \mathfrak{a}$ yields an isomorphism $A/\mathfrak{a}\otimes_A A/\mathfrak{a} \simeq A/\mathfrak{a}$.

Finite abelian groups

5.18 A modest instance of the tensor product being zero, is found among finite abelian groups. Powers of two relatively prime integers p and q are comaximal—for natural numbers μ and ν it holds that $(p^\mu, q^\nu) = \mathbb{Z}$—and we infer that

$$\mathbb{Z}/p^\mu\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/q^\nu\mathbb{Z} = 0.$$

We also infer that if the two natural nu,bers satify $\mu \leqslant \nu$ it holds that true that

$$\mathbb{Z}/p^\mu\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/p^\nu\mathbb{Z} \simeq \mathbb{Z}/p^\mu\mathbb{Z}$$

for any prime number p since $(p^\mu, p^\nu) = (p^{\min(\nu,\mu)})$. Together with the formulas from Proposition 5.13 and the Fundamental Theorem for Finitely Abelian Groups, these two formulas make it clear how to compute the tensor product of any pair of finite abelian groups.

The case of free modules

5.19 In the second example we show that the tensor product of two free modules is free.

PROPOSITION 5.20 *Assume that E and F are free A-modules. Then the tensor product $E\otimes_A F$ is free. More precisely, if $\{e_i\}_{i\in I}$ and $\{f_j\}_{j\in J}$ are bases for respectively E and F, the tensors $e_i\otimes f_j$ with $(i,j) \in I \times J$ form a basis for $E\otimes_A F$.*

This proposition holds true regardless of the cardinalities of I and J, but the case when E and F are of finite rank, warrants to be mentioned specially. One may deduce the finite tank case from Proposition 5.13 by a sta esforward induction, however we offer another and simple proof that is generally valid.

COROLLARY 5.21 *If E and F are free A-modules of finite ranks n and m respectively, the tensor product $E\otimes_A F$ is free of rank nm. In particular, for vector spaces V and W of finite dimension over a field k it holds true that* $\dim_k V\otimes_k W = \dim_k V \cdot \dim_k W$.

PROOF OF PROPOSITION 5.20: We contend that the set $\{e_i\otimes f_j\}_{(i,j)\in I\times J}$ is a basis for the tensor product $E\otimes_A F$. As already observed, the elements $e_i\otimes f_j$ form a generating set for$E\otimes_A F$ so we merely have to verify they are linearly independent.

Denote by $a_i(x)$ the i-th coordinate of an element $x \in E$ relative to the basis $\{e_i\}$; that is, one has $x = \sum_i a_i(x)e_i$. Similarily, let $\beta_j(y)$ be the j-th coordinate

of an element $y \in F$. All the $a_i(x)$'s and all the $b_j(y)$'s depend linearly on their arguments.

For each pair of indices $\mu \in I$ and $\nu \in J$ the expression $a_\mu(x)b_\nu(y)$ depends bilinearly on x and y and therefore $x \otimes y \to a_\mu(x)b_\nu(y)$ gives a map $\delta_{\mu\nu} \colon E \otimes F \to A$. This map vanishes on $e_i \otimes f_j$ unless $i = \mu$ and $j = \nu$, and takes the value one on $e_\mu \otimes f_\nu$.

With the $\delta_{\mu\nu}$'s up our sleeve, the rest is a piece of cake: Just apply $\delta_{\mu\nu}$ to a potential dependence relation

$$\sum c_{ij} \cdot e_i \otimes f_j = 0$$

to obtain $c_{\mu\nu} = 0$ for every pair μ and ν of indices. ❑

5.3 *Functorial properties*

5.22 The tensor product functor $- \otimes_A N$ and the functor $\mathrm{Hom}_A(N, -)$ live in a close partnership; they form what is called *a pair of adjoint functors* in the vernacular of homological algebra; that is, there is an identity as in the following proposition:

PROPOSITION 5.23 (ADJOINTNESS) *There is a functorial isomorphism*

$$\mathrm{Hom}_A(M \otimes_A N, L) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, L)).$$

The word "functorial" refers to all three variable. The dependence is covariant in L and contravariant in M and N (A sanity check is that the variances are the same on both sides!). We refrain from diving into the general details afraid of laying a notational smokescreen over the matter which is quit simpe, but in Example 5.1 below we discuss the situation with M being the variabale.
PROOF: The salient point is that $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N, L))$ is canonically isomorphic to the space of bilinear maps $M \times N \to L$; and once one realizes that, the proposition becomes just another reformulation of the Universal Property of the tensor product.

One may think about the members of $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N, L))$ as being maps $\Phi(x, y)$ defined on $M \times N$: When x is a specified member of M, the corresponding map $\Phi(x, -)$ from N to L is given as $y \mapsto \Phi(x, y)$. That $\Phi(x, -)$ is A-linear, means that $\Phi(x, y)$ is linear in y, and that $\Phi(x, -)$ depends linerly on x, means that $\Phi(x, y)$ is linear in x: Hence at the end of the day $\Phi(x, y)$ is *bilinear*!

And that's it: By the Universal Property of the tensor product any such map can be written unambiguously as $\Phi(x, y) = \phi(x \otimes y)$ with a linear map $\phi \colon M \otimes_A N \to L$. ❑

EXAMPLE 5.1 As promised we shall check functoriallity with respect to maps

$\beta\colon M \to M'$; that is, we shall prove the formula

$$\theta_M \circ (\beta \otimes \mathrm{id}_N)^* = \beta^* \circ \theta_{M'}, \tag{5.5}$$

or in other words verify the diagram below commutes, whose vertical maps are the isomorphisms θ_M and $\theta_{M'}$ furnished by Proposition 5.23:

$$\begin{array}{ccc} \mathrm{Hom}_A(M' \otimes_A N, L) & \xrightarrow{(\beta\otimes \mathrm{id}_N)^*} & \mathrm{Hom}_A(M \otimes_A N, L) \\ \downarrow{\scriptstyle \theta_{M'}} & & \downarrow{\scriptstyle \theta_M} \\ \mathrm{Hom}_A(M', \mathrm{Hom}_A(N, L)) & \xrightarrow[\beta^*]{} & \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, L)) \end{array}$$

Now, β^* acts on maps by composition from the right so that $\beta^*(\Phi) = \Phi \circ \beta$. That is, $\beta^*(\Phi)(x, y) = \Phi(\beta(x), y)$, and hence

$$\beta^* \theta_{M'}(\phi)(x, y) = \phi(\beta(x) \otimes y).$$

The same applies to $(\beta \otimes \mathrm{id}_N)^*$ so that $(\beta \otimes \mathrm{id}_N)^*(\phi)(x \otimes y) = \phi(\beta(x) \otimes y)$. And voilà: We find

$$\theta_M(\beta^* \otimes \mathrm{id}_N)\phi(x, y) = \phi(\beta(x) \otimes y),$$

and the two sides of equation (5.5) agree. ☆

PROBLEM 5.2 Convince yourself (along the lines of this example) that the isomorphisms in Proposition (5.23) are functorial in N and L as well. ★

Right exactness

In analogy with the notion of left exactness, which we discussed in connection with the hom-functors, a covariant and additive functor F between two module-categories[1] Mod_A and Mod_B is said to be *right exact* if it transforms exact sequences shaped like

$$M_0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow 0$$

into exact sequences shaped like

$$F(M_0) \longrightarrow F(M_1) \longrightarrow F(M_2) \longrightarrow 0.$$

A fundamental and most useful property of the tensor product is that it is right exact. This section is devoted to giving a proof this, with some easy consequences included atthe end.

[1] Or more generally, between two abelian categories

Right exact functors (Høyre eksakte funktorer)

5.24 Here it comes:

PROPOSITION 5.25 (RIGHT EXACTNESS) *Given a ring A and an A-module N. The functor $-\otimes_A N$ is a right exact functor.*

Our approach relies on Proposition 5.23 above and illustrates the general fact that adjoint functors tend to share exactness properties; if one is exact in some sense, the other tends to be exact in a related sense. It is possible to give a proof of right exactness based on the construction of the tensor product. This is however tedious, cumbersome and not very enlightening, and according to our mantra should be avoided.

Flat modules (*Flate moduler*)

It is common usage to call N a *flat* A-module if the functor $(-)\otimes_A N$ is exact; *i.e.* when it transforms injective maps into injective maps.

PROOF: Let the exact sequence[2]

$$M_\bullet : \; M_0 \xrightarrow{\alpha} M_1 \xrightarrow{\beta} M_2 \longrightarrow 0$$

be given, and the task is to show that the sequence

$$M_\bullet\otimes_A N : \; M_0\otimes_A N \xrightarrow{\alpha\otimes \mathrm{id}_N} M_1\otimes_A N \xrightarrow{\beta\otimes \mathrm{id}_N} M_2\otimes_A N \longrightarrow 0$$

is exact. Our tactics will be to apply the principle of left exactness of the hom-functor as expressed in the proposition called LEFT EXACTNESS II (Proposition 4.61 on page 92), and in fact, we shall do this twice. With that principle in mind, we start out by observing that the sequence $\mathrm{Hom}_A(M_\bullet\otimes_A N, L)$ being exact for every A-module L will be sufficent, and this sequence appears as the upper line in the following grand diagram.

[2] A notation like $M_\bullet$ is commonplace in homological algebra for so-called *complexes*; the bullet indicates a slot where to place indices. A *complex* is a linear sequence of A-linear maps the composition of two consecutive once being zero.

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_A(M_2\otimes_A N, L) & \xrightarrow{(\beta\otimes \mathrm{id}_N)^*} & \mathrm{Hom}_A(M_1\otimes_A N, L) & \xrightarrow{(\alpha\otimes \mathrm{id}_N)^*} & \mathrm{Hom}_A(M_0\otimes_A N, L) \\
 & & \wr\downarrow \theta_{M_2} & & \wr\downarrow & & \wr\downarrow \\
0 & \longrightarrow & \mathrm{Hom}_A(M_2, \mathrm{Hom}_A(N, L)) & \xrightarrow[\beta^*]{} & \mathrm{Hom}_A(M_1, \mathrm{Hom}_A(N, L)) & \xrightarrow[\alpha^*]{} & \mathrm{Hom}_A(M_0, \mathrm{Hom}_A(N, L))
\end{array}$$

The next step is to evoke Proposition 5.23 above and replace the complex $\mathrm{Hom}_A(M_\bullet\otimes_A N, L)$ with $\mathrm{Hom}_A(M_\bullet, \mathrm{Hom}_A(N, L))$; the latter is displayed as the bottom line of the grand diagram. The crux of the proof is that this latter sequence is exact, again by LEFT EXACTNESS II, so once we know that the two rows in the grand diagram are isomorphic (as sequences) we are through. But indeed, they are since with the vertical maps being the canonical isomorphisms from Proposition 5.23 (ADJOINTNESS), the two squares commute according to Example 5.1 above. ❑

5.26 Proposition 5.17 on page 107 describes the tensor product of two cyclic module. An analogous result holds true with just one of the modules being cyclic while the other can be arbitrary:

PROPOSITION 5.27 *Let $\mathfrak{a}\subseteq A$ be a an ideal and M and A-module. Then one has a canonical isomorphism $M\otimes_A A/\mathfrak{a} \simeq M/\mathfrak{a}M$ that sends $m\otimes[a]$ to $[am]$.*

PROOF: The starting point is the exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0,$$

which when tensorized by M, yields the exact sequence

$$\mathfrak{a}\otimes_A M \xrightarrow{\alpha} M \longrightarrow M\otimes_A A/\mathfrak{a} \longrightarrow 0,$$

because the tensor product is right exact. The map α sends $a\otimes x$ to ax, hence its image is equal to $\mathfrak{a}M$, and we are done. ❑

Example 5.2 Be aware that the tensor product can be a bloodthirsty killer. Injective maps may cease being injective when tensorized, and they can even become zero. The simplest example is multiplication by an integer n, that is; the map $\mathbb{Z} \to \mathbb{Z}$ that sends x to nx. It vanishes when tensorized by $\mathbb{Z}/n\mathbb{Z}$. This also illustrates the fact that the functor $-\otimes_A N$ is not always exact, even though always being right exact. In this example the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

is transformed into the exact sequence (right exactness of $\otimes$)

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{0} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\beta} \mathbb{Z}/n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

where β must be an isomorphism—its kernel is zero since the sequence is exact. So part of the conclusion is that $\mathbb{Z}/n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$ which as well ensues from Proposition 5.17 on page 107. ☆

5.28 Even whole modules may succumb under the action of tge tensor product; for instance, we saw that $\mathbb{Z}/p\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/q\mathbb{Z} = 0$ when p and q are relatively prime integers, which illustrates a general fact. Recall that an A-module M is *divisible* by an element $a \in A$ if the multiplication map $M \to M$ is surjective; in other words every $x \in M$ may be written as ax' for some $x' \in M$.

Proposition 5.29 *Let $a \in A$ and assume that M and N are A-modules such that M is divisible by a and $a \in \operatorname{Ann} N$, then $M\otimes_A N = 0$.*

Proof: The short argument goes like this. Every $x \in M$ is of the form ax' for some $x' \in M$, so that $x\otimes y = ax'\otimes y = x'\otimes ay = 0$, and as the decomposable tensors generate $M\otimes_A N$ we are through. ❑

Problems

5.3 Compute $\mathbb{Z}/16\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/36\mathbb{Z}$ and $(\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/15\mathbb{Z})\otimes_{\mathbb{Z}}(\mathbb{Z}/21\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z})$. ✲

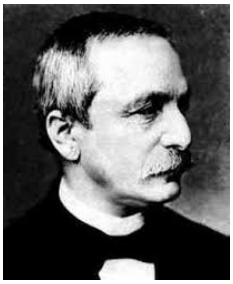
5.4 Let A be a ring and M an A-module. Show that $M\otimes_A A/\operatorname{Ann} M = M$. Show that if N is a second A-module and the annihilators $\operatorname{Ann} M$ and $\operatorname{Ann} N$ are comaximal ideals, then $M\otimes_A N = 0$. ✲

5.5 Show that $\mathbb{Q}/\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q} = 0$. Show that one has $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Q} \simeq \mathbb{Q}$, but that $\mathbb{Q}/\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q}/\mathbb{Z} = 0$. Hint: Proposition 5.29. ✲

5.6 Let $\mathfrak{a}$ be a proper ideal in the ring A. Assume that M is an A-module for which there is surjection $M \to A/\mathfrak{a}$. Show that $\mathfrak{a}M \neq M$.

5.7 Let M be finitely generated module over the ring A: Show that $M^{\otimes n} \neq 0$ for any natural number n. Hint: Exhibit a surjective map $M \to A/\mathfrak{p}$. Proceed by induction on n and right exactness of the tensor product. ✲

5.8 *(The Kronecker product.)* Let $\phi\colon E \to F$ and $\psi\colon G \to H$ be two A-linear maps between free A-modules of finite rank. Let $\{e_i\}_{i\in I}$, $\{f_j\}_{j\in J}$, $\{g_k\}_{k\in K}$ and $\{h_l\}_{l\in L}$ be bases of E, F, G and H respectively, and let the matrices of ϕ and ψ in the appropriate bases be Φ and Ψ. Show that the matrix of $\phi\otimes\psi$ in the bases $\{e_i\otimes f_j\}_{(i,j)\in I\times J}$ and $\{g_k\otimes h_l\}_{(k,l)\in K\times L}$ is given as the matrix $(\Phi_{ij}\Psi_{kl})$ with rows indexed by pairs $(i,j) \in I\times J$ and colums by $(k,l) \in K\times L$. This matrix is called the *Kronecker product* of Ψ and Φ.



Leopold Kronecker (1823–1891) German mathematician

The Kronecker product (*Kronecker-produktet*)

5.9 Assume that G is a finite abelian group. Show that $G\otimes_{\mathbb{Z}}\mathbb{Q} = 0$. ✲

5.10 Let A be a domain contained in a field K and let M be an A-module. Assume that $\operatorname{Ann} M \neq (0)$. Prove that $K\otimes_A M = 0$. ✲

5.11 Let $A \to B$ be a surjective ring homomorphism. Show that for any two B-modules M and N (which automatically are A-modules) it holds true that $M\otimes_A N = M\otimes_B N$. ✲

5.12 Show that $\mathbb{Z}[i]\otimes_{\mathbb{Z}}\mathbb{Z}[i]$ is a free abelian group of rank 4 while $\mathbb{Z}[i]\otimes_{\mathbb{Z}[i]}\mathbb{Z}[i] = \mathbb{Z}[i]$ and is of rank two as an abelian group. ✲

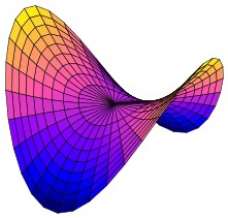
5.13 Merely in a very few highly special cases will all elements in a tensor product be decomposable; the commonplace situation is that most are not. A simple example is $W = V\otimes_k V$ where V is a two-dimensional vector space over k. Let $\{e_1, e_2\}$ be a basis for V. The tensor product W is of dimension four with a basis $\{e_i\otimes e_j\}$ where $1 \leqslant i, j \leqslant 2$. Let x_i be coordinates relative to this basis; that is, any vector v is expressed as $v = x_1\cdot e_1\otimes e_1 + x_2\cdot e_1\otimes e_2 + x_3\cdot e_2\otimes e_1 + x_4\cdot e_2\otimes e_2$,

a) Establish that he decomposable tensors are shaped like

$$(ue_1 + ve_2)\otimes(se_1 + te_2) = us\cdot e_1\otimes e_1 + ut\cdot e_1\otimes e_2 + vs\cdot e_2\otimes e_1 + vt\cdot e_2\otimes e_2,$$

with u, v, s and t being scalars.

b) Show that the decomposable tensors are precisely those lying on the subset $x_1x_4 - x_2x_3 = 0$.



c) In the real case, that is when $k = \mathbb{R}$, convince youself that this locus is the cone in $\mathbb{R}^4$ with apex the origin over a saddle-surface in $\mathbb{R}^3$; *i.e.* one given as $z = xy$ (or in our coordinates $x_3 = x_1x_2$).

5.14 *(The rank stratification.)* Let V be a vector space over a field k of finite dimension. The dual space $V^* = \mathrm{Hom}_k(V,k)$ consists of linear functionals on V and is a vector space of the same dimension as V. Chose a basis $\{e_i\}$ for V and let $\{\phi_i\}$ be the *dual* basis for V^*. That is, the functionals ϕ_i are defined as $\phi_i(e_j) = 0$ when $i \neq j$ and $\phi_i(e_i) = 1$.

a) Let W be a second vector space of finite dimension over k with basis $\{f_j\}$. Prove that the assignment $\phi \otimes w$ to $v \mapsto \phi(v)w$ induces an isomorphism $\Gamma\colon V^* \otimes_k W \xrightarrow{\simeq} \mathrm{Hom}_k(V,W)$.

b) Given a linear map $\theta\colon V \to W$ whose matrix relative to the bases $\{e_i\}$ and $\{f_j\}$ is (a_{ij}). Show that the element in $V^* \otimes W$ corresponding to θ equals $\sum_i \phi_i \otimes \theta(e_i)$ and that $\sum_i \phi_i \otimes \theta(e_i) = \sum_{ij} a_{ij}\phi_i \otimes f_j$.

c) Show that the non-zero decomposable tensors in $V^* \otimes_k W$ under the map Γ correspond to the linera maps of rank one. HINT: Chose an appropriate basis for V.

d) Show that a linear map in $\mathrm{Hom}_k(V,W)$ is of at most rank r if and only if the corresponding tensor in $V^* \otimes W$ is the sum of at most r decomposable tensors. HINT: Chose an appropriate basis for V

5.4 *Change of rings*

A commonplace application of the tensor product is to change the ground ring.

Suppose that B is an A-algebra. In particular B has an A-module sructure, and consequently we may form the tensor product $M \otimes_A B$ of B with any A-module M. Now, the point is that one may multiply elements in $M \otimes_A B$ by elements from B "in the second variable", and in that way produce a B-module structure on the tensor product $M \otimes_A B$. Indeed, if $b \in B$ the "multiplication by b map" $x \mapsto bx$ is an A-linear map $[b]\colon B \to B$, and therefore induces a map $\mathrm{id}_M \otimes [b]$ on the tensor product. Its action on a tensor t will we denoted $b \cdot t$ or simply bt, and on decomposable tensors it acts as $b \cdot x \otimes c = x \otimes bc$. Checking the module axioms is straightforward (for free from functoriality of $- \otimes_A B$), and in view of the tensor product being additive (Proposition 5.10 on page 104) and right exact (Proposition 5.25 on page 110) we arrive at

PROPOSITION 5.30 *Given an A-algebra B. The the change-of-rings-functor, which sends M to $M\otimes_A B$, is a right exact additive functor $-\otimes_A B\colon \mathsf{Mod}_A \to \mathsf{Mod}_B$.*

5.31 Notice, that elements in B coming from A may be moved past the $\otimes$-sign; *i.e.* if the structure map is $u\colon A \to B$ one has $x\otimes ab = ax\otimes b$. Be aware however, there is a hidden pitfall. For any $b \in B$ the notation $a \cdot b$ is a sloppy version of the correct notation $u(a) \cdot b$, where the product is the product in the ring B. Hence $ax\otimes b = x\otimes u(a)b$ would be the correct way of writing.

This leads to equalities like $a(x\otimes b) = u(a)(x\otimes b)$ where on the left side $M\otimes_A B$ is considered an A module (through the left factor) and on the right a B-module (through the right factor).

Transitivity and adjointness

5.32 Sometimes one wants to perform consecutive base changes, and the tensor product behaves well in such a situation. It is transitive in the following sense.

PROPOSITION 5.33 (TRANSITIVITY) *Assume that B is an A-algebra and C is a B-algebra. Then there is a canonical isomorphism $(M\otimes_A B)\otimes_B C \simeq M\otimes_A C$ as C-modules.*

PROOF: The short description of the maps are $m\otimes x\otimes y \mapsto m\otimes xy$ and $m\otimes z \mapsto m\otimes 1\otimes z$. By the principles of bi- and tri-linearity both extend to maps between the tensor products, and they act as mutually inverses on the decomposable tensors. Hence the are mutually inverse maps. ❑

5.34 Changing the base ring preserves tensor products, but not hom-modules in general. One has the following:

PROPOSITION 5.35 *Let B be an A algebra and M and N two A-modules. Then there is a canonical isomorphism of B-modules*

$$(M\otimes_A N)\otimes_A B \simeq (M\otimes_A B)\otimes_B (N\otimes_A B).$$

In other words, the functor $(-)\otimes_A B$ takes tensor products into tensor products.

PROOF: Two mutually inverse B-module homomorphisms are defined by the assignments

$$x\otimes y\otimes b \mapsto x\otimes 1\otimes y\otimes b$$
$$x\otimes y\otimes bb' \leftarrow\!\shortmid\, x\otimes b\otimes y\otimes b'$$

of decomposable tensors. The obey respectively a tri-linear and a quadri-linear requirement and thereby define genuine maps between the modules. ❑

5.36 In a base change situation there are two natural functors between the two module categories. In addition to the base change functor, given as the

tensor product $(-)\otimes_A B\colon \mathsf{Mod}_A \to \mathsf{Mod}_B$, there is a functor going the other way: $(-)_A\colon \mathsf{Mod}_B \to \mathsf{Mod}_A$. The action of this functor is kind of trivial. If N is a B-module, N_A is equal to N but regarded as an A-module—one forgets the B-module structure. With maps the same happens; they are kept intact, but merely regarded as being A-linear. Such functors that "throws away" part of the structure, are called *forgetful functors* in the parlance of the category theory.

The point is that the tensor product $(-)\otimes_A B$ and the forgetful functor $(-)_A$ are adjoint functors:

PROPOSITION 5.37 (ADJOINTNESS) *Given an A-algebra B. Then there is a canonical isomorphism*

$$\mathrm{Hom}_B(M\otimes_A B, N) \simeq \mathrm{Hom}_A(M, N_A).$$

PROOF: The from left two right is simply a "restriction" map. It sends a given B-linear map $\phi\colon M\otimes_A B \to N$ to $\phi(x\otimes 1)$ which is A-linear in x. To define a map from the right side to the left side, let $\phi\colon M \to N_A$ be A-linear. The expression $\psi(x\otimes b) = b\phi(x)$ is A-bilinear and by the universal property enjoyed by the tensor product it extends to an A-linear map $\psi\colon M\otimes_A B \to N$ which turns out to be B-linear (remember, multiplication by elements from B is performed in the right factor):

$$\psi(b'\cdot x\otimes b) = \psi(x\otimes bb') = bb'\phi(x) = b'\cdot\psi(x\otimes b).$$

At last and as usual, the two maps are inverses to each other, since they are when acting on decomposable tensors. ❑

Maps between free modules and base change

The tensor product being an additive functor, it is clear that the change-of-ring-functors transforms free modules into free modules; indeed, if $E \simeq nA$ with a basis $\{e_i\}$ corresponding to the standard basis $\{\epsilon_i\}_i$ of nA, it holds true that $E\otimes_A B \simeq nB$ with a basis $\{e_i\otimes 1\}_i$ corresponding to the standard basis $\{\epsilon_i\}_i$ (as a basis for nB this time).

5.38 It is of interest to know how changing the base ring affects maps between free modules and how their associated matrices change. So let F be a second free A-module of rank m with a basis $\{f_j\}$ and suppose further that $\phi\colon E \to F$ is an A-linear map. Recall that the entires of the matrix $\Phi = (a_{ij})$ associated with ϕ are the coefficients in the developments

$$\phi(e_i) = \sum_j a_{ji} f_j$$

of $\phi(e_i)$ in terms of the basis elements f_j. Applying $\phi\otimes\mathrm{id}_B$ to the basis element $e_i\otimes 1$, yields

$$\phi\otimes\mathrm{id}_B(e_i\otimes 1) = \phi(e_i)\otimes 1 = (\sum_j a_{ji} f_j)\otimes 1 = \sum u(a_{ji})\cdot f_j\otimes 1$$

where $u\colon A \to B$ denotes the structure maps as in paragraph 5.31 above. Hence the matrix of $\phi\otimes\mathrm{id}_B$ is the matrix $(u(a_{ji}))$ obtained by applying the structure map u to the entries of (a_{ji}).

EXAMPLE 5.3 As an example we consider the polynomial ring $A = \mathbb{C}[x]$ and let $a \in \mathbb{C}$ be a complex number. Furthermore, we let $B = \mathbb{C}[x]/(x-a) \simeq \mathbb{C}$, so that the structure map u is the evaluation at a; *i.e.* $u(P(x)) = P(a)$. If ϕ is a map between two free $\mathbb{C}[x]$-modules with matrix $P = (P_{ij}(x))$ relative to some bases, the matrix of $\phi\otimes\mathrm{id}_{\mathbb{C}}$ is just the matrix P evaluated at a; that is, the matrix $(P_{ij}(a))$. ☆

EXAMPLE 5.4 For a second example, take $A = \mathbb{Z}$ and $B = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ for some prime number p. If ϕ is a map between two free abelian groups whose matrix relative to some bases is (n_{ij}), the matrix of $\phi\otimes\mathrm{id}_{\mathbb{F}_p}$ relative to the corresponding bases will be $([n_{ij}])$ (where $[n]$ as usual denotes the congruence class of an integer n modulo p).

On the other hand, changing the ring from $\mathbb{Z}$ to $\mathbb{Q}$; that is, passing to the map $\phi\otimes\mathrm{id}_{\mathbb{Q}}$, does not change the matrix. We merely consider the integers n_{ij} as being rational numbers! ☆

EXAMPLE 5.5 Our third example is of a rather different flavour than the two previous ones. This time we let A be a ring of characteristic p; that is, we assume it contains the prime field $\mathbb{F}_p$. The Frobenius map $a \to a^p$ is then a ring homomorphism $A \to A$ and gives A an alternative A-algebra structure in which $a \cdot x = a^p x$ (the product to the left is the *new* product, whereas the one to the right is the original product in A). In view of the considerations above, a ring-change via the Frobenius map, changes matrices of A-linear maps between free A- modules by rising their entries to the p-th power. ☆

5.5 *Tensor products of algebras*

Setting the stage of this section we let C and introduce two C-algebras A and B. The star of the show will be the tensor product $A\otimes_C B$ and the objective of the play is to give a ring structure compatible with its underlying C-module structure, thus making it a C-algebra.

5.39 On decomposable tensors the product ought to abide by the rule

$$a\otimes b \cdot x\otimes y = ax\otimes by, \tag{5.6}$$

and indeed, this extends to a product on $A\otimes_C B$:

PROPOSITION 5.40 *Given a ring C and two C-algebras A and B. Then there is a unique C-algebra structure on $A\otimes_C B$ whose product on decomposable tensors satisfies $a\otimes b \cdot a'\otimes b' = aa'\otimes bb'$.*

Notice that the C-module structure on $A\otimes_C B$ is in pace *a priori* being the induced structure on the tensor product, so merely the ring structure is lacking.

PROOF: To argue that the assignment of (5.6) can be extended to give a product of arbitrary tensors, we once more we appeal to the principle of bilinearity (at the end of paragraph 5.2 on page 103). In fact, we shall apply it twice—once for each factor—the basic observation being that the right side of (5.6) is C-bilinear both in (a, b) and (x, y)

The first application of the principle shows that multiplication by a fixed pair (a, b) extends to a C-linear map $A\otimes_C B \to A\otimes_C B$. This yields a map

$$\eta_0 \colon A \times B \to \mathrm{Hom}_C(A\otimes_C B, A\otimes_C B)$$

that sends (a, b) to the multiplication-by-$a\otimes b$-map; that is, it holds that $\eta_0(a, b)(\sum_i x_i\otimes y_i) = \sum_i ax_i\otimes by_i$. In its turn, this map depends bilinearly on the pair (a, b), and by a second application of the principle we arrive at a C-linear map

$$\eta \colon A\otimes_C B \to \mathrm{Hom}_C(A\otimes_C B, A\otimes_C B),$$

which on decomposable tensors behave as desired; *i.e.* $\eta(a\otimes b)(x\otimes y) = ax\otimes by$. Subsequently we define the product of two arbitrary tensors s and t as $s \cdot t = \eta(t)(s)$. This establishes the product in $C\otimes_A B$, but there are verifications to be done.

That the ring axioms hold, is a matter of straightforward verifications —they follow by the uniqueness parts of the principles of bilinearity and trilinearity. For example, both expressions $\eta(t)(s)$ and $\eta(s)(t)$ are bilinear in s and t and since they agree on decomposable tensors, they are equal, so that the product is commutative. One checks associativity in a similar manner, but by using the Trilinearity Principle (Lemma 5.15 on page 106). The two expressions $\eta(tu)(s)$ and $\eta(t)(us)$ are both linear in each of the variables s, t and u, and agreeing on decomposable tensors, they coincide; that is, $(t \cdot u) \cdot s = t \cdot (u \cdot s)$. ❑

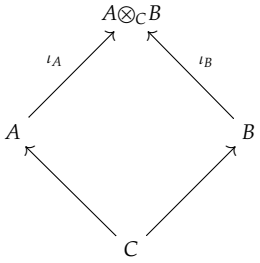
The universal property

The tensor product $A\otimes_C B$ enjoys a universal property that plays a paramount role in algebraic geometry. It reflects the geometric construction of so called fibre products; the simple variant being the product $X \times Y$ of two schemes. This is a foundational construct on which the whole theory rest.

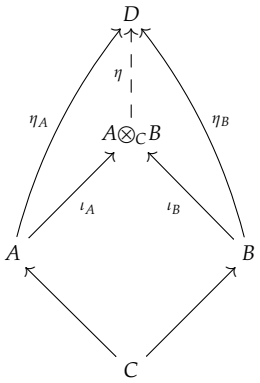
5.41 With the setting as in the previous section, there are two canonical C-algebra homomorphisms having target $A\otimes_C B$; one with A as source and the other sourced at B.

The first, call it ι_A, is given as $a \mapsto a\otimes 1$ and the second, call it ι_B, as $b \mapsto 1\otimes b$. Elements from C may be moved past the tensor product sign so that $c\otimes 1 = 1\otimes c$ for $c \in C$; or expressed in terms of a diagrams: The upper diagram in the margin commutes. (Where the maps $C \to A$ and $C \to B$ are the structure maps defining the C-algebra structures.)

The tensor product is universal among C-algebras living in such diagrams:



Proposition 5.42 (The universal property) *With the notation as just introduced, assume given a C algebra D and two C-algebra homomorphisms $\eta_A\colon A \to D$ and $\eta_B\colon B \to D$. Then there is a unique map of C-algebras $A\otimes_C B \to D$ such that $\eta\circ\iota_A = \eta_A$ and $\eta\circ\iota_B = \eta_B$.*



Proof: Indeed, the expression $\eta_A(a)\eta_B(b)$ is C-bilinear, and according to the universal property of the tensor product it gives rise to a C-linear map $A\otimes_C B \to D$ satisfying $\eta(a\otimes b) = \eta_A(a)\eta_B(b)$. This is our desired map, but some checking remains to be done. Let us begin with verifying that η respects products. Since e know η is linear, it will suffice to do this for decomposable tensors:

$$\eta(aa'\otimes bb') = \eta_A(aa')\eta_B(bb') = \eta_A(a)\eta_A(a')\eta_B(b)\eta_B(b') = \eta(a\otimes b)\eta(a'\otimes b')$$

where the two extreme equalities hold true by the very definition of η, and the middle one because both η_a and η_B are ring maps.

Next, one has $\eta\circ\iota_A = \eta_A$ and $\eta\circ\iota_B = \eta_B$ since $\eta_A(1) = \eta_B(1) = 1$, and finally, that η is unique follows, since it is determined by the values on decomposable tensors, and these satisfy

$$\eta(a\otimes b) = \eta((a\otimes 1)(1\otimes b)) = \eta(a\otimes 1)\eta(1\otimes b) = \eta_A(a)\eta_B(b)$$

❑

Polynomial rings

We continue with the stage set as above, with B being an A-algebra through the structure map $u\colon A \to B$. In the name of the inherent human laziness, we shall write $A[x_\bullet]$ for a polynomial ring $A[x_1,\dots,x_r]$.

5.43 A natural question is how polynomial rings behave under base change, and the answer is they do in the obvious and simplest way.

There is a map of A-algebras $A[x_1,\dots,x_r] \to B[x_1,\dots,x_r]$ sending x_i to x_i (hence a polynomial $\sum_\alpha a_\alpha x^\alpha$ maps to $\sum_\alpha u(a_\alpha)x^\alpha$). Together with the inclusion of B as the constants in $B[x_1,\dots,x_r]$ it induces, in view of the universal property of the tensor product, a map of A-algebras $A[x_1,\dots,x_r]\otimes_A B \to B[x_1,\dots,x_r]$. It sends the variable to the variables, and gives an isomorphism:

Recall the notation from Paragraph 1.16 on page 15 where the monomial $x_1^{\alpha_1}\cdot\ldots\cdot x_r^{\alpha_r}$ was denoted by x^α, with α being the multi-index $(\alpha_1,\dots,\alpha_r)$.

Lemma 5.44 *Let A be a ring and B be an A-algebra. Then $A[x_1,\dots,x_r]\otimes_A B = B[x_1,\dots,x_r]$*

Proof: Considered as A-module, the polynomial ring $A[x_1,\dots,x_r]$ is free, and the monomials x^α, with α running through all multi-indices, form a basis. The same holds for $B[x_1,\dots,x_r]$; the monomials x^α form a B-basis.

According to what we figured out in Paragraph 5.36 on page 116 the elements $x^\alpha \otimes 1$ form a B basis for $A[x_1,\dots,x_r]\otimes_A B$; but our map sends these to x^α which form a basis for $B[x_1,\dots,x_r]$. ❑

LEMMA 5.45 *Let $\mathfrak{a}\subseteq A[x_1,\dots,x_r]$ be an ideal. Then $A[x_1,\dots,x_r]/\mathfrak{a}\otimes_A B = B[x_1,\dots,x_r]/\mathfrak{a}B[x_1,\dots,x_r]$*

Suppose that $\mathfrak{a}$ is generated by a collection $\{f_i\}$ of polynomials. Then $\mathfrak{a}B[x_1,\dots,x_r]$ will be generated by the images of f_i's under the natural map $A[x_1,\dots,x_r]\to B[x_1,\dots,x_r]$ that is the polynomials obtained by applying the structure map u to coefficients.

In several context, when *e.g.* u is a canonical inclusion; like $\mathbb{Z}\subseteq\mathbb{Q}$ or $\mathbb{Q}\subseteq\mathbb{C}$, the effect is nil, one just considers the generators as being members of $B[x_1,\dots,x_r]$. However, in other situations the effect on f_i's can be dramatic, in the worst case they can even vanish! For examples this occurs if the structure map is the reduction mod p-map $u\colon\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p$ and the coefficients of $f_i\in\mathbb{Z}[x]$ are all divisible by p.

EXAMPLE 5.6 A particular application of the previous lemma is that the tensor product of two polynomial rings (over the base ring) again is a polynomial ring. If case both rings are polynomial rings in one variable, one has $A[x]\otimes_A A[y]=A[x,y]$, and in general it holds true that

$$A[x_1,\dots,x_r]\otimes_A A[y_1,\dots,y_s]=A[x_1,\dots,x_r,y_1,\dots,y_s].$$

Polynomials give a striking example that the decomposable tensors are scarce. In $A[x,y]$ for instance, the decomposable tensors are the polynomials that factor as $p(x)q(y)$ of which there are few. ☆

EXAMPLE 5.7 Be aware that the tensor product of two integral domains need not be an integral domain. Even if both factors are fields, the tensor product might acquire zero-divisors. A simple example is $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$. The complex numbers $\mathbb{C}$ can be described as the quotient $\mathbb{R}[x]/(x^2+1)$ so by Lemma 5.45 above it holds that $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}=\mathbb{C}[x]/(x^2+1)$. This latter ring is isomorphic to the direct product $\mathbb{C}\times\mathbb{C}$, sending the residue class of a polynomial $p(x)$ to the pair $(p(i),p(-i))$ yields an isomorphism, and the direct product has many zero divisors. ☆

Problems

5.15 Let k be a field and let $f(x)$ be an irreducible polynomial in $k[x]$ so that $K=k[x]/(f(x))$ is field. Moreover let L be field extension of k over which f splits as a product $f(x)=f_1(x)\dots f_r(x)$ of irreducible polynomials. Use the Chinese remainder theorem to prove that $K\otimes_k L\simeq\prod L_i$ where L_i is the field $L_i=L[x]/(f_i(x))$. ✲

5.16 Assume that K is an algebraic number field; *i.e.* a finite extension of the field $\mathbb{Q}$ of rational numbers. Show that $K \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to a product of fields each being isomorphic either to $\mathbb{R}$ or $\mathbb{C}$. Show that $[K : \mathbb{Q}] = r_1 + 2r_2$ where r_1 denotes the number of factors isomorphic to $\mathbb{R}$ and r_2 the number of factors isomorphic to $\mathbb{C}$. HINT: By the Primitive Element Theorem one may assume that $K = \mathbb{Q}[x]/(f(x))$ where $f(x) \in \mathbb{Q}[x]$ is irreducible polynomial. ✳

5.17 Show that $A = \mathbb{R}[x, y]/(x^2 + y^2)$ is an integral domain, but that $A \otimes_{\mathbb{R}} \mathbb{C}$ is not. ✳

5.18 Let $\phi \colon A \to B$ be a ring homomorphism and $\mathfrak{p} \subseteq A$ a prime ideal. Show that the fibre of $\phi^* \colon \operatorname{Spec} B \to \operatorname{Spec} A$ over $\mathfrak{p}$ is naturally homeomorphic to $\operatorname{Spec} A/\mathfrak{p} \otimes_A B$.

5.19 Let K be a field of positive characteristic p and let $t \in K$ be an element which is not a p-th power. Show that $L = K[x]/(x^p - t)$ is a field and that $L \otimes_K L$ has non-trivial nilpotent elements.

5.20 Let k be a field of positive characteristic p, and let $\mathfrak{a}$ be an ideal in $A = k[x_1, \ldots, x_r]$ generated by polynomials $f_i(x) = \sum_\alpha a_{i\alpha} x^\alpha$. Let $F \colon k \to k$ be the Frobenius map $a \mapsto a^p$; and let k_F denote the field k endowed with the k-algebra structure induced by the Frobenius map; that is, members a of k act on k_F as $a \cdot x = a^p x$, Show that $(k[x_1, \ldots, x_r]/\mathfrak{a}) \otimes_k k_F \simeq k[x_1, \ldots, x_r]/\mathfrak{a}_F$ where $\mathfrak{a}_F$ is the ideal generated by the polynomials $f_i = \sum_\alpha a_{i\alpha}^p x^\alpha$

5.21 Let $\bar{\mathbb{C}}$ be $\mathbb{C}$ equipped with the alternative algebra structure induced by complex conjugation; *i.e.* $a \cdot z = \bar{a}z$. Let $f(x) \in \mathbb{C}[x]$ be a polynomial. Describe $\mathbb{C}[x]/(f(x)) \otimes_{\mathbb{C}} \bar{\mathbb{C}}$. When are the $\mathbb{C}$-algebras $\mathbb{C}[x]/(f(x)) \otimes_{\mathbb{C}} \bar{\mathbb{C}}$ and $\mathbb{C}[x]/(f(x))$ isomorphic?

★

Changes:

2018-09-23 Have reworked almost everything until section 5.4; not yet finished.

05/10/2018 Reworked the last part about tensor products of algebras.

07/10/2018 Added an exercise, corrected lots of misprints and minor errors.

08/10/2018 Have rewritten the proof of Proposition 5.23 about Adjointness on page 109 and the subsequent example with substantial simplifications.

10/10/2018 Have added a prop about tensor prods and bases change; prop 5.35 on page 115.

11/10/2018 Added Exercise 5.6 on page 113

18/10/2018 Corrected misprints, minor changes in the text.

22/10/2018 Minor changes of the language.

Lecture 6

Localization

Preliminary version 2.0 as of 2018-10-22 at 09:43 (typeset 3rd December 2018 at 10:03am)—Prone to misprints and errors and will change.
28/10/2018 Added new exercise 6.6

Very early in our mathematical carrier, if not in our lives, we were introduced to *fractions*, and we should be familiar with their construction. Anyhow, recall that to every pair of integers m and n with $n \neq 0$, one forms the "fraction" m/n with m being the enumerator and n the denominator. Two such fractions m'/n' and m/n are considered equal—that is, have the same numerical value—precisely when $nm' = n'm$. The fractions—or the rational numbers as we call them—are entities *per se* and not only results of division. They obey the rules for adding and multiplying we learned in school—that is, the field axioms—and they thus form a field $\mathbb{Q}$.

There is a simple and very general version of this construction. It gives us the freedom to pass to rings were *a priori* specified elements become invertible. Virtually any set of elements can be inverted; there is merely one natural constraint. If s and t occur as denominators, their product st will as well; indeed, one has $s^{-1}t^{-1} = (st)^{-1}$. Hence the natural notion to work with is the concept of *multiplicatively closed sets*.

The process is indeed very general. It even accepts zero-divisors as denominators, but can then be "murderous". If a is a zero-divizor, say $a \cdot b = 0$, and a becomes inverted, b gets killed; indeed, it will follow that $b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$. In principle, one can even push this so far that 0 is inverted; but this will be devastating and the resulting ring not very interesting, it will be the null-ring.

There are several ways of defining the localized rings. We shall follow most text books and mimic the way one constructed the rational numbers. This is a direct and intuitive construction not requiring much machinery.

The name "localization" has its origin in geometry and rings of functions, say on a topological space X. If $U \subseteq X$ is an open set, every function whose zeros all lie in the complement $X \backslash U$ of U, become invertible when restricted to U; hence one obtains many functions on U by inverting certain functions on X. In general far from all are shaped like that, but in special situations, important

in algebraic geometry, all algebraic functions on U arise in this way.

6.1 *Localization of rings*

We start out with introducing the notion of multiplicatively closed sets, and proceed to the construction of the localized rings. They will be characterized by a universal property. Core examples will be given, and the basic properties of localized rings will be established, notably the relation between ideals in the ring A and ideals in the localizations A_S.

Multiplicatively closed sets (*Multiplicativt lukkede mengder*)

6.1 Rrecall that a subset $S \subseteq A$ is *multiplicatively closed*, or for short a *multiplicative set*, if it contains the unit element and the product of any two elements from S belongs to S. That is, the following two conditions are satisfied

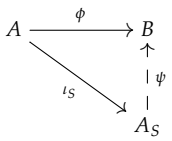
- $1 \in S$;
- If $s, t \in S$, then $st \in S$.

6.2 We mention two important examples. If a is any element in A the set $S = \{ a^n \mid n \in \mathbb{N}_0 \}$ of all the powers of a is obviously multiplicatively closed. Secondly, the complement $S = A \backslash \mathfrak{p}$ of any *prime ideal* $\mathfrak{p}$ in A is multiplicatively closed as well; indeed, from $st \notin S$ ensues that $st \in \mathfrak{p}$ and at least one of the factors s or t belongs to $\mathfrak{p}$; that is, it does not lie in S.

6.3 It is fairly clear that the intersection of two multiplicatively closed sets is multiplicatively closed, and one can speak about the *the multiplicative set generated* by a subset T of A. It equals the intersection of all multiplicatively closed sets containing T, and one convinces oneself on the spot that the elements are all finite products of elements from T. So for example, the multiplicative set in $\mathbb{Z}$ generated by 2 and 5 consists of all numbers of the form $2^a 5^b$, with $a, b \in \mathbb{N}_0$.

The universal property

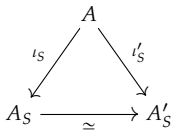
6.4 The localized ring A_S comes together with a ring homomorphism $\iota_S \colon A \to A_S$ such that all the images $\iota_S(s)$ of elements s from S are invertible, and moreover, the map ι_S is universal in this respect. This means the following:



- Any map of rings $\phi \colon A \to B$ sending members of S to invertible elements, factors through ι_S in a unique manner; *i.e.* one has $\phi = \psi \circ \iota_S$ for an unambiguously defined map of rings $\psi \colon A_S \to B$.

In the sequel we shall mostly suppress the reference to the map ι_S and just write a for $\iota_S(a)$. This calls however for a word of warning: The map ι_S is not always injective! Membres of A killed by elements from S become zero in A_S; indeed, from $as = 0$ follows $\iota_S(a)\iota_S(s) = 0$, and $\iota_S(s)$ being invertible forces $\iota_S(a) = 0$.

As any other objects characterised by a universal property, the pair ι_S and A_S is unique up to an unambiguous isomorphism; if $\iota'_S\colon A \to A'_S$ solves the same universal problem, one has $\iota'_S = \psi \circ \iota_S$ for a unique $\psi\colon A_S \to A'_S$.



The construction of the localization A_S

6.5 The construction of the localized ring A_S follows *grosso modo* the same lines as the construction of the rational numbers, but there is a necessary twist to it due to the possible presence of zero divisors in S with the consequence that the cancellation law does not necessarily hold.

6.6 A fraction has an enumerator and a denominator, and the latter is confined to S. A natural starting point is therefore the product $A \times S$ with the first factor representing the enumerators and the second the denominators. The next step is to introduce an equivalence relation on $A \times S$ telling when two fractions are to be considered equal, and inspired by the case of classical fractions, we declare the pairs (a, s) and (b, t) to be equivalent when for some $u \in S$, it holds true that $u(at - bs) = 0$. In that case we temporarily write $(a, s) \sim (b, t)$.

This relation is obviously reflexive and a symmetric. To see it is transitive, assume given three pairs (a, s), (b, t) and (c, u) such that $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$; transcribing the equivalences into equalities in A, we find that $v(at - bs) = 0$ and $w(bu - ct) = 0$ for some elements $v, w \in S$. Since

$$t(au - cs) = u(at - bs) + s(bu - ct),$$

we infer that

$$vwt(au - cs) = wu(v(at - bs)) + sv(w(bu - ct)) = 0.$$

From S being multiplicatively closed it ensues that $vwt \in S$, and so $(a, s) \sim (c, u)$.

6.7 Now, we let A_S be the set of equivalence classes $A \times S/\sim$, and we denote by a/s or as^{-1} the class of the pair (a, s). The next task is to give a ring structure to A_S, and there is no hocus-pocus about that; it is done by the familiar formulas for adding and multiplying fractions:

$$a/s + b/t = (at + bs)/st \qquad a/s \cdot b/t = ab/st. \tag{6.1}$$

However, some checking is necessary. First of all, the definitions are expressed in terms of representatives of the equivalence classes, and it is paramount they do not dependent on which representatives are used. Secondly, the ring axioms must be verified; once the definitions are in place, this is just straightforward high school algebra safely left to volunteering students.

6.8 As an illustration, let us check that the sum is well defined. Notice that it suffices to vary the representatives of one of the addends at the time; so assume that $(a, s) \sim (a', s')$; *i.e.* $u(as' - a's) = 0$ for some $u \in S$. We find

$$s't(at + bs) - st(a't + bs') = t^2(s'a - a's)$$

which is killed by u. Therefore the sum does not depend on the representative of the first addend used, and by symmetry, neither on the representative of the second, and the sum is well defined.

PROBLEM 6.1 Show that the product is well defined. On a rainy day when all your friends are away, verify the ring axioms for A_S. ★

6.9 The localisation map ι_S is nothing but the canonical map $\iota_S\colon A \to A_S$ that sends an element a in A to the class of the pair $(a,1)$; that is, a is mapped to the fraction $a/1$. By the very definition in (6.1) of the sum and the product in the localization A_S this a ring homomorphism. (Seemingly, this map does nothing to a, but kill it if necessary).

6.10 Our next proposition gives a more practical description of the ring A_S:

PROPOSITION 6.11 *All elements in A_S are of the form a/s. It holds true that $\iota_S(a) = 0$ if and only if a is killed by some element from S; i.e. if and only if there is an $s \in S$ such that $sa = 0$.*

PROOF: By definition every element in A_S is an equivalence class a/s. The zero element in A_S is represented by the pair $(0,1)$ and $\iota_S(a)$ by the pair $(a,1)$. Hence $\iota_S(a) = 0$ if and only if $s\cdot(a\cdot 1 - 0\cdot 1) = 0$ for an $s \in S$; that is, if and only if $s\cdot a = 0$ for an $s \in S$. ❑

6.12 The map ι_S will often be injective; for instance, when A is a domain this is always the case. This allows us to identify A with its image in A_S which significantly simplifies the notation. We can safely write a instead of $\iota_S(a)$, and the inverse image $\iota_S^{-1}\mathfrak{b}$ of an ideal (or any subset for that matter) will simply be the intersection $A \cap \mathfrak{b}$.

The universal property

We shall show that the pair A_S and ι_S solves the universal problem formulated at the top of paragraph 6.4.

6.13 So assume we are given another ring B and a map of rings $\phi\colon A \to B$ such that $\phi(s)$ is invertible for all $s \in S$. The sole way to realize a ring map $\psi\colon A_S \to B$ extending ϕ is to put

$$\psi(a/s) = \phi(a)\cdot\phi(s)^{-1},$$

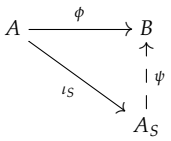
and the salient point is that this is a legitimate definition, *i.e.* $\phi(a)\cdot\phi(s)^{-1}$ is independent on the chosen representative (a,s). But from $a/s = a'/s'$ ensues that $t\cdot(as' - sa') = 0$ for an element $t \in S$, and hence, since ϕ is map of rings, that

$$\phi(t)\cdot\big(\phi(a)\cdot\phi(s') - \phi(a')\cdot\phi(s)\big) = 0.$$

The element $\phi(t)$ is invertible by assumption, and we conclude that $\phi(a)\cdot\phi(s)^{-1} = \phi(a')\cdot\phi(s')^{-1}$.

This proves most of the following proposition:

PROPOSITION 6.14 *Let A be a ring and $S \subseteq A$ a multiplicative subset. Then there is a ring A_S and a ring homomorphism $\iota_S \colon A \to A_S$ solving the universal problem in paragraph 6.4. The pair is unique up to an unambiguous isomorphism.*



PROOF: What remains to be seen is that ψ is a ring homomorphism, but this follows directly from the rules in (6.1) once ψ is well defined. ❑

Examples

6.1 We have not excluded that 0 lies in S. In this case however, the localized ring will be the null-ring since 0 becomes invertible. This situation occurs *e.g.* when S has nilpotent members.

6.2 An simple situation to have in mind is when A is contained in a field K. The localized ring A_S is then just the subring $A[s^{-1}|s \in S]$ of K generated by the inverses of members of S. The elements of this ring are all shaped like as^{-1}; indeed, every sum $\sum_i a_i s_i^{-1}$ can be rendered on this form with s the common denominator of the terms. The universal property of the localized ring A_S then immediately gives a map of rings $A_S \to A[s^{-1}|s \in S]$ which one easily checks is an isomorphism using the description of A_S in Proposition 6.11 on page 126.

6.3 *(The field of fraction of a domain)* Every domain is contained in a smallest field $K(A)$ called the *field of fractions of* A. The set S of non-zero elements in A is multiplicativily closed when A is a domain (by definition, a domain has no zero-divisors), and $K(A)$ is the localization A_S. Every non-zero element becomes invertible in $K(A)$, hence $K(A)$ is a field. The elements are of the form ab^{-1} with $b \neq 0$, and since zero divisors are absent, it holds true that $a/b = a'/b'$ if and only if $ab' = a'b$. In the sequel we shall tacitly identify a and $a/1$, and A will be considered a subring of $K(A)$.

The field of fractions of a domain (*Kvotientkroppen til et område*)

The field $K(A)$ is the smallest field containing A in the sense that if $A \subseteq L$ with L a field, there is a canonical copy of $K(A)$ lying between A and L; *i.e.* one has $A \subseteq K(A) \subseteq L$.

Examples of fraction fields are the field $\mathbb{Q}$ of rational numbers and the field $\mathbb{C}(x_1, \ldots, x_r)$ of rational functions in the variable s $x_1, \ldots, x_r$, which is the fraction field of the polynomial ring $\mathbb{C}[x_1, \ldots, x_r]$.

6.4 The ring of integers $\mathbb{Z}$ within the field rationals $\mathbb{Q}$ is a particular instance of the situation in the previous example. When S is the set of all powers of a given number p, that is, $S = \{p^n\}$, the ring $\mathbb{Z}_S = \mathbb{Z}[1/p] = \{\, a/p^n \mid a \in \mathbb{Z}, n \in \mathbb{N}_0 \,\}$ will be the ring of rational numbers whose denominators are powers of p. (see also Example 1.12 on page 12).

In a similar vein, when p is a prime and S is the complement of the principal ideal $p\mathbb{Z}$, the localization $\mathbb{Z}_S$ will be the ring $\mathbb{Z}_{(p)} = \{\, a/b \mid a, b \in$

$\mathbb{Z}, (p, b) = 1\}$ of rational numbers whose denominator is prime to p. We have already met these ring in Example 2.19 on page 45.

6.5 Consider the polynomial ring $k[x, y, z]$ in three variable over the field k. We shall describe the localisation of $k[x, y, z]$ in the prime ideaal (z) and show that $k[x, y, z]_{(z)} = k(x, y)[z]_{(z)}$; that is, the polynomial ring over the fraction ield $k(x, y)$ localised at the prime (z).

In process we introduce the subset of $k[x, y]$ whose members are the polynomials involving only the variables x and y. It is obviously multiplicatively closed, and as obvious it holds that $k[x, y, z]_S = k(x, y)[z]$. Localising both rings in the ideals generated by z we obtain the desired equality, noticing that $S \subseteq k[x, y]\backslash(z)$, so elements in S are already invertible in $k[x, y, z]_{(z)}$ and $(k[x, y, z]_S)_{(z)} = k[x, y, z]_{(z)}$.

☆

Problems

6.2 Show that $\mathbb{Z}[1/10] = \mathbb{Z}[1/2, 1/5]$. Generalize.

6.3 Prove that any intermediate ring $\mathbb{Z} \subseteq A \subseteq \mathbb{Q}$ is a localization of $\mathbb{Z}$ in a multiplicative set S. ✳

6.4 Prove that the group of units A^* in A is a multiplicative set. Show that the localization maps ι_S is an isomorphism if and only if S is a subset of A^*.

6.5 When L is a set of primes in $\mathbb{Z}$ (finite or infinite), let $\mathbb{Z}_{(L)}$ denote the localization in all primes outside L; that is, we put $\mathbb{Z}_{(L)} = \bigcap_{p \in L} \mathbb{Z}_{(p)}$. Show that there is a natural isomorphism $\mathbb{Z}_{(L)} \otimes_{\mathbb{Z}} \mathbb{Z}_{(L')} \simeq \mathbb{Z}_{(L \cap L')}$. ✳

6.6 Consider be the polynomial ring $A = k[x_1, \ldots, x_n]$ over the field k. Let S be the set polynomials in A that depend only on the first r variables; *i.e.* those on the form $p(x_1, \ldots, x_r)$. Show that S is multiplicatively closed and that $A_S = K[x_{r+1}, \ldots, x_n]$ where K is the field $k(x_1, \ldots, x_r)$ of rational functions.

★

Ideals and localization

6.15 Extension of ideals from A to A_S yields a map from the set $\mathcal{I}(A)$ of ideals in A to the set of ideals $\mathcal{I}(A_S)$ in the fraction ring A_S. The map operates by sending an ideal $\mathfrak{a}$ to the ideal $\mathfrak{a}A_S$ generated by the image $\iota_S(\mathfrak{a})$, and one verifies that members of $\mathfrak{a}A_S$ are all shaped like as^{-1} for some $a \in \mathfrak{a}$ and some $s \in S$. The map is inclusion preserving and preserves products and sums of ideals as extension maps always do (see Paragraph 2.9 on page 26).

6.16 In general the extension map from $\mathcal{I}(A)$ to $\mathcal{I}(A_S)$ is not injective. For instance, it may happen that $S \cap \mathfrak{a} \neq \varnothing$, in which case the extension $\mathfrak{a}A_S$ will contain an element invertible in A_S and consequently be equal to A_S; and of course, this may be the case for several different ideals. In quite another corner, ideals $\mathfrak{a}$ contained in the kernel of ι_S reduce to the zero ideal in A_S. So, some ideals are blown up to A_S (those meeting S) and some collapsed to zero (those contained in $\ker \iota_S$).

EXAMPLE 6.6 A simple instance of the extension map not being injective is the case when $A = \mathbb{Z}$ and $S = \{ p^n \mid n \in \mathbb{Z} \}$ for some prime p. All the ideals $\mathfrak{a} = (p^m)$ extend to the entire ring $\mathbb{Z}_S$. This also illustrates that forming extensions does not commute with forming infinite intersections; indeed, one has $\bigcap_m (p^m) = 0$ whereas $\bigcap_m p^m \mathbb{Z}_S = \mathbb{Z}_S$. ☆

6.17 The extension map is however surjective. Any ideal $\mathfrak{b} \subseteq A_S$ equals $\iota_S^{-1}(\mathfrak{b})A_S$; that is, when pulling an ideal back to A and subsequently extending the result, one recovers the original ideal. To see this, notice that if $b = a/s$ belongs to $\mathfrak{b}$, the element a belongs to $\iota_S^{-1}(\mathfrak{b})$ as $\iota_S(a) = b \cdot s$, and therefore b lies in the extension $\iota_S^{-1}(\mathfrak{b})A_S$.

PROPOSITION 6.18 (IDEALS IN LOCALIZATIONS) *The extension map from $\mathcal{I}(A)$ to $\mathcal{I}(A_S)$ given by $\mathfrak{a} \to \mathfrak{a}A_S$ is surjective. It preserves inclusions, products, sums and finite intersections. One has $\iota_S^{-1}(\mathfrak{a}A_S) = \{ a \in A \mid sa \in \mathfrak{a} \text{ for some } s \in S \}$, and for ideals $\mathfrak{b} \subseteq A_S$ it holds true that $\mathfrak{b} = \iota_S^{-1}(\mathfrak{b})A_S$.*

PROOF: We have already proved most of the proposition, only the assertions about sums, products and intersections remain unproven. It is a general feature of extension of ideals that products and sums are preserved, and we concentrate on the finite intersections; and of course, the case of two ideals will suffice.

Clearly $(\mathfrak{a} \cap \mathfrak{a}')A_S \subseteq \mathfrak{a}A_S \cap \mathfrak{a}'A_S$. So assume that $b \in \mathfrak{a}A_S \cap \mathfrak{a}'A_S$. One may then express b as $b = a/s = a'/s'$ with elements a and a' from respectively $\mathfrak{a}$ and $\mathfrak{a}'$. This yields $t(a \cdot s' - a' \cdot s) = 0$ for some $t \in S$. But then $tsa' = ts'a \in \mathfrak{a} \cap \mathfrak{a}'$ and consequently $b = tsa'/tss'$ lies in $(\mathfrak{a} \cap \mathfrak{a}')A_S$. ❑

6.19 Prime ideals behave more lucidly under localization than general ideals. Either they blow up and become equal to the entire localized ring A_S, or they persist being prime. Moreover, every prime ideal in A_S is of the shape $\mathfrak{p}A_S$ for an unambiguous prime ideal $\mathfrak{p}$ of A. One has:

PROPOSITION 6.20 (PRIME IDEALS IN LOCALIZATIONS) *Assume that $\mathfrak{p}$ is a prime ideal in the ring A and S is a multiplicative subset of A. Extending $\mathfrak{p}$ to the localization A_S has two possible outcomes. Either $\mathfrak{p}A_S = A_S$, and this occurs if and only if $\mathfrak{p} \cap S \neq \varnothing$, or otherwise $\mathfrak{p}A_S$ is a prime ideal and $\iota_S^{-1}(\mathfrak{p}A) = \mathfrak{p}$.*

PROOF: If $S \cap \mathfrak{p} \neq \varnothing$ the ideal $\mathfrak{p}$ blows up to the entire ring in A_S; that is, it holds that $\mathfrak{p}A_S = A_S$. If not, $\mathfrak{p}A_S$ is a prime ideal; indeed, suppose that

$bb' \in \mathfrak{p}A_S$ and that $b = a/s$ and $b' = a'/s'$ with $a, a' \in A$ and $s, s' \in S$. We infer that $tss'bb' = taa' \in \mathfrak{p}$ for some $t \in S$, and hence either a or a' lies in $\mathfrak{p}$ since t does not. Moreover, if $\iota_S(a) = a's^{-1}$ for some $a' \in \mathfrak{p}$, if follows that $sta = ta' \in \mathfrak{p}$, hence $a \in \mathfrak{p}$ since $\mathfrak{p}$ is a prime ideal. ❑

PROPOSITION 6.21 *The prime ideals of A_S are precisely the ideals of the form $\mathfrak{p}A_S$ for $\mathfrak{p}$ a prime ideal in A not meeting S. The prime ideal $\mathfrak{p}$ is uniquely defined.*

PROOF: By the previous proposition, the ideals $\mathfrak{p}A_S$ are all prime, so let $\mathfrak{q}$ be a prime ideal in A_S. Then $\mathfrak{p} = \iota_S^{-1}\mathfrak{q}$ is prime, and by the last sentence in proposition 6.18 above it holds that $\mathfrak{q} = \mathfrak{p}A_S$. ❑

6.22 The localization processe commutes with the formation of radicals:

PROPOSITION 6.23 *Let $\mathfrak{a}$ be an ideal in A and $S \subseteq$ a multiplicative set. The it holds true that*

$$\sqrt{\mathfrak{a}_S} = (\sqrt{\mathfrak{a}})_S.$$

PROOF: If $xs^{-1} \in (\sqrt{\mathfrak{a}})_S$ with $x^n \in \mathfrak{a}$ and $s \in S$, it holds that $(xs^{-1})^n = x^n s^{-n} \in \mathfrak{a}_S$, and so xs^{-1} lies in $\sqrt{\mathfrak{a}_S}$. If $xs^{-1} \in \sqrt{\mathfrak{a}_S}$, it holds that $(xs^{-1})^n = at^{-1}$ with $t \in S$ and $a \in \mathfrak{a}$. Hence $(xt)^n = s^n a t^{n-1} \in \mathfrak{a}$, and consequently $x \in (\sqrt{\mathfrak{a}})_S$. ❑

Problems

6.7 Show that if $\mathfrak{a}A_S = A_S$, then the same holds for all powers $\mathfrak{a}^m$ of $\mathfrak{a}$.

6.8 Let p and q be different prime numbers and let S be the multiplicative set $S = \{ p^n \mid n \in \mathbb{N}_0 \}$. Describe $\mathbb{Z} \cap (pq)\mathbb{Z}_S$. ✲

6.9 Let S be multiplicatively closed in the ring A and let $\mathfrak{a} \subseteq A$ be an ideal. Show that the ideals $(\mathfrak{a} : s)$ when s runs through S form a directed family of ideals; hence their union is an ideal. Show that $\bigcup_{s \in S}(\mathfrak{a} : s) = \iota_S^{-1}(\mathfrak{a}A_S)$. ✲

6.10 Suppose that $\mathfrak{p}$ is a prime ideal and that $\mathfrak{a}$ an ideal contained in $\mathfrak{p}$. Show that $\iota_S^{-1}(\mathfrak{a}A_s) \subseteq \mathfrak{p}$.

6.11 Let $j\colon \operatorname{Spec} A_S \to \operatorname{Spec} A$ be the map induced from the localization map $\iota_S\colon A \to A_S$. Show that j is a homeomorphism onto its image (when the image is endowed with induced topology). Show that the image $j(\operatorname{Spec} A)$ equals the intersection of all the open sets containing it.

6.12 Show by an example that j is not necessarily an open embedding. HINT: Let *e.g.* $A = \mathbb{Z}$ and S the multiplicative subset generated by every second prime.

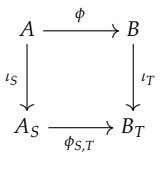
6.13 Given an example of a ring A and a non-zero prime ideal $\mathfrak{p}$ such that $A_\mathfrak{p} = A/\mathfrak{p}$. HINT: Let A be the product of two fields.

6.14 Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in A, Prove that $(\mathfrak{a} : \mathfrak{b})_S = (\mathfrak{a}_S : \mathfrak{b}_S)$. ✳

★

Functoriality

6.24 The ring A_S depends of course on both A and S, so functoriality is naturally formulated in terms of the pair (A, S). Given another pair T and B and a map of rings $\phi\colon A \to B$ taking elements of S into T, there is an induced map of rings $\phi_{S,T}\colon A_S \to B_T$ satisfying $\phi_{S,T} \circ \iota_S = \iota_T$. Since ϕ takes S into T, the elements $\phi(s)$ become invertible in B_T and the universal property of A_S guarantees that $\iota_T \circ \phi$ extends to a map $A_S \to A_T$. This map simply sends a/s to $\phi(a)/\phi(s)$.



6.25 A particular case to notice is when $A = B$ and $\phi = \mathrm{id}_A$. If $S \subseteq T$, there is a canonical map $A_S \to A_T$ which just interprets fractions a/s in A_S as a fractions in A_T. This map might appear very much like doing nothing; but be aware, it can have a non-trivial kernel. When some member of T kills elements in A not killed by anyone in S there will non-zero members of the kernel.

However, when S contains no zero-divisors, the localization map $A \to A_S$ is injective and we shall identify A as a subring of A_S. In particular, when A is an integral domain all the localization maps are injective, and we may—and tacitly will do—identify the localized rings as subrings of the field of fractions $K(A)$. After this identification, the ring A_S is a subring of A_T, when $S \subseteq T$.

The local ring at a prime ideal.

A few ways of forming rings of fraction are omnipresent in algebra and algebraic geometry and are used over and over again. The most prominent one is may be the localization $A_\mathfrak{p}$ at a prime ideal $\mathfrak{p}$.

6.26 The complement $S = A\backslash\mathfrak{p}$ of a prime ideal $\mathfrak{p}$ is multiplicatively closed, and the corresponding localized ring is written as $A_\mathfrak{p}$. The elements are fractions a/b with $b \notin \mathfrak{p}$. It is a local ring whose only maximal ideal is $\mathfrak{p}A_\mathfrak{p}$:

PROPOSITION 6.27 *The localisation $A_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}A_\mathfrak{p}$. The assignment $\mathfrak{q} \mapsto \mathfrak{q}A_\mathfrak{p}$ is a one-to-one correspondence bewteen prime ideals in $A_\mathfrak{p}$ and prime ideals $\mathfrak{q}$ in A contained in $\mathfrak{p}$.*

PROOF: This is nothing but Proposition 6.21 above on page 6.21, according to which the prime ideals in $A_\mathfrak{p}$ are precisely the ideals in $A_\mathfrak{p}$ of the form $\mathfrak{q}A_\mathfrak{p}$ where $\mathfrak{q}$ is a prime ideal in A contained in $\mathfrak{p}$, and it holds true that $\mathfrak{q} = \iota^{-1}(\mathfrak{q}A_\mathfrak{p})$. ❑

Notice that the kernel of the localization map $\iota\colon A \to A_\mathfrak{p}$ is contained in any prime ideal $\mathfrak{q} \subseteq \mathfrak{p}$; indeed, if $sa = 0$ with $s \notin \mathfrak{p}$, *a fortiori* $s \notin \mathfrak{q}$ and hence $a \in \mathfrak{q}$.

The residue field $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is frequently written $k(\mathfrak{p})$. Since $\iota^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$ it holds true that $A/\mathfrak{p}$ maps invectively into $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. And in fact, $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ equals the fraction field $K(A/\mathfrak{p})$ of $A/\mathfrak{p}$.

EXAMPLE 6.7 If p is a prime number, the localized ring $\mathbb{Z}_{(p)}$ at the maximal ideal generated by p consists of rational numbers whose reduced form is a/b where b is relatively prime to p. The maximal ideal is generated by p and the residue field is the field $\mathbb{F}_p$ with p elements. ☆

6.28 Clearly an arbitrary intersection of multiplicatively closed sets is multiplicatively closed, therefore complements of unions of prime ideals are multiplicatively closed. If the prime ideals involved are $\{\mathfrak{p}_i\}_{i\in I}$; and hence that $S = A\backslash\bigcup_{i\in I}\mathfrak{p}_i$, the maximal ideals of A_S will be the extension $\mathfrak{p}_i A_S$. In particular, if the $\mathfrak{p}_i$'s are merely finite in numbers, A_S will be a semi-local ring.

Inverting powers of a single element.

Given an element $f \in A$. The set $S = \{ f^n \mid n \in \mathbb{N}_0 \}$ of all powers of f is obviously multiplicatively closed, and the corresponding ring fractions A_S is denoted A_f. The prime ideals in A_f are exactly those on the form $\mathfrak{p}A_f$ for $\mathfrak{p}$ a prime ideal in A with $f \notin \mathfrak{p}$; that is, for the members of the distinguished open subset $D(f)$ of Spec A.

There is a natural isomorphism between $A[x]/(xf-1)$ and A_f that sends x to f^{-1}. By the universal mapping property of the polynomial ring the map is well defined, and f being invertibel in $A[x]/(xf-1)$, the unversal property of A_f furnishes an inverse. This makes the notation $A[f^{-1}]$ for A_f legitimate; the usage is however poisonous when f is a zero-divisor. Adding f^{-1} kills, and in case f is nilpotent, the intoxication is lethal; everything is killed and $A[f^{-1}] = 0$.

EXAMPLE 6.8 It is worthwhile mentioning a concrete example. Consider the ring $A = \mathbb{C}[z]$ of complex polynomials in the variable z and let $f = z - a$. The localized ring A_f consists of those rational functions that are regular away from a; that is, they have at most a pole at a. This generalizes to the ring $\mathcal{O}(\Omega)$ of functions holomorphic in any domain Ω of the complex plane containing a. The localized ring $\mathcal{O}(\Omega)_{z-a}$ has the functions meromorphic in Ω with at most a pole at a as elements. ☆

The total ring of fractions

The set S of non-zero divisors in the ring A is closed under multiplication; indeed, if s and t are non-zero divisors and $sta = 0$ with $a \neq 0$ it would follow that $ta \neq 0$ contradicting that s is a non-zero divisor. The corresponding ring of fractions is denoted by $K(A)$ and called the *total ring of fractions* of A. When A is an integral domain, $S = A\backslash\{0\}$, and all non-zero elements become invertible in $K(A)$. Consequently $K(A)$ is a field; it is called the *field of fractions*

The total ring of fractions (*Kvotientringen*)

The field of fractions (*Kvotientkroppen*)

of A, which we met already in Example 6.3 on page 6.3. The ring $K(A)$ is in general not a field, but by definition has the property that all non-zero divisors are invertible.

In any case, the canonical map $A \to K(A)$ is injective; indeed, if s is a non-zero divisor, by definition $sa = 0$ implies that $a = 0$.

PROPOSITION 6.29 *The total ring of fractions $K(A)$ of a ring A has the property that every non-zero divisor is invertible. The natural map A to $K(A)$ is injective. Moreover, $K(A)$ is a field if and only if A is an integral domain.*

6.30 We give two examples. The first is a simple but typical situation in algebraic geometry. The ring A is the ring of polynomial functions on a variety X with two components; in our specific example the two components are the coordinate axes in the plane. The total ring of fractions of A turns out to be the product of two fields, the elements are pairs of rational functions, one on each of the axes. Contrary to what is requested of polynomial functions on X, there is no continuity condition at the origin to be fulfilled; the two rational functions may take different values, or for that matter, may have poles at the origin.

This behavior is fairly general; for any ring A without nilpotent elements and which merely has finitely many minimal prime ideals (that is, there is a representation $(0) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ of the zero ideal as a finite intersection of prime ideals) it holds that $K(A)$ is a product of fields. The only moral of the second example, is that if A has nilpotents, the ring of fractions $K(A)$ can be rather involved; and far from being a product of fields.

EXAMPLE 6.9 Let $A = k[X,Y]/(XY)$ and let x and y be the classes of X and Y respectively. Since $(XY) \cap k[X] = (0)$ it holds that $k[X] \simeq k[x]$ and ditto $k[Y] \simeq k[y]$, thus we may talk about the rational function fields $k(X)$ and $K(Y)$ as $k(x)$ and $k(y)$.

We shall see the total quotient ring $K(A)$ is isomorphic to the product $k(x) \times k(y)$ of the rational functions fields in $k(x)$ and $k(y)$. In geometric terms, A is the ring of polynomial functions on the union $Z = V(x) \cup V(y)$ of the y-axis and the x-axis in the plane, and the elements of $K(A)$ are just a pair of a rational function, one on the x-axis and one on the y-axis.

All cross-terms are killed in A, and the elements are all shaped like $a + p(x) + q(y)$ where $p(x)$ and $q(y)$ are polynomials vanishing at zero and a is scalar in k. The zero-divisors in A is the union[1] $(x) \cup (y)$, so that the non-zero-divisors of A are of the form $a + p(x) + q(y)$ with either $a \neq 0$ or neither $p(x)$ nor $q(y)$ identically equal to zero.

[1] If $P(x,y)$ is a zero divisor, there is a relation like $P(X,Y)Q(Y,Y) = A(X,Y)XY$, so either X or Y divides $P(X,Y)$

There is a map of rings

$$A \to k(x) \times k(y)$$

sending the class of a polynomial $a + p(x) + q(y)$ to the pair $(a + p(x), a + p(y))$,

these are invertibel in $k(x) \times k(y)$ and the there is induced a ring map

$$K(A) \to k(x) \times k(y),$$

which clearly is injective; but it is slightly more subtle that it is surjective. Let $\xi = (Q(x)/R(x), S(y)/T(y))$ be an element in $k(x) \times k(y)$; then $R(x)$ and $T(y)$ are non-vanishing polynomial. Then

$$\xi = (Q(x)x/R(x)x, S(y)y/T(y)y),$$

and $xR(x) + yT(y)$ is a non-zero divisor in A mapping to $(xR(x), yT(y))$ ☆

PROBLEM 6.15 Why is it necessary to introduce the seemingly pointless factors x and y in the fractions? ★

EXAMPLE 6.10 Let $B = k[X, Y]/(X^2, XY)$ and let as usual x and y be the classes of X and Y in B. Then $\mathfrak{m} = (x, y)$ is a maximal ideal (one has $B/\mathfrak{m} = k$). Let $A = B_{\mathfrak{m}}$ be the ring B localized at $\mathfrak{m}$. As in every local ring the units of A are precisely the members not lying in the maximal ideal $\mathfrak{m}$. We contend that all elements in $\mathfrak{m}$ are zero-divisors, and hence A is its own total ring of fraction. Indeed, x kills both x and y, hence the whole ideal $\mathfrak{m} = (x, y)$.

It worth while noticing that (x) is a prime ideal, since it holds true that $B/(x) = k[X, Y]/(X^2, XY, X) = k[Y]$ is an integral domain, and (x) is the only other prime ideal in B and is equal to the radical $\sqrt{(0)}$ of B; indeed, if $\mathfrak{p}$ is prime one has $x^2 \in \mathfrak{p}$, hence $x \in \mathfrak{p}$.

Thus B has two prime ideals, the maximal ideal (x, y) whose elements constitute all zero-divisors and a sole minimal ideal (x) whose elements are all the nilpotents of B. ☆

PROBLEM 6.16 Show that $A_{(x)}$ equals the rational function field $k(Y)$. ★

Problems

6.17 Let n be a natural number. Determine the total quotient ring of $\mathbb{Z}/n\mathbb{Z}$. ✳

6.18 Let A be any ring. Show that the nil-radical of $K(A)$ is equal to the extension of the nil-radical of A. ✳

6.19 Let A be a ring. ✳

a) Show that if the elements of A are either zero divisors or invertible, then $A = K(A)$.

b) If A has only one prime ideal, prove that $K(A) = A$.

c) Let A be a direct product (of any cardinality) of any number of rings each having only one prime ideals. Prove that $K(A) = A$.

6.20 Let k be a field and consider the polynomial ring $A = k[x_1, \ldots, x_n]$. Let $r < n$ be a natural number. Let S be the subset of A of polynomials in the variable $x_{r+1}, \ldots, x_n$. Show that S is multiplicatively closed and that $k[x_1, \ldots, x_n]_S = K[x_1, \ldots, x_r]$ where $K = k(x_{r+1}, \ldots, x_n)$ is the field of rational functions in the variables $x_{r+1}, \ldots, x_n$.

6.21 Let A be a domain with quotient field K. Denote by S the multiplicative set $A \backslash 0$ of non-zero elements in A. Show that $A[T]_S = K[T]$.

A last example

6.31 There is multiplicatively closed set associated with any ideal $\mathfrak{a}$ in A which is not that frequently met. It equals the set $S = 1 + \mathfrak{a}$; that is, the set consisting of elements shaped like $1 + a$ with $a \in \mathfrak{a}$. one has the subset S of elements of the form $1 + a$ with $a \in \mathfrak{a}$ which is multiplicatively closed. In this case the the maximal ideals in A_S are those of the form $\mathfrak{m}A_S$; hence $\mathfrak{a}A_S$ is contained in the Jacobson radical of A_S.

6.2 *Localization of modules*

There is also a procedure to localize any A-module M in S closely resembling the way the fraction ring A_S was constructed. The localized module will be denoted by M_S. The construction of M_S is functorial in M and gives a functor $\mathsf{Mod}_A \to \mathsf{Mod}_{A_S}$ with the important property of being additive and exact.

6.32 To construction the localized module M_S we mimick the way A_S was fabricated. Details will be skipped; they may *mutatis mutandis* be verified as in the case of ring.

To begin with one introduces an equivalence relation on the Cartesian product $M \times A$ by declaring two pairs (m, s) and (m', s') to be equivalent if

$$t(ms' - m's) = 0 \tag{6.2}$$

for some $t \in S$. The equivalence class of (m, s) will be designated by either m/s or ms^{-1}. The module structure on M_S consists of an additive group structure and an action of A_S. The additive structure is defined in analogy with the usual way of adding fraction, namely as $m/s + n/t = (mt + sn)/st$. And the action of an element $a/s \in A_S$ is given in the staightforward way: $a/s \cdot m/t = am/st$. There is natural map $\iota_S \colon M \to M_S$ sending m to the class of $(m, 1)$, and as in the case of rings, we shall often merely write m for the image.

Naturally, there is a lot of checking to be done. Every single step is straightforward, and we leave these soporific verifications to the students for a rainy day. Summing up, one has:

LEMMA 6.33 *Every element of M_S is of the form m/s. The map $\iota_S\colon M \to M_S$ is A-linear, and its kernel consists of the elements m in M killed by some member of S; that is,* $\ker \iota = \{\, m \in M \mid tm = 0 \text{ for some } t \in S \,\}$.

6.34 The same applies to the maps ι_S when it comes to modules as with rings. To simplify the notion, one soon drops the reference to the map and writes x or $x/1$ for $\iota_S(x)$, but with some cautiousness since the image very well can be zero.

When the module M is finitely generated, say by members $m_1, \dots, m_r$, the images $\iota_S(m_i)$ of the m_i's will obviously generate M_S. Indeed, pick a member xs^{-1} from M_S and write $x = \sum a_i m_i$ then of course $xs^{-1} = \sum a_i s^{-1} m_i$.

Functoriality

6.35 Given two A-modules M and N and an A-linear map $\phi\colon M \to N$. Sending m/s to $\phi(m)/s$ gives an A_S-linear map between the localized modules M_S and N_S; that is, a map $\phi_S\colon M_S \to N_S$.

A formal definition starts with the map $(m, s) \to (\phi(m), s)$ between the Cartesian product, and the salient point is that this respects the equivalence relations as in (6.2). Indeed, a relation like $t(ms' - m's) = 0$ leads to the relation $t(\phi(m)s' - \phi(m')s) = 0$ because ϕ is A-linear. Therefore there is induced a map between the equivalence classes.

6.36 From the definition of ϕ_S we infer immediately that a linear combination of maps between N and M localizes to the corresponding linear combination; that is, one has

$$(a\phi + b\psi)_S = a\phi_S + b\psi_S,$$

where ϕ and ψ are A-linear maps from M to N and a and b ring elements. And it is equally clear that the association is functorial; it holds true that

$$(\psi \circ \phi)_S = \psi_S \circ \phi_S$$

whenever ϕ and ψ are composable since it already holds at the level of the Cartesian products—and of course, $(\mathrm{id}_M)_S = \mathrm{id}_{M_S}$.

PROPOSITION 6.37 *Let A be a ring and S a multiplicative subset of A. The localization functor $\mathsf{Mod}_A \to \mathsf{Mod}_{A_S}$ is additive and exact.*

PROOF: The only subtle point is that the functor is exact. In other words that it brings an exact sequence

$$N \xrightarrow{\psi} M \xrightarrow{\phi} L \tag{6.3}$$

to an exact sequence. So our task is to verify that the sequence

$$N_S \xrightarrow{\psi_S} M_S \xrightarrow{\phi_S} L_S$$

is exact, which amounts to checking that $\ker \phi_S = \operatorname{im} \psi_S$. To that end, pick an element m/s in the kernel of ϕ_S. This means that $\phi(m)/s = 0$, hence $t\phi(m) = 0$ for some $t \in S$. But then $tm \in \ker \phi$, and since the sequence (6.3) is exact, there is an element n in N such that $\psi(n) = m$. But then we have $\psi_S(n/s) = \psi(n)/s = m/s$, and we are through. ❑

Submodules

Given a submodule $N \subseteq M$. The localized module N_S can be considered to be submodule of M_S. The inclusion map localizes to an injection whose image consists of elements shaped like fractions ns^{-1} with $n \in N$ and $s \in S$, and thus it can naturally be identified with N_S.

6.38 Localization behaves nicely with respect to sums and finite intersections of submodules; the following two assertions hold:

- ❑ $(\sum_i N_i)_S = \sum_i (N_i)_S$
- ❑ $(N \cap N')_S = N_S \cap N'_S$

where N, N' and the N_i's are submodules of N. However, localization does not commute with infinite intersections as we saw in example 6.6 on page 129. In particular, formation of arbitrary direct sums commute with localizations.

- ❑ $(\bigoplus_{i\in I} M_i)_S \simeq \bigoplus_{i\in I} (M_i)_S$

To establish the first equality observe that it ensues from the inclusion $N_i \subseteq \sum_i N_i$ that $(N_i)_S \subseteq (\sum_i N_i)_S$, hence that $\sum_i (N_i)_S \subseteq (\sum_i N_i)_S$. Any element in $(\sum_i N_i)_S$ is of the form $(\sum_i x_i)s^{-1}$ with merely finitely many of the x_i's being non-zero, which obviously lies in $\sum_i (N_i)_S$.

The second follows because $y = n/s = n'/s'$ means $ts'n = tsn'$ for some $t \in S$, and putting $x = ts'n$ we then infer that $x \in N \cap N'$ and $y = x/tss'$.

Problem 6.22 Locization does not commute with infinite direct products. Let $p \in \mathbb{Z}$ be a number and denote by S the multiplicative set $S = \{p^n\}$ in $\mathbb{Z}$. Show that there is a natural inclusion

$$(\prod_{i\in\mathbb{N}} \mathbb{Z})_S \subseteq \prod_{i\in\mathbb{N}} \mathbb{Z}_S,$$

but that the inclusion is strict. ★

Relation with the tensor product

6.39 The action of A_S on M is expressed by the bilinear map $M \times A_S \to M_S$ that sends (m, as^{-1}) to $am \cdot s^{-1}$, and in view of the univeral property enjoyed by the tensor product, it induces an A-linear map $\Psi\colon M \otimes_A A_S \to M_S$ which on decomposable tensors acts by sending $m \otimes as^{-1}$ to ams^{-1}. This map turns out to be an isomorphism:

PROPOSITION 6.40 *The map Ψ defined above is an isomorphism $M_S \simeq M \otimes_A A_S$.*

PROOF: The crux of the poof is that all the elements in $M \otimes_A A_S$ are decomposable; that is, they are of the form $m \otimes s^{-1}$ with $m \in M$ and $s \in S$. Granted this, if $m \otimes s^{-1}$ is mapped to zero; that is, if $ms^{-1} = 0$, the element m is annihilated by some t from S. But then $m \otimes s^{-1} = tm \otimes s^{-1}t^{-1} = 0$, so that the map Ψ is injective, and Ψ is obviously surjective as well.

A priori an element from $M \otimes A_S$ is of the shape $\sum_i m_i \otimes a_i s_i^{-1}$ with $a_i \in A$ and $s_i \in S$. Moving the a_i through the tensor product, we we may bring it on the form $\sum_i m_i \otimes s_i^{-1}$. The trick is now to let $s = s_1 \cdots s_r$ and $t_i = ss_i^{-1}$, and we arrive at

$$x = \sum_i m_i t_i \otimes s^{-1} = (\sum_i m_i t_i) \otimes s^{-1} = m \otimes s^{-1}$$

with $m = \sum_i m_i t_i$. ❑

6.41 We saw that base change preserves tensor products (Proposition 5.35 on page 115) and combining that with Proposition 6.40 above, we see that localization process preserves tensor product as well:

PROPOSITION 6.42 *Let M and N be two A-modules and S a multiplicative set in A. Then there is a canonical isomorphism*

$$(M \otimes_A N)_S \simeq M_S \otimes_{A_S} N_S.$$

6.43 When it comes to hom-sets, the behaviour is rather nice, at least for modules of finite presentation. In general, sending an A-linear map ϕ between two A-modules M and N to the localized map ϕ_S is an A-linear map $\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_{A_S}(M_S, N_S)$. By the universal property of localization it extends to a map $\mathrm{Hom}_A(M, N)_S \to \mathrm{Hom}_{A_S}(M_S, N_S)$; and in case M is of finite presentation, this map is an isomorphism:

PROPOSITION 6.44 *Let M and N be two A modules and S a multiplicative set in A. Assume that M is of finite presentation. Then the canonical map*

$$\mathrm{Hom}_A(M, N)_S \xrightarrow{\simeq} \mathrm{Hom}_{A_S}(M_S, N_S)$$

induced by sending ϕ to ϕ_S is an isomorphism.

PROOF: Recall that both localization and the hom-functors are additive functors, hence the proposition holds true whenever M is a free A module of finite rank n; indeed, one finds

$$\mathrm{Hom}_A(nA, N)_S \simeq (nN)_S \simeq n(N_S) \simeq \mathrm{Hom}_{A_S}(nA_S, N_S)$$

where the isomorphisms are the natural ones (the one in the middle is an isomorphism since localization is additive, and the two others are because hom-functors are additive). Since M is assumed to be of finite presentation, it lives in an exact sequence

$$mA \xrightarrow{\phi} nA \xrightarrow{\pi} M \longrightarrow 0, \tag{6.4}$$

with $m, n \in \mathbb{N}$ and where ϕ and π are A-linear maps. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_A(M,N)_S & \longrightarrow & \mathrm{Hom}_A(nA,N)_S & \longrightarrow & \mathrm{Hom}_A(mA,N)_S \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Hom}_{A_S}(M_S,N_S) & \longrightarrow & \mathrm{Hom}_{A_S}(nA_S,N_S) & \longrightarrow & \mathrm{Hom}_{A_S}(mA_S,N_S) \end{array}$$

The upper sequence is obtain from (6.4) by applying $\mathrm{Hom}_A(-,N)_S$ to it and is therefore exact by left exactness of hom-functors. The bottom sequence is the localization in S of the upper one, and since localization is an exact functor, it is exact. The vertical maps are the canonical maps induced by sending ϕ to ϕ_s, and it is a matter of simple verification to check that the squares commute.

Now, the final point is that the two rightmost maps are isomorphisms by the beginning of the proof, and then the Five Lemma tells us that the third map is an isomorphisms as well, which is precisely what we aim at proving! ❑

6.3 *Nakayama's lemma*

Nakayama's lemma is a workhorse in commutative algebra and is applied over and over again. As often is the case with popular courses, it comes in quit a lot of different flavours. One way of viewing this famous result—which we shall adopt as our point of departure—is as an extension to finitely generated modules of the fundamental existence result for maximal ideals in rings (Theorem 2.50 on page 40): Maximal proper submodules of finitely generated modules always exist; or what amounts to the same in view of the character of simple modules (Proposition 4.35 on page 78), simple quotients exist.

This is may be an unorthodox place to treat Nakayama's lemma, but in fact Nakayama's lemma is about whether modules are zero or not, and we find its appropriate placement to be in together with the treatment of the support of modules.

6.45 The notion of the Jacobson radical will frequently appear in the hypotheses of subsequent results, so for the convenience of the students we recall the definition. The Jacobson radical $J(A)$ of a ring A is the intersection of all maximal ideals in A; that is, $J(A) = \bigcap_{\mathfrak{m} \subseteq A} \mathfrak{m}$ where $\mathfrak{m}$ runs through the maximal ideals in A. The elements in $J(A)$ are precisely those $a \in A$ so that $1 + ax$ is invertible for all $x \in A$ (Proposition 2.67 on page 45).

Nakayama's lemma and simple quotients

6.46 It is not true that every A-module has a simple quotient, an elementary example being the $\mathbb{Z}$-module $\mathbb{Q}$; every ideal $\mathfrak{a}$ in $\mathbb{Z}$ satisfies $\mathfrak{a}\mathbb{Q} = \mathbb{Q}$ and hence $\mathbb{Q}$ has no simple quotient. However finitely generated modules always have, and this is our first version of Nakayama's lemma:

PROPOSITION 6.47 (NAKAYAMA'S LEMMA I) *Let M be a non-trivial finitely generated A-module. Then M has a non-zero simple quotient. In other words, there exists maximal ideal $\mathfrak{m}$ with an A-linear surjection $M \to A/\mathfrak{m}$; or equivalently, $\mathfrak{m}M$ is a proper submodule of M.*

PROOF: If M is cyclic, it is of the form $A/\mathfrak{a}$ for some proper ideal and has $A/\mathfrak{m}$ as a quotient for any maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$. Assume next that M is not cyclic, and let n be the the least number such that M can be generated by n elements. Then $n \geqslant 2$. Let $x_1, \ldots, x_n$ generate M. The submodule N generated by $x_2, \ldots, x_n$ is a proper submodule and M/N is cyclic (generated by the class of x_1), and has a simple quotient by the first part of the proof. ❑

6.48 An alternative proof of Nakayama's lemma (tailored to the same pattern as the proof of the Basic Existence Theorem for ideals (Theorem 2.50 on page 40)) is to apply Zorn's to establish that any finitely generated A-module M has a maximal proper submodule. If N is one, M/N will be a nontrivial simple quotient. To checks that chains have upper bounds, observe that the union of any chain $\{M_i\}$ of proper submodules of M will be proper; were it not, the elements of a finite generating set would eventually all lie in one of the submodules from the chain, and that submodules would not be proper. In the case of M being Noetherian, any collection of submodule contains maximal members, and existence of maximal proper submodules, comes for free!

Nakayama classic

6.49 To assure anyone (hopefully there are none) that finds our approach a blasphemous assault on their most cherished tradition, we surely shall include Nakayama classic; here it comes:

PROPOSITION 6.50 (NAKAYAMA CLASSIC) *Let $\mathfrak{a}$ be an ideal in A contained in the Jacobson radical of A. Let M be a finitely generated A-module and assume that $\mathfrak{a}M = M$. Then $M = 0$.*

PROOF: Recall that the Jacobson radical of A equals the intersection of all the maximal ideals in A. Assume $M \neq 0$. By Nakayama I (Proposition 6.47 above) there is a maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}M$ is a proper submodule, which is impossible since $\mathfrak{a} \subseteq \mathfrak{m}$ and $\mathfrak{a}M = M$ by assumption. ❑

With the isomorphism $M \otimes_A A/\mathfrak{a} \simeq M/\mathfrak{a}M$ in mind, one may rephrase Nakayama's lemma as follows.

PROPOSITION 6.51 (NAKAYAMA'S LEMMA III) *Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal contained in the Jacobson-radical of A. If $M \otimes_A A/\mathfrak{a} = 0$, it holds true that $M = 0$.*

6.52 The by far most common situation when Nakayama's lemma is applied, is when A is a local ring and $\mathfrak{a} = \mathfrak{m}$ is the maximal ideal, and this situation merits to be mentioned specially:

PROPOSITION 6.53 (NAKAYAMA'S LEMMA FOR LOCAL RINGS) *Let A be a local ring with maximal ideal $\mathfrak{m}$. Assume that M is finitely generated A module such that $\mathfrak{m}M = M$. Then $M = 0$.*

PROOF: The Jacobson radical of A equals $\mathfrak{m}$. ❑

Other formulations

6.54 There are several other reformulations of Nakayama's lemma, and here we offer a few of the most frequently applied version.

PROPOSITION 6.55 *Assume that $\phi\colon N \to M$ is A-linear and M is finitely generated. Moreover, let $\mathfrak{a}$ be an ideal contained in the Jacobson radical of A: If $\phi \otimes \mathrm{id}_{A/\mathfrak{a}}$ is surjective, it holds that ϕ is surjective.*

PROOF: The tensor product is right exact so $\operatorname{coker}(\phi \otimes \mathrm{id}_{A/\mathfrak{a}}) = (\operatorname{coker}\phi) \otimes A/\mathfrak{a}$. The cokernel $\operatorname{coker}\phi$ is finitely generated since M is, and $\operatorname{coker}(\phi \otimes \mathrm{id}_{A/\mathfrak{a}}) = (\operatorname{coker}\phi) \otimes A/\mathfrak{a} = 0$ by hypothesis. Hence $\operatorname{coker}\phi = 0$ by Nakayama III (Proposition 6.51 above). ❑

PROPOSITION 6.56 *Let M is be a finitely generated A module. Assume that $\mathfrak{a}$ is an ideal contained in the Jacobson radical of A and that N a submodule of M such that $N + \mathfrak{a}M = M$. Then $N = M$.*

PROOF: The quotient M/N is finitely generated since M is, and it holds true that $\mathfrak{a}M/N = M/N$ because any m from M lies in $\mathfrak{a}M$ modulo elements in N; or if you prefer, use the previous proposition with ϕ being the inclusion map $N \hookrightarrow M$. ❑

PROPOSITION 6.57 *Assume that $\mathfrak{a} \subseteq A$ is an ideal contained in the Jacobson-radical of A. Let M be a finitely generated A-module and assume that $\{m_i\}_{i \in I}$ are elements in M whose residue classes generate $M/\mathfrak{a}M$. Then the m_i's generate M.*

PROOF: Let N be the submodule of M generated by the m_i's. The hypothesis that the residue classes generate $M/\mathfrak{a}M$ translates into the statement that $M = N + \mathfrak{a}M$, and the proposition follows from Proposition 6.56. ❑

An extended version of Nakayama's lemma

6.58 There is a version of Nakayama valid for all ideals not only those lying in the Jacobson radical; but of course, when weakening the hypothesis you get a weaker conclusion. The proof relies on a localization technique.

Proposition 6.59 (Nakayama extended) *Let $\mathfrak{a}$ be an ideal in the ring A, and assume that M is a finitely generated A-module satisfying $\mathfrak{a}M = M$. Then M is killed by an element of the form $1 + a$ with $a \in \mathfrak{a}$; that is, there is an $a \in \mathfrak{a}$ so that $(1 + a)M = 0$.*

Proof: Let S be the multiplicative set $\{\, 1 + a \mid a \in \mathfrak{a} \,\}$. Then $\mathfrak{a}A_S$ is contained in the Jacobson radical of A_S (by Propostion 2.67 on page 45), and by Nakayama Classic we may conclude that $M_S = 0$. Thence there is for each generator x_i of M, an element $s_i \in S$ killing x_i. The x_i's being finite in number we may form the product of the s_i's, which obviously kills M and is of the required form. ❑

Problems

6.23 Let Φ be an $n \times n$-matrix with coefficients in a local ring A and denote by $\bar{\Phi}$ the matrix whose entries are the classes of the entries of Φ in the residue class field k of A. Show that if the determinant $\det \bar{\Phi}$ does not vanish, then Φ is invertible. ⁂

6.24 *(Demystifying Nakayama's lemma.)* Let A be a local ring with residue class field k. Assume that $\phi\colon E \to F$ is an A-linear map between free module of finite rank, and let Φ be the matrix of ϕ in some bases. ⁂

a) Show that if one of the maximal minors of $\bar{\Phi}$ does not vanish, one of the maximal minors of Φ is invertible in A. Conclude ϕ is surjective when $\phi \otimes \mathrm{id}_k$ is.

b) Show the classical Nakayama's lemma for finitely presented modules over a local ring by using the previous subproblem.

c) *(Mystifying the demystification.)* Show Nakayma's lemma for finitely generated modules over a local ring by using subproblem a). Hint: The key word is "right sections" of linear maps, if you don', prefer coping with maximal minors of $n \times \infty$-matrices!!

6.25 Let A be a local ring with residue class field k. Let $\phi\colon E \to F$ be a map between finitely generated free A-modules, and suppose that $\phi \otimes \mathrm{id}_k$ is injective. Prove that ϕ is a split injection. Hint: Prove that at least one maximal minor of the matrix of ϕ in some bases is invertible in A. Then the projection $\pi\colon mA \to nA$ corresponding to that minor furnishes a section. ⁂

6.26 Let M an A-module such that $\mathfrak{m}M = M$ for any maximal ideal $\mathfrak{m}$. Show that M has the property that if one discards any finite part from a generating set one still has a generating set.

6.27 Let M be a finitely generated A-module and let $\phi\colon M \to M$ be a *surjective* A-linear map. Show that ϕ is injective. Show by exhibiting examples that this is no longer true if M is not finitely generated. HINT: Regard M as a module over the polynomial ring $A[t]$ with t acting on $x \in M$ as $t \cdot x = \phi(x)$. Use the extended version of Nakayama's lemma with $\mathfrak{a} = (t)A[t]$.

6.28 *(Nilpotent Nakayama.)* This exercise is about a result related to Nakayama's lemma, but of a much more trivial nature. Let A be a ring M an A-module. Assume that $\mathfrak{a}$ is a nilpotent ideal in A. Show that if $\mathfrak{a}M = M$, then $M = 0$.

6.29 *(Graded Nakayama.)* Let $M = \bigoplus_i M_i$ be a graded module over the graded ring $R = \bigoplus_i R_i$. Assume that $M_{-i} = 0$ for i sufficiently big; that is, the degrees of the elements from M are bounded below. Let $\mathfrak{a}$ be a homogenous ideal whose generators are of positive degree. Assume that $\mathfrak{a}M = M$ and show that $M = 0$. HINT: Consider the largest n so that $M_{-n} \neq 0$.

6.30 Let A be ring and P a finitely generated projective module. Show that there is a set of elements $\{f_i\}$ in A such that the distinguished open subsets $D(f_i)$ cover Spec A, and such that each localized module P_{f_i} is a free module over A_{f_i}.

6.31 Let A a ring and let e be a non-trivial idempotent element. Show that the principal ideal $I = (e)A$ is projective, and that a direct sum $\bigoplus_i I$ of a any number, finite or not, of copies of I never can be free. HINT: Such sums are killed by $1 - e$.

6.4 *The support of a module*

The spectrum Spec A of a ring a geometric structure associated to A. The points are the prime ideals in A and the topology is the Zariski topology whose closed sets are those of the form $V(\mathfrak{a}) = \{\, \mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$, where $\mathfrak{a}$ is any ideal in A.

Based on the belief that modules over local rings are simpler than other, a general technique is to try to pass from local data—that is properties of the localized modules $M_{\mathfrak{p}}$—to global data; that is, to infer properties of the module M itself from properties of the localized modules $M_{\mathfrak{p}}$.

Since prime ideals $\mathfrak{p}$ such that $M_{\mathfrak{p}} = 0$ are insignificant in this process, it is very natural to introduce the subset Supp M of Spec A consisting of the

prime ideals $\mathfrak{p}$ so that $M_\mathfrak{p} \neq 0$. This subset is called the *support* of M and is a geometric structure associated with M. In many case (*e.g.* when M is finitely generated) it is a closed subset.

The support of a module (*støtten til en modul*)

The localness of being zero

We shall see several applications of the local to global principles, but begin with the simplest of all properties, namely that of being zero! Applied to kernels and cokernels this leads to a local criterion for a homomorphism to be injective or surjective.

6.60 The point of departure is the following easy lemma that describes when elements remain non-zero in localizations.

Lemma 6.61 *Let M be an A-module and x and element in M. Assume that $\mathfrak{p}$ is a prime ideal in A. Then x does not map to zero in $M_\mathfrak{p}$ if and only if* $\operatorname{Ann} x \subseteq \mathfrak{p}$.

Proof: The module $M_\mathfrak{p}$ is M localized in the multiplicative set $S = A\backslash\mathfrak{p}$. Recall from Lemma 6.33 on page 136 that the image of x in $M_\mathfrak{p}$ being zero is equivalent to there being an element in $S = A\backslash\mathfrak{p}$ killing x; that is an element belonging to $\operatorname{Ann} x$ but not to $\mathfrak{p}$. ❑

This lemma immediately yields the following principle:

Proposition 6.62 *An A-module M equals zero if and only if $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ in A.*

That the ideals be maximal in the second condition can (of course) be replaced by they being prime.

Proof: One way is obvious. So assume that M is non-zero and let x be a non-zero element in M. Then the annihilator $\operatorname{Ann} x$ of x is a proper ideal as $x \neq 0$ and hence contained in a maximal ideal $\mathfrak{m}$. By the simple lemma above, the image of x in $M_\mathfrak{m}$ is non-zero and *a fortiori* $M_\mathfrak{m}$ is non-zero. ❑

Corollary 6.63 *A map $M \to N$ is injective (respectively surjective) if and only if $\phi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is injective (respectively surjective) for all maximal ideals $\mathfrak{m}$ in A.*

Proof: Localization is exact, so $(\ker\phi)_\mathfrak{m} = \ker(\phi_\mathfrak{m})$ and Proposition 6.62 above tells us that $\ker\phi = 0$ if and only if $\ker\phi_\mathfrak{m} = 0$ for all $\mathfrak{m}$. ❑

Corollary 6.64 *A map $\phi : M \to M$ is an isomorphism if and only if the localized map $\phi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is an isomorphism for all maximal ideals $\mathfrak{m}$.*

The support of a module

When we introduced the spectrum $\operatorname{Spec} A$ of a ring and gave it the Zariski topology, we associated a closed set $V(\mathfrak{a})$ with every ideal $\mathfrak{a}$ in A. It consisted of all the prime ideals $\mathfrak{p}$ in A such that $\mathfrak{a} \subseteq \mathfrak{p}$. One may interpreted this

in terms of localizations. A prime ideal $\mathfrak{p}$ belongs to $V(\mathfrak{a})$ precisely when $(A/\mathfrak{a})_\mathfrak{p} \neq 0$; just apply the simple lemma 6.61 to the element 1 in $A/\mathfrak{a}$.

This can be generalized to finitely generated modules; for any such module there is associated a closed subset of Spec A where the module is non-zero.

The support of a module (Sstøtten til en modul)

6.65 Given a module M, finitely generated or not. Recall that the *support* of M is denote by Supp M and consists of the prime ideals $\mathfrak{p}$ such that $M_\mathfrak{p} \neq 0$; that is,

$$\operatorname{Supp} M = \{\, \mathfrak{p} \in \operatorname{Spec} A \mid M_\mathfrak{p} \neq 0 \,\}.$$

Remember that elements of $M_\mathfrak{p}$ are all shaped like xs^{-1}, and such an element is zero precisely when $tx = 0$ for some $t \notin \mathfrak{p}$.

PROPOSITION 6.66 *If M is finitely generated A-module, the support* Supp M *equals the closed subset $V(\operatorname{Ann} M)$ of* Spec A*; that is, it consists of the prime ideals $\mathfrak{p}$ containing* Ann M.

PROOF: Our task is to show that $M_\mathfrak{p} \neq 0$ if and only if $\operatorname{Ann} M \subseteq \mathfrak{p}$, or equivalently, that $M_\mathfrak{p} = 0$ if and only if $\operatorname{Ann} M \nsubseteq \mathfrak{p}$. In case an element $a \in A$ kills M and does not belong to $\mathfrak{p}$, it holds true that $M_\mathfrak{p} = 0$ because a becomes invertible in $A_\mathfrak{p}$; this takes care of the if part of the proof. To attack the only if part, assume that $M_\mathfrak{p} = 0$, and let $x_1, \ldots, x_r$ be generators of M. By the simple lemma 6.61 above, there is for each of the x_i's an element s_i killing x_i, but not lying in $\mathfrak{p}$. The product s of the s_i's clearly kills M, and it does not belong to the prime ideal $\mathfrak{p}$ since none of the s_i's does. Therefore s is an element with the desired property. ❑

6.67 The hypothesis that M be finitely generated was used only in the last part of the proof, and it holds true for a general module M that Supp $M \subseteq V(\operatorname{Ann} M)$. The other inclusion may however fail when M is not finitely generated.

Examples

6.11 Clearly the support of a cyclic module $A/\mathfrak{a}$ equals the closed set $V(\mathfrak{a})$. Indeed, an element s lying in $\mathfrak{a}$, but not in $\mathfrak{p}$ would kill $A/\mathfrak{a}$ and hnece $(A/\mathfrak{a})_\mathfrak{p} = 0$.

6.12 One has Supp $\mathbb{Q}$ = Spec $\mathbb{Z}$ since $\mathbb{Q}_S = \mathbb{Q}$ for any multiplicative set S in $\mathbb{Z}$. More generally, for the fraction field K of any domain A it holds that Supp K = Spec A.

6.13 An example of this failure for "large modules", can be the $\mathbb{Z}$-module $\mathbb{Z}_{p^\infty} = \mathbb{Z}[p^{-1}]/\mathbb{Z}$ where p is a prime.

Every element of $\mathbb{Z}_{p^\infty}$ is killed by a power of p; indeed, an element x is the class of a rational number shaped Every element of $\mathbb{Z}_{p^\infty}$ is of the form $x = a/p^r$ with a prime to p. Since $ax \in \mathbb{Z}$ is and only if a is divisible by p^r, one has $\operatorname{Ann} x = (p^r)$ and from Lemma 6.61 above it follows that Supp $\mathbb{Z}_{p^\infty} = (p)\mathbb{Z}$.

Even though every element of $\mathbb{Z}_{p^\infty}$ is killed by a power of p, the annihilator of $\mathbb{Z}_{p^\infty}$ reduces to the zero ideal because no power of p kills the entire module $\mathbb{Z}_{p^\infty}$ (the power p^r kills p^{-n} only if $n \leqslant r$).

This shows that even though $\operatorname{Supp} \mathbb{Z}_{p^\infty}$ is closed, it differs from $V(\operatorname{Ann} \mathbb{Z}_{p^\infty})$.

6.14 The support is not always a closed subset of Spec A. Take any infinite sequence of primes p_i not including all primes—for instance, every second prime—and consider the module $M = \bigoplus_i \mathbb{Z}/p_i\mathbb{Z}$. The support of M is the infinite subset $\{(p_i)\}$. The only infinite closed subset of Spec $\mathbb{Z}$ being the entire spectrum, this set is not closed.

☆

The support of extensions

6.68 Since localisation is an additive functor so that $(M \oplus N)_\mathfrak{p} \simeq M_\mathfrak{p} \oplus N_\mathfrak{p}$ it is obvious that the support of a direct sum of two A-modules is the union of their supports. This generalises to so-called extensions; that is, modules in the midst of an exact sequence which is not necessarily split exact.

PROPOSITION 6.69 *Assume that*

$$0 \longrightarrow N \longrightarrow M \longrightarrow L \longrightarrow 0$$

is an exact sequence of A-modules. Then $\operatorname{Supp} M = \operatorname{Supp} N \cup \operatorname{Supp} L$.

PROOF: This follows immediately from localization functor being exact. For each prime $\mathfrak{p}$ the localized sequence

$$0 \longrightarrow N_\mathfrak{p} \longrightarrow M_\mathfrak{p} \longrightarrow L_\mathfrak{p} \longrightarrow 0$$

is exact, and the middle module vanishes if and only if the two extreme do. ❑

The support of a tensor product

6.70 The aim of this paragraph is the prove that the support of a tensor product is the intersection of the supports of the two factors, at least when the involved modules are finitely generated. The result hinges on Nakayama's lemma.

PROPOSITION 6.71 *Let M and N be two finitely generated A-modules. Then* $\operatorname{Supp} M \otimes_A N = \operatorname{Supp} N \cap \operatorname{Supp} M$.

We begin with a local lemma:

LEMMA 6.72 *Let A be a local ring with maximal idea $\mathfrak{m}$. Let M and N be two finitely generated A-modules. Then $M \otimes_A N = 0$ if and only if either $N = 0$ or $M = 0$.*

PROOF: The proof is an application of Nakayama's lemma. Let $k = A/\mathfrak{m}$ be the residue class field of A. Assume that both N and M are non-zero. Nakayama's lemma then ensures that both $N \otimes_A k$ and $M \otimes_A k$ are non-zero, and since base change respects tensor products (Proposition 5.35 on page 115), one has

$$(M \otimes_A N) \otimes_A k = (M \otimes_A k) \otimes_k (N \otimes_A k).$$

The tensor product of two non-zero vector spaces being non-zero (*e.g.* Proposition 5.20 on page 108), we infer that $(M \otimes_A N) \otimes_A k \neq 0$, and hence $N \otimes_A M \neq 0$ *a fortiori*. ❑

PROOF OF PROPOSITION 6.71: Since localization is an exact operation, the localized modules $N_\mathfrak{p}$ and $M_\mathfrak{p}$ are finitely generated over $A_\mathfrak{p}$ whenever M and N are finitely generated over A, and in view of the isomorphism

$$(M \otimes_A N)_\mathfrak{p} \simeq M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p},$$

the proposition then follows from the lemma. ❑

EXAMPLE 6.15 Proposition Proposition 6.71 may fail when one of the factors is not finitely generated. For instance, if one factor equals the fraction field K of a domain A and the other is of the form $A/\mathfrak{a}$ where $\mathfrak{a}$ is a non-trivial proper ideal, it holds true that $A/\mathfrak{a} \otimes_A K = 0$; hence $\operatorname{Supp} A/\mathfrak{a} \otimes_A K = \varnothing$, but the fraction field K is of global support (one has $K_\mathfrak{p} = K$ for all $\mathfrak{p} \in \operatorname{Spec} A$) so that $\operatorname{Supp} K \cap \operatorname{sup} A/\mathfrak{a} = V(\mathfrak{a})$, which is non-empty. ☆

PROBLEM 6.32 Let p be a prime number and let M be the abelian group $M = \bigoplus_{i \in \mathbb{N}_0} \mathbb{Z}/p^i\mathbb{Z}$. Determine the annihilator $\operatorname{Ann} M$ and the support $\operatorname{Supp} M$. ★

PROBLEM 6.33 An abelian group M is said to be of bounded exponent if some power p^n of a prime p kills every element of M. Give an example of a group of bounded exponent that is not finitely generated. Prove that if M is of bounded exponent, then $\operatorname{Supp} M = V(\operatorname{Ann} M)$. ★

PROBLEM 6.34 Let M be a finitely generated A-module. Prove that if $M \otimes_A A/\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ in A, then $M = 0$. HINT: Combine Nakayama's lemma with Proposition 6.62. ★

09/10/2018 Still Much work remaining; but the first section should be readable now. More follows!

10/10/2018 Added a exercise 6.8; Minor changes in the first section; brushed up the second section.

11/10/2018 Added prop 6.23 on page 130 and a new exercise 6.14 on page 131.

15/10/2018 Have moved the section about Nakayama's lemma to this chapter.

Lecture 7

Chain conditions

Preliminary version 1.2 as of 2018-11-01 at 10:16 (typeset 3rd December 2018 at 10:03am)—Much work remaining. Prone to misprints and errors and will change.
20/10/2018 Almost every thing has been redone!!
29/10/2018 Corrected a few misprints in lemma **??** in section about Krull's intersection theorem.
29/10/2018 Have added exercise 7.13 in connection with Krulls' intersection theorem. Several minor cahnges
01/11/2018 Added two exercises on page 172. Rewritten prop 7.50 on page 169. Added theorem 7.58 on page 172.

One of the great moments of mathematics was the appearance of Emmy Noether's paper *Idealtheorie in Ringbereichen* in 1921 where she introduced the ascending chain condition on ideals and proved the general version of the Primary Decomposition Theorem. The chain conditions turned out to be extremely useful, and today they permeate both commutative and non-commutative algebra.

Emmy Noether
(1882–1935)
German mathematician

7.1 Noetherian modules

We introduced the concept of chains in partially ordered sets already when discussing Zorn's lemma (in Paragraph 2.46 on page 39). Recall that a chain $\mathcal{C}$ in a partially ordered set Σ is just a linearly ordered subset; that is, a set such that any two members of the subset $\mathcal{C}$ are comparable.

7.1 In the present setting, when studying modules over a ring A, we give the term *chain* a more restrictive meaning. The chains we shall consider will all be countable and well ordered. For practical reasons two sorts of chains will be distinguished, ascending and descending ones. An *ascending chain* in M will be a sequence of submodules $\{M_i\}_{i\in\mathbb{N}_0}$ such that every term M_i is contained in in the successor M_{i+1}; or written out in a display, it is a chain of inclusions like

Ascending chains
(oppstigend kjeder)

$$M_0 \subseteq M_1 \subseteq \ldots \subseteq M_i \subseteq M_{i+1} \subseteq \ldots.$$

Similarly, a *descending chain* is a sequence $\{M_i\}_{i\in\mathbb{N}_0}$ of submodules fitting into a chain of inclusions shaped like

Descending chain
(nedstigende kjeder)

$$\ldots \subseteq M_{i+1} \subseteq M_i \subseteq \ldots \subseteq M_1 \subseteq M_0.$$

Such chains are said to be *eventually constant* or *eventually terminating* if the submodules become equal from a certain point on; that is, for some index i_0 it holds that $M_i = M_j$ whenever $i, j \geqslant i_0$. Common usage is also to say the chain *stabilizes* at i_0.

Eventually constant chains (*terminerende kjeder*)

7.2 An A-module M is said to be *Noetherian* if every ascending chain in M is eventually constant. This condition is frequently referred to as the *Ascending Chain Condition* abbreviated to ACC . The module is *Artinian* if every descending chain terminates, a condition also called the *Descending Chain Condition* with the acronym DCC .

Noetherian modules (*noetherske moduler*)

The Ascending Chain Condition (*Den oppstigende kjedebetingelsen*)

Artinian modules (*artinske moduler*)

The Descending Chain Condition (*Den nedstigende kjedebetingelser*)

A ring A is called *Noetherian* if it is Noetherian as module over itself, and of course, it is *Artinian* if it is Artinian as module over itself. The submodules of A are precisely the ideals, so A being Noetherian amounts to ideals of A satisfying the ACC, and similarly, A is Artinian precisely when the ideals comply with the DCC.

Noetherian and Artinian rings (*noetherske og artinske ringer*)

7.3 The two conditions, being Noetherian and Artinian, might look similar, but in fact there is a huge difference between the two. Noetherian and Artinian modules belong in some sense to opposite corners of the category Mod_A. In what follows we shall treat Noetherian modules and Noetherian rings and establish their basic properties, but will lack time to discuss the Artinian ones in any depth, although Artinian rings will be discussed (in section 7.5 below). In fact, according to a result of Akizuki, they turn out to be Noetherian as well.

7.4 The constituting property of Noetherian modules is the following theorem. It is due to Emmy Noether and appears as one of the main theorems in her famous paper from 1921.

Emil Artin (1898–1962) Austrian mathematician

PROPOSITION 7.5 (THE MAIN THEOREM FOR NOETHERIAN MODULES) *Let A be a ring and let M be a module over A. The following three conditions are equivalent:*

- *M is Noetherian; that is, it satisfies the ascending chain condition;*
- *Every non-empty family of submodules has a maximal element;*
- *Every submodule of M is finitely generated.*

PROOF: Assume first that M is Noetherian and let Σ be a non-empty set of submodules. We must prove that Σ has a maximal element. Assuming the contrary—that there is no maximal elements in Σ—one proves by an easy induction on the length that every finite chain in Σ can be strictly lengthened upwards. The resulting chain does not terminate, and the ACC is violated.

Next, suppose that every non-empty set of submodules in N possesses maximal elements. Our mission is to prove[1] that every submodule N is finitely generated. To that end, let Σ denote the set of finitely generated submodules. It is clearly non-empty (the zero modules is finitely generated) and consequently has a maximal element N_0. Let $x \in N$ be any element. The module

[1] Appealing to Zorn's lemma, from which the implication follows directly, would be using a sledgehammer to crack a nut. Apart from avoiding unduly use of brute force, it is of interest that the proposition is independent of the Axiom of Choice.

$Ax + N_0$ is finitely generated and contains N_0, so from the maximality of N_0 it ensues that $x \in N_0$. Hence $N = N_0$, and N is finitely generated.

For the third and last implication, assume that all submodules of N are finitely generated, and let an ascending chain

$$M_0 \subseteq M_1 \subseteq \ldots . \subseteq M_i \subseteq M_{i+1} \subseteq \ldots$$

be given. The union $N = \bigcup_i M_i$ is by assumption finitely generated and have say $x_1, \ldots, x_r$ as generators. Each x_j lies in some M_{ν_j}, and the chain being ascending, they all lie in M_ν with $\nu = \max_j \nu_j$. Therefore $N = M_\nu$, and the chain stabilizes at ν. ❑

7.6 It warrants a comment that Zorn's lemma is not used in the proof of families of submodules having maximal elements. As chains are eventually constant, we avoid problems with limit ordinals, and ordinary inductions works perfectly. As a consequence a large portion of the theory of Noetherian modules does not depend on the Axiom of Choice. Notably existence theorems like Theorem 2.50 on page 40 come for free for Noetherian rings.

7.7 The Noetherian modules, as do the Artinian modules, form a subcategory of Mod_A which enjoys a strong closedness property. They are what in category theory are called *thick subcategories*. Submodules and quotients of Noetherian modules are Noetherian as is an extension of two, and the same is true for Artinian modules.

PROPOSITION 7.8 *Let M', M and M'' be three A-modules fitting in the short exact sequence*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

Then the middle module M is Noetherian (respectively Artinian) if and only if the two extremal modules M' and M'' are.

In particular—as may be proven by a straightforward induction—finite direct sums of Noetherian (or Artinian) modules will be Noetherian (respectively Artinian), and *vice versa*: If a direct sum is Noetherian (or Artinian) it is finite and all the summands are Noetherian (or Artinian).

PROOF: We may without loss of generality identify M' with its image. Every chain in M' is of course a chain in M, so if M is Noetherian (or Artinian), the same is true for M'. In the same vein, if $\beta\colon M \to M''$ denotes the quotient map, a chain $\{N_i\}$ in M'' lifts to the chain $\{\beta^{-1}N_i\}$ in M. Since β is surjective, it holds that $\beta\beta^{-1}M_i = M_i$, and the former stabilizes whenever the latter does, so if M is Noetherian (or Artinian), M'' is as well.

To prove the remaining half of the proposition assume that the two extreme modules M' and M'' are Noetherian (or Artinian) and let $\{N_i\}$ be a chain in M. The chain $\{N_i \cap M'\}$ stabilizes at some ν, hence $N_i \cap M' = N_j \cap M'$ for $i, j \geqslant \nu$.

Mapping the N_i's into M'' one obtains the chain $\{\beta(N_i)\}$ in M'', and since M'' by assumption is Noetherian (or Artinian), it stabilizes at some μ. Hence

$\beta(N_i) = \beta(N_j)$ for $i, j \geqslant \mu$. For $i, j \geqslant \max \mu, \nu$ this gives

$$N_i/N_i \cap M' = \beta(N_i) = \beta(N_j) = N_j/N_i \cap M',$$

and hence $N_i = N_j$. ❑

7.9 The properties of being Noetherian or Artinian are retained when a module is localized. The setting is as follows: A is a ring with a multiplicative set S and M is an A-module. We let $\iota\colon M \to M_S$ denote the localization map.

PROPOSITION 7.10 *Let S be a multiplicative set in the ring A and let M be an A-module, if M is Noetherian or Artinian the localized module M_S is Noetherian or Artinian as well.*

PROOF: The proof is based on the simple observation that for any submodule $N \subseteq M_S$ one has $(\iota^{-1}N)_S = N$, which is clear since elements in N are of the form $\iota(y)s^{-1}$. Now, any chain $\{N_i\}$ in M_S, whether ascending or descending, induces a chain $\{\iota^{-1}N_i\}$ in M, and if this chain stabilizes, say $\iota^{-1}N_i = \iota^{-1}N_j$ for $i, j \geqslant i_0$, it holds true that $N_i = (\iota^{-1}N_i)_S = (\iota^{-1}N_j)_S = N_j$, and the original chain stabilizes at i_0 as well. ❑

EXAMPLE 7.1 *(Vector spaces)* A vector space V over a field k is Noetherian if and only if it is of finite dimension. Indeed, if V is of finite dimension it is the direct sum of finitely many copies of k, hence Noetherian.

If V is not of finite dimension one may find an infinite set $v_1, \ldots, v_r, \ldots$ of linearly independent vectors, and the subspaces $V_i =< v_1, \ldots, v_i >$ form a strictly ascending chain of subspaces; hence V is not Noetherian. A similar argument shows that neither is V Artinian: The spaces $W_j =< v_j, v_{j+1} \cdots >$ form a strictly decreasing chain of subspaces. ☆

EXAMPLE 7.2 *(Finite product of fields)* The conclusions of the preceding example extend to rings that are finite products of fields; say $A = \prod_{1 \leqslant i \leqslant r} k_i$. Modules over such rings are direct sums $V = \bigoplus_{1 \leqslant i \leqslant r} V_i$ where each V_i is a vector space over k_i with the A-module structure induced by the projection $A \to k_i$. From Proposition 7.8, or rather the succeeding comment, ensues that V is Noetherian (or Artinian) if and only if each V_i is of finite dimension over k_i. ☆

Problems

7.1 Prove the assertion just after Proposition 7.8 that if a direct sum of Noetherian modules is Noetherian, the sum is finite and all the summands are Noetherian.

7.2 Show that $\mathbb{Z}$ is a Noetherian $\mathbb{Z}$-module, but that $\mathbb{Z}_{p^\infty} = \mathbb{Z}[p^{-1}]/\mathbb{Z}$ is not. Show that $\mathbb{Z}_{p^\infty}$ is an Artinian $\mathbb{Z}$-module, but that $\mathbb{Z}$ is not.

7.3 let $\phi\colon A \to B$ be a map of rings and let M be a B-module. Prove that if M is Noetherian as a A-module, it is Noetherian as an B-module as well. Show by exhibiting examples that the converse is not true in general, but prove that the converse holds true when ϕ is surjective.

7.4 Show that a direct sum of finitely many simple modules is both Noetherian and Artinian.

★

7.2 *Noetherian rings*

Recall that a ring A is called *Noetherian* if it is Noetherian as a module over itself. The Noetherian rings form a large natural class of rings with a very rich theory. The lion's share of the rings appearing in classical algebraic geometry are of so-called *essential finite type* over a field k (or over a Noetherian ground ring); that is, they are localizations of finitely generated k-algebras. All these rings are Noetherian. Hilbert's basis theorem ensures that algebras finitely generated over a Noetherian base are Noetherian, and by Proposition 7.10 above localizing a ring preserves the property of being Noetherian.

Be aware that even having lots nice properties, Noetherian rings can be treacherous and show an unexpectedly bad behaviour. Local Noetherian rings, however, are rather tame and well-behaved animals.

7.11 The ring A being Noetherian means that any ascending chain of ideals eventually terminates. Applying Proposition 7.5 on page 152 to the ring A itself while remembering that the submodules of A are precisely the ideals, we arrive at the following:

PROPOSITION 7.12 (THE MAIN THEOREM FOR NOETHERIAN RINGS) *Let A be a ring. The following three conditions are equivalent:*

- *A is Noetherian, that is, the ideals in A comply to the ascending chain condition;*
- *Every non-empty family of ideals in A has a maximal element;*
- *Every ideal in A is finitely generated.*

It is trivial that fields are Noetherian and we shall shortly see that polynomial rings over fields are Noetherian; this is the celebrated Hilbert's Basis Theorem. Other examples are the principal ideal domains (see Exercise 7.6 below).

7.13 Quotients of Noetherian rings are Noetherian (Proposition 7.12), but subrings are not necessarily Noetherian. A stupid example being the fraction field of a non-noetherian domain, a more subtle example will be given below (Example 7.4).

PROPOSITION 7.14 *Let A be a noetherian ring and M an A-module. Then M is Noetherian if and only if M is finitely generated.*

PROOF: A finitely generated A-module M can be realized as the quotient of a finite direct sum nA of n copies of A. When A is Noetherian, it follows from Proposition 7.8 on page 153 that nA is Noetherian; indeed, one obtains nA by successive extensions of A by itself. By Proposition 7.8 again, quotients of nA are Noetherian as well.

Noetherian modules are finitely generated since all their submodules are (Proposition 7.5 on page 152). ❑

7.15 A converse to this proposition does not hold in the sense that rings may have Noetherian modules without being Noetherian; in fact, this applies to all non-Noetherian rings. Simple modules are Noetherian (all submodules are finitely generated!), and every ring possesses non-trivial simple modules by THE BASIC EXISTENCE THEOREM (Theorem 2.50 on page 40). These examples are in some sense illustrative; any Noetherian module over a non-Noetherian ring must have a non-trivial annihilator ideal; or phrased in another way, they can not be what are called *faithful* modules; that is, modules M with $\operatorname{Ann} M = (0)$.

Faithful modules (*trofaste moduler*)

PROPOSITION 7.16 *Assume that M is a module over A. If M is Noetherian, then $A/\operatorname{Ann} M$ is Noetherian as well.*

PROOF: Let $x_1, \ldots, x_r$ be generators for M, and consider the map $\phi\colon A \to rM$ sending x to the tuple $(x \cdot x_1, \ldots, x \cdot x_r)$. If x kills all the x_i's, it kills the entire module M, the x_i's being generators, and we infer that the kernel of ϕ equals the annihilator $\operatorname{Ann} M$. This means that $A/\operatorname{Ann} M$ is isomorphic to a submodule of rM, hence it is Noetherian by Proposition 7.8 above. ❑

Examples

7.3 The obvious example of a non-Noetherian ring is the ring $A[x_1, x_2, \ldots]$ of polynomials in infinitely many variables over any ring A. The chain of ideals

$$(x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, x_2, \ldots, x_i) \subset \ldots$$

does obviously not stabilize.

7.4 One might be mislead by the previous example to believe that non-noetherian rings are monstrously big. There are, however, non-noetherian rings contained in the polynomial ring $\mathbb{Q}[x]$. The simplest example is even a subring of the ring $\mathbb{Z}[p^{-1}][x]$ where p is a natural number greater than one. It is formed by those polynomials in $\mathbb{Z}[p^{-1}][x]$ that assume an integral value at zero; that is, the polynomials $P(x)$ such that $P(0) \in \mathbb{Z}$. In this ring A one finds the following ascending chain of principal ideals

$$(p^{-1}x) \subset (p^{-2}x) \subset \ldots \subset (p^{-i}x) \subset \ldots,$$

which does not stabilize. Indeed, if $p^{-(i+1)}x \in (p^{-i}x)$, one would have $p^{-(i+1)}x = P(x)p^{-i}x$ for some polynomial $P(x) \in A$. Cancelling $p^{-i}x$ would give $p^{-1} = P(x)$, which contradicts that $P(0) \in \mathbb{Z}$.

7.5 A large class of important non-Noetherian rings are formed by the rings $H(\Omega)$ of holomorphic functions in an open domain Ω in the complex plane. Chains that do not terminate arise from sequences of distinct points in Ω that do not accumulate in Ω. If $\{z_i\}$ is such a sequence, let $\mathfrak{a}_n$ be the ideal of functions in $H(\Omega)$ vanishing in the set $Z_n = \{z_{n+1}, z_{n+2}, \ldots\}$. These ideals clearly form an ascending chain, and from Weierstrass' Existence Theorem ensues that there are functions f_n holomorphic in Ω whose zeros are exactly the points in Z_n. Then $f_n \in \mathfrak{a}_n$, but $f_n \notin \mathfrak{a}_{n-1}$, and the chain can not stabilize at any stage.

☆

A structure theorem

As an illustration of the strength and elegance the Noetherian method can show, we offer a structure theorem for finitely generated modules over Noetherian rings- it does not reveal the fine features of a module , but rather describes the overall structure. Every such module is obtained by successive extensions of cyclic modules shaped like $A/\mathfrak{p}$ with $\mathfrak{p}$ a prime ideal.

7.17 The structure theorem builds on the following result which is of independent importance and will be use later.

PROPOSITION 7.18 *Assume that A is a Noetherian ring and M an A-module. Let* Ann x *be maximal among the annihilators of non-zero elements in M. Then* Ann x *is a prime ideal.*

PROOF: To begin with, observe that Ann x is a proper ideal as x is non-zero. Let then a and b be ring elements such that $ab \in$ Ann x and assume that $a \notin$ Ann x. Then $ax \neq 0$. It is generally true that Ann $x \subseteq$ Ann ax, but since $ax \neq 0$ it holds that Ann $x =$ Ann ax because Ann x is maximal among annihilators of non-zero elements. Now, $bax = 0$, so $b \in$ Ann $ax =$ Ann x. ❑

COROLLARY 7.19 *Any non-zero module over a Noetherian ring contains a module isomorphic to $A/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$.*

PROOF: The set of annihilators of non-zero elements is non empty and has a maximal element since A is Noetherian. Then we cite Proposition 7.18 above.

❑

7.20 The ground is now prepared for the announced structure theorem; here it comes:

PROPOSITION 7.21 *Let A a Noetherian ring and let M be a non-zero A module. Then M finitely generated if and only if it possesses a finite chain of submodules $\{M_i\}_{1\leqslant i\leqslant \nu}$ whose subquotients are shaped like cyclic modules $A/\mathfrak{p}_i$ with the $\mathfrak{p}_i$'s being prime; that is, there are short exact sequences*

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow A/\mathfrak{p}_i \longrightarrow 0$$

for $1 \leqslant i \leqslant \nu$.

PROOF: Let M be finitely generated A module. The set of submodules of M for which the theorem is true is non-empty by Corollary 7.19 and has thus a maximal element, say N. If N were a proper submodule, the quotient M/N would be non-zero and hence contain a submodule isomorphic to $A/\mathfrak{p}$ for some prime $\mathfrak{p}$. The inverse image N' of $A/\mathfrak{p}$ in M would be a submodule containing N and satisfying $N'/N \simeq A/\mathfrak{p}$, so the theorem would also hold for N' violating the maximality of N. ❑

Problems

7.5 Let $A \subseteq \mathbb{Q}$ be any proper subring. Show that the polynomials in $\mathbb{Q}[t]$ assuming values in A at the origin, is not Noetherian. ✲

7.6 Let A be a principal ideal domain. Show that A is Noetherian. HINT: If $\mathfrak{a}_i = (a_i)$ is an ascending chain, the union $\bigcup_i \mathfrak{a}_i$ is also principal. ✲

7.7 Let $\{A_1, \ldots, A_r\}$ be a finite family of Noetherian rings. Show that the product $\prod_i A_i$ is Noetherian. ✲

7.8 Let k be a field. Show that the product $\prod_{i\in\mathbb{N}} k$ of a countable numbers of copies of k is not Noetherian. ✲

7.9 Show that the ring of numerical polynomials in $\mathbb{Q}[x]$ is not Noetherian.

7.10 Let $\mathbb{A}$ be the subring of the complex numbers $\mathbb{C}$ whose elements are algebraic integers; that is, they are solutions of equations of the type

$$z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0$$

where the coefficients a_i are integers. Show that $\mathbb{A}$ is not Noetherian. HINT: For instance, the principal ideals $(\sqrt[2n]{2})$ form an ascending sequence that does not terminate.

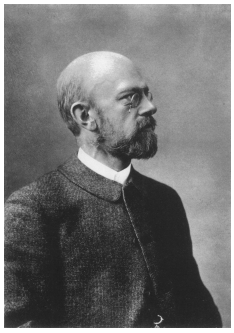
★

7.3 *Hilbert's Basis Theorem and two other results*

There is almost an infinity of strong results about Noetherian rings, unfortunately we have time to treat too few of them. As a beginning, in this section we shall discuss three. In addition to Hilbert's basis theorem, we treat a criterion for rings being Noetherian due to I.S. Cohen and finally give one of Wolfgang Krull's many important results, his intersection theorem.

Hilbert's Basis Theorem

As one might think the name indicates, Hilbert's Basis Theorem lies at the basis for the theory of commutative rings, and thereby is paramount for the development of algebraic geometry. It guarantees that most rings appearing in those parts of mathematics are Noetherian. However the name originate from the content of the theorem, that any ideal in a polynomial ring over a field has a finite basis—the modern version is that polynomial rings over Noetherian rings are Noetherian.



David Hilbert
(1862–1943)
German mathematician

Hilbert proved this theorem as early as in 1890. The proof was published in the paper *Über die Theorie der algebraischen Formen*. Naturally the formulation was slightly different from the modern one (the term Noetherian was of course not in use; Emmy Noether was only eight years old at the time), and the context was confined to polynomial rings over fields or specific rings like the integers, but the spirit was entirely the same. The abstract and non-constructive proof was revolting at a time when that part of mathematics was ruled by long and soporific computations, making it extremely difficult to obtain general results, and it opened up the path to modern algebra. Part of the mythology surrounding the theorem is the exclamation by the "König der Invariant Theorie" Paul Gordan: "Das ist nicht Mathematik, das ist Theologie!". The truth is that Hilbert had proved in a few pages what Gordan and his school had not proved in twenty years.

Paul Albert Gordan
(1837–1912)
German mathematician

7.22 There are several different proofs in circulation, and we shall give one of the shortest. These days many constructive proofs are known and good algorithms exist for exhibiting explicit generators for ideals in polynomial rings; however, we shall present a non-constructive proof in the spirit of Hilbert's.

Theorem 7.23 (Hilbert's Basis Theorem) *Assume that A is a Noetherian ring. Then the polynomial ring $A[x]$ is Noetherian.*

Before giving the proof of Hilbert's basis theorem we state three important corollaries. A straightforward induction on the number variables immediately yields the following:

Corollary 7.24 *Assume that A is a Noetherian ring. Then the polynomial ring $A[x_1, \ldots, x_n]$ is Noetherian.*

An important special case is when the ground ring A is a field. Since fields are Noetherian, the Basis Theorem tells us that polynomial rings over fields are Noetherian. Moreover, quotients of Noetherian rings are Noetherian, and we obtain directly the next corollary. In particular it says that algebras of finite type over a field, a class of rings that include the coordinate rings of affine varieties, are Noetherian.

COROLLARY 7.25 *Any algebra finitely generated over a Noetherian ring is Noetherian.*

Finally, the last corollary we offer before giving the proof of Hilbert's Basis Theorem, combines that theorem with Proposition 7.10 on pag 154 which states that localization preserves Noetherianess. Recall that and A-algebra is said to be *essentially of finite type* if it is the localization of a finitely generated A-algebra.

COROLLARY 7.26 *Any ring essential of finite type over a Noetherian ring is Noetherian.*

PROOF OF HILBERT'S BASIS THEOREM: Let $\mathfrak{a}$ be an ideal in $A[x]$ and for each n let $\mathfrak{a}_n$ be the set of leading coefficients of elements from $\mathfrak{a}$ of degree at most n. Each $\mathfrak{a}_n$ is an ideal in A, and they form an ascending chain which eventually stabilizes, say for $n = N$. Each $\mathfrak{a}_n$ is finitely generated, so for each $n \leqslant N$ we may chose a finite set of polynomials of degree at most n whose leading coefficients generate $\mathfrak{a}_n$. Let $f_1, \ldots, f_r$ be all these polynomials in some order and let $a_1, \ldots, a_r$ be their leading coefficients.

We contend that the f_i's generate $\mathfrak{a}$. So assume not, and let f be of minimal degree n among those polynomials in $\mathfrak{a}$ that do not belong to the ideal generated by the f_i's. If the leading coefficient of f is a, it holds that $a \in \mathfrak{a}_n$ and we may write $a = \sum_j b_j a_{i_j}$ with the f_{i_j}'s corresponding to a_{i_j} of degree at most the degree of f. Then $f - \sum_j b_j x^{(\deg f - \deg f_{i_j})} f_{i_j}$ is of degree less than $\deg f$ and does not lie in the ideal generated by the f_i's since f does not contradicting the minimality of $\deg f$. ❑

Cohen's criterion

One may wonder if there are conditions only involving prime ideals that ensure a ring be Noetherian. An ACC-condition on prime ideals is far from sufficient; there are non-Noetherian rings with merely one prime ideal. For instance, let $\mathfrak{m}$ be the ideal generated by all the variables x_i in the ring $k[x_1, x_2, \ldots]$ of polynomials in infinitely many variables. The quotient $k[x_1, x_2, \ldots]/\mathfrak{m}^2$ has only one prime ideal, namely the one generated by the images of all the variables, but is not Noetherian since that prime ideal is not finitely generated. However, a result of Irvin Cohen's tells us that for a ring to be Noetherian it suffices that the prime ideals are finitely generated.

7.27 We begin with stating a lemma about maximal ideals that are not finitely generated; it joins the line of results of type ideals maximal subjected to some condition being prime:

LEMMA 7.28 *Let $\mathfrak{a}$ be maximal among the ideals in A that are not finitely generated. Then $\mathfrak{a}$ is a prime ideal.*

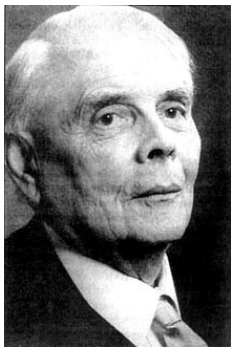
Cohen's criterion ensues easily from this lemma:

PROPOSITION 7.29 *Assume that all prime ideals in the ring A are finitely generated. Then A is Noetherian.*

PROOF: Assume that A is not Noetherian. The set of ideals that are not finitely generated is then non-empty and according to Zorn's lemma has a maximal element, say $\mathfrak{a}$; indeed, if the union $\bigcup_i \mathfrak{a}_i$ of an ascending chain of ideals were finitely generated, the chain would stabilize (argue as in the last part of the proof of Proposition 7.12 on page 155) and a member of the chain would be finitely generated. From the lemma we infer that $\mathfrak{a}$ is prime, which is a flagrant contradiction. ❑

PROOF OF LEMMA 7.28: The ring $A/\mathfrak{a}$ is Noetherian since all its ideals are finitely generated. Let a and a' be two members of A and assume that the product aa' lies in $\mathfrak{a}$, but that neither a nor a' lies there. Let $\mathfrak{c} = \mathfrak{a} + (a)$ and $\mathfrak{c}' = \mathfrak{a} + (a')$. These ideals both contain $\mathfrak{a}$ properly and are therefore finitely generated by the maximality of $\mathfrak{a}$, moreover it holds that $\mathfrak{c}\mathfrak{c}' \subseteq \mathfrak{a}$ because $aa' \in \mathfrak{c}$. The quotient $\mathfrak{c}/\mathfrak{c}\mathfrak{c}'$ is a finitely generated module over $A/\mathfrak{a}$, and contains $\mathfrak{a}/\mathfrak{c}\mathfrak{c}'$. Hence $\mathfrak{a}/\mathfrak{c}\mathfrak{c}'$ is finitely generated, and by consequence $\mathfrak{a}$ since $\mathfrak{c}\mathfrak{c}'$ is finitely generated. ❑

Krull's intersection theorem



Wolfgang Krull (1899–19715) German mathematician

The German mathematician Wolfgang Krull was one of the greatest contributor to the development of algebra in the years between the two World Wars, and in this section we shall discuss one of his most famous results, the so-called the "Krull's intersection theorem". In its simplest form, the theorem asserts that all the powers $\mathfrak{a}^\nu$ of a proper ideal $\mathfrak{a}$ in a local Noetherian ring do not have common elements apart from 0; that is, it holds true that $\bigcap_\nu \mathfrak{a}^\nu = 0$.

There are several proofs of Krull's intersection theorem, and the one we give is among the shortest possible with the means at hand at the present stage of the course. There is a really short an elegant proof for the case of the ring itself due to Hervé Perdry which we present as Exercise 7.13.

EXAMPLE 7.6 To motivate and illustrate the reasons behind the result, let us consider the ring of complex polynomials $\mathbb{C}[x_1, \ldots, x_r]$ and a point $a = (a_1, \ldots, a_r)$ in $\mathbb{C}^r$. The ideal $\mathfrak{m} = (x_1 - a_1, \ldots, x_r - a_r)$ consists precisely of the polynomials that vanish at a, and the members of the powers $\mathfrak{m}^\nu$ are those that

vanish to the ν-th order. In this simple situation Krull's theorem expresses the well-known and obvious fact that no non-zero polynomial vanishes to all orders. Of course, Krull's result is a vast generalization of this prosaic example; ideals in local Noetherian rings are infinitely more intricate than maximal ideals in a ring of complex polynomials. ☆

7.30 The show begins with a technical lemma, and again submodules maximal subjected to a specific condition enter the scene:

LEMMA 7.31 *Let $\mathfrak{a} \subseteq A$ be a finitely generated ideal. Let M be a Noetherian A-module and N a submodule. If K is submodule of M maximal subjected to the condition $K \cap N = \mathfrak{a}N$, then $\mathfrak{a}^\nu M \subseteq K$ for some $\nu \in \mathbb{N}$.*

PROOF: Since $\mathfrak{a}$ is finitely generated, it suffices to show that $x^\nu M \subseteq K$ for every $x \in \mathfrak{a}$ and ν sufficiently big. By the maximality of K, it suffices to prove that $(x^\nu M + K) \cap N = \mathfrak{a}N$. The crucial inclusion is $(x^\nu M + K) \cap N \subseteq \mathfrak{a}N$, the other being clear as $\mathfrak{a}N = K \cap N$.

Now, the submodules $(K : x^i)$ form an ascending chain which since M is Noetherian stabilizes at say ν; so that $(K : x^\nu) = (K : x^{\nu+1})$. If $y = x^\nu m + k$ with $m \in M$ and $k \in K$, is a member of $(x^\nu M + K) \cap N$ it holds that $xy \in xN \subseteq K \cap N$ from which ensues that $m \in (K : x^{\nu+1})$ since $xy = x^{v+1}m + xk$. Hence $m \in (K : x^\nu)$, and $y \in K \cap N = \mathfrak{a}N$. ❑

PROPOSITION 7.32 *Suppose that A is a ring, that $\mathfrak{a}$ is a finitely generated ideal in A and that M is a Noetherian module over A. Putting $N = \bigcap_i \mathfrak{a}^i M$, one has $\mathfrak{a}N = N$.*

PROOF: Because M is Noetherian, there is a maximal submodule K of M such that $K \cap N = \mathfrak{a}N$. By the lemma it holds that $\mathfrak{a}^\nu M \subseteq K$ for some natural number ν. Because $N \subseteq \mathfrak{a}^\nu M$, i holds that $N \subseteq K$, and consequently $N = N \cap K = \mathfrak{a}N$. ❑

7.33 Combining Proposition 7.32 above with Nakayama's lemma, we obtain the classical version of Krull's intersection theorem:

THEOREM 7.34 (KRULL'S INTERSECTION THEOREM) *Let A be ring and $\mathfrak{a}$ an ideal contained in the Jacobson radical of A. Assume that $\mathfrak{a}$ is finitely generated. If M is a Noetherian A-module, it holds true that $\bigcap_i \mathfrak{a}^i M = 0$.*

PROOF: Let $N = \bigcap_i \mathfrak{a}^i M$. Then $\mathfrak{a}N = N$ after Proposition 7.32, and we may finish by applying Nakayama's lemma (Proposition 6.50 on page 140) since N is a submodule of the Noetherian module M and therefore is finitely generated. ❑

COROLLARY 7.35 *Let A be a Noetherian ring and $\mathfrak{a}$ an ideal contained in the Jacobson radical of A. Then $\bigcap_i \mathfrak{a}^i = 0$. In particular, if A is a Noetherian local ring whose maximal ideal is $\mathfrak{m}$, one has $\bigcap_i \mathfrak{m}^i = 0$.*

7.36 In general it is not true that the intersection of successive powers of an ideal vanishes even when the ring is Noetherian and the ideal is proper. Principal ideals generated by non-zero idempotents e furnish simple counter examples. If $\mathfrak{a} = (e)$ with e idempotent, one has $\mathfrak{a}^2 = \mathfrak{a}$ and a straightforward induction shows that $\mathfrak{a}^i = \mathfrak{a}$ for all i. Hence $\bigcap_i \mathfrak{a}^i = \mathfrak{a}$. However, the powers of proper ideals in Noetherian integral domains have vanishing intersections:

COROLLARY 7.37 *Assume that $\mathfrak{a}$ is a proper ideal in the Noetherian integral domain A, then $\bigcap_i \mathfrak{a}^i = 0$.*

PROOF: We combine Proposition 7.32 above by the extended Nakayama's lemma (Proposition 6.59 on page 142) and exhibit an element $a \in \mathfrak{a}$ so that $(1 + a)N = 0$ where $N = \bigcap_i \mathfrak{a}^i$. But $\mathfrak{a}$ being proper, $1 + a$ is non-zero, and consequently $N = 0$ since A is an integral domain. ❑

Problems

7.11 The aim in this exercise is to exhibits a domain A with a maximal ideal $\mathfrak{m}$, which is principal, such the intersection $\bigcap_i \mathfrak{m}^i$ is non-zero. It is in some a minimal example of this behaviour, and illustrates how Krull's intersection theorem (may) fail in non-noetherian rings.

Let $k[T, X_1, X_2 \ldots]$ be the ring of polynomials in infinite many variables having coefficients in the field k. Consider the quotient $A = k[T, X_1, X_2, \ldots]/\mathfrak{a}$ by the ideal $\mathfrak{a}$ generated by the polynomials $X_i - TX_{i+1}$ for $i \in \mathbb{N}$. That is, the ideal $\mathfrak{a}$ is given as $\mathfrak{a} = (X_1 - TX_2, X_2 - TX_3, \ldots)$. As usual, letting lower case letters, in the present case t and the x_i's, stand for the classes of their upper case counterparts, the equalities $x_i = tx_{i+1}$ hold in A.

a) Show that $\mathfrak{m} = (t)A$ is a maximal ideal and that the ideal $\mathfrak{p} = (x_1, x_2, \ldots)$ generated by all the x_i's is a prime ideal contained in $\mathfrak{m}$.

b) Prove that $\bigcap_i \mathfrak{m}^i = \mathfrak{p}$.

c) Let B be a domain containing k in which there is a principal ideal $\mathfrak{a} = (f)$ such that $\bigcap_i \mathfrak{a}^i \neq (0)$. Show that there is a map of k-algebras $A \to B$.

7.12 Let A be a local ring with maximal ideal $\mathfrak{m}$. Assume that $\mathfrak{m}$ is a principal ideal. Prove that if $\bigcap_i \mathfrak{m}^i = (0)$, then the powers $\mathfrak{m}^i$ are the only ideals in A. Prove that A is Noetherian if and only if $\bigcap_i \mathfrak{m}^i = (0)$.

7.13 *(Perdry's proof of Krull's intersection theorem.)* Let $\mathfrak{a}$ be an ideal in a Noetherian ring A and assume that $x \in \bigcap_i \mathfrak{a}^i$. The aim of the exercise is to prove that $x \in x \cdot \mathfrak{a}$. Assume that $a_1, \ldots, a_r$ are generators for $\mathfrak{a}$.

a) Let $v \in \mathbb{N}$ be a natural number. Use that $x \in \mathfrak{a}^v$ to prove there is a homogenous polynomial $P_v(x_1, \ldots, x_r)$ of degree v in $A[x_1, \ldots, x_r]$ so that $x = P(a_1, \ldots, a_r)$.

b) Let $\mathfrak{c}_n$ be the ideal in $A[x_1, \ldots, x_r]$ generated by $P_1, \ldots, P_n$. Show there is an N so that $\mathfrak{c}_{N+1} = \mathfrak{c}_N$.

c) Show that one has a relation $P_{N+1} = \sum_{1 \leqslant i \leqslant N} Q_i \cdot P_i$ where the Q_i's are homogenous polynomials of positive degree.

d) Conclude that $x \in x\mathfrak{a}$.

e) Deduce hat $\bigcap_i \mathfrak{a}^i = 0$ if $\mathfrak{a}$ is contained in the Jacobson radical of A.

7.14 Let p be a prime number and let $A_0 = \mathbb{Z}_{(p)}$ and $\mathfrak{m}_0 = (p)\mathbb{Z}_{(p)}$. Let $A_n = A_0[p^{1/n}]$ be the ring obtained by adjoining a n-th root of p to A_0.

a) Show that A_n is local wih $\mathfrak{m}_n$ as sole macximal ideal. HINT: show that $\mathfrak{m} \cap A_0 = \mu_0$

★

7.4 *Modules of finite length*

Finite dimensional vector space are civilized creatures having several features that make them pleasant to work with, one being that they have a dimension. Over any ring there is a class of modules with a numerical invariant attached resembling the dimension of a vector space. This invariant is called *the length*, and the modules in question are said to be of *finite length*. Modules do not possess bases in general, so it is a lot more involved to define the length than the dimension. The trick is to use *maximal chains* of submodules, maximal in the sense that there is no room for inserting new modules in the chain.

Maximal chains (*maksimale kjeder*)

7.38 An ascending chain $\{M_i\}$ in an A-module M is called a *composition series* if all of its subquotients M_{i+1}/M_i are simple modules. Even though most composition series we shall meet are finite, we do not exclude they being infinite. By convention simple modules are non-zero, so in particular the inclusions $M_i \subsetneq M_{i+1}$ are strict. A finite composition series when displayed appears like

Composition series (*komposisjonsserier*)

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_{n-1} \subseteq M_n = M,$$

where each subquotient M_{i+1}/M_i is shaped like $A/\mathfrak{m}_i$ for some maximal ideal $\mathfrak{m}_i$ in A. The number n is called the *the length* of the series; it is the number of non-zero constituencies of the series. In case the series is infinite, the length is of course said to be infinite. More generally, *the length* of any finite chain will be the number of inclusions; that is, one less than the number of modules.

The length of a composition series (*lengden av en komposisjonskjede*)

The length of a chain (*lengden av en kjede*)

Being a composition series is equivalent to being a maximal chain as described in the introduction to this section; that is, no module is lying strictly

between two consecutive terms of the chain. Would-be submodules in-between M_i and M_{i+1} would we in a one-to-one correspondence with submodules of M_{i+1}/M_i with a submodule N corresponding to the quotient N/M_i, but as each M_{i+1}/M_i is simple, there are none. The term *saturated* is also a common usage for suchlike chains.

Saturated chains (*mettede kjeder*)

7.39 The main result of this section is that once a module has one finite composition series, they are all finite and have the same length. This is a result of Jordan-Hölder type, but one on the weak side—the true Jordan-Hölder theorem states that the subquotients of any two composition series are the same up to a permutation. The original Jodan-Hölder theorem is about (finite) groups, but one finds analogues in many categories, so also in the subcategory of Mod_A of finite lengths modules.

THEOREM 7.40 (WEAK JORDAN-HÖLDER) *Assume that M has a finite composition series. Then all composition series in M are finite and they have the same length.*

The common length of the composition series is called the *length* of the module and denoted $\ell_A(M)$; for modules not being of finite length this means that $\ell_A(M) = \infty$. As a matter of pedantry, the zero module[2] is considered to be of finite length and its length is zero (what else?).

The length of modules (*lengden til moduler*)

[2] This is just a formality: By convention, the zero module is not included among the simple modules and does therefore not have a composition series!

PROOF: The proof goes by induction on the length of the shortest composition series in a module; this is well defined and finite for all modules concerning us. A module having a composition series of length one is simple, and for those the theorem is obviously true. The induction can begin and the fun can start.

Let $\mathcal{M} = \{M_i\}$ be a composition series of minimal length n in M which displayed is shaped like

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M.$$

The image of $\mathcal{M}$ in the quotient M/M_1 is one shorter than $\mathcal{M}$, hence all composition series in M/M_1 are of length $n-1$ by induction. Denote by $\beta\colon M \to M/M_1$ the quotient map.

Given another another composition series $\mathcal{N} = \{N_j\}$ in M. Its length r is at least n, and by induction its image in M/M_1 is of length $n-1$. Consequently at least one of the inclusions in $\mathcal{N}$ becomes an equality in M/M_1; that is, for some index ν it holds that $\beta(N_\mu) = \beta(N_{\mu+1})$, and we pick ν to be the least such index. Then $\beta(\mathcal{N})$ displays as

$$0 = \beta(N_0) \subsetneq \beta(N_1) \subsetneq \ldots \subsetneq \beta(N_\nu) = \beta(N_{\nu+1}) \subseteq \ldots \subseteq \beta(N_r) = M. \tag{7.1}$$

We contend that there is just one index μ for which equality occurs— this is the fulcrum of the proof from which it clearly ensues that $r = n$; indeed, on the one hand, the length of $\beta(\mathcal{N})$ is one less than that of $\mathcal{N}$ and on the other, it equals $n-1$ by induction .

From the equality $\beta(N_\nu) = \beta(N_{\nu+1})$ comes the equality $N_\nu + M_1 \cap N_{\nu+1} = N_{\nu+1}$, and M_1 being simple, either $M_1 \cap N_{\nu+1}$ vanishes or equals M_1. It cannot vanish, however, because $N_\nu \neq N_{\nu+1}$, and thus we infer that $M_1 \subseteq N_{\nu+1}$. It follows that there are strict inclusions $\beta(N_j) \subsetneq \beta(N_{j+1})$ for $j \geqslant \nu + 1$, and hence all inclusions in $\beta(\mathcal{N})$ are strict except the one at stage ν. ❑

7.41 A closer look at the proof above reveals that it as well gives the full Jordan-Hölder theorem:

THEOREM 7.42 (TRUE JORDAN-HÖLDER) *Any two composition series of a module of finite length have the same subquotients up to order.*

PROOF: We continue with the above proof and go on with induction on the length; hence the two series $\beta(\mathcal{M})$ and $\beta(\mathcal{N})$ have the same subquotients up to order. Now, the subquotients of $\mathcal{M}$ and $\beta(\mathcal{M})$ differ only at the bottom stage M_1, so $\mathcal{M}$ has the subquotient M_1 in addition to those shared with $\beta(\mathcal{M})$. On the other hand, the subquotients of $\mathcal{N}$ and $\beta(\mathcal{N})$ coincide except at stage ν, but in the proof above, we showed that $N_v + M_1 = N_{v+1}$, and the additional subquotient of $\mathcal{N}$ is M_1 as well. ❑

7.43 Just like the dimension of vector spaces the length is additive along short exact sequence, and this is an indispensable property making it possible to compute the length in many cases. Observe also that a submodule (or a quotient) of M having the same length as M must be equal to M.

PROPOSITION 7.44 (ADDITIVITY OF LENGTH) *Given a short exact sequence of A-modules*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

Then M is of finite length if and only if the two others are, and it holds true that $\ell_A(M) = \ell_A(M') + \ell_A(M'')$.

PROOF: Firstly, assume M is of finite length. Pushing a finite composition series forward[3] along β gives one in M'' and pulling it back along α gives one in M'. Assume next that the two modules on the side are of finite length. It suffices to exhibit one composition series of M with the additive property. To this end, we begin with one in M'', say $\{M''_i\}$, and pull it back to M along β. The smallest module in the pulled back chain is $\beta^{-1}M''_0 = \beta^{-1}(0)$, which equals M', so we may splice $\{\beta^{-1}M''_i\}$ with any composition series of M' to obtain one in M, and obviously, the length of the spliced series equals the sum of lengths of the two being spliced. ❑

[3] Of course, not repeating terms that become equal in ″

7.45 An immediate corollary of Proposition 7.44 is that modules of finite length are both Noetherian and Artinian. Obviously this is true for simple modules (no submodules, no chains) and hence follows in general by a straightforward induction on the length using Proposition 7.8 on page 153. The converse holds as well:

PROPOSITION 7.46 *An A-module M is of finite length if and only if it is both Noetherian and Artinian.*

PROOF: Assume M both Noetherian and Artinian. Since M is Artinian every non-empty set of submodules has a minimal element, so if M is not of finite length, there is a submodule, N say, minimal subjected to being non-zero and not of finite length. It is finitely generated because M is Noetherian and hence Nakayama's lemma applies: There is surjection $\phi\colon M \to k$ onto a simple module k. The kernel of ϕ is of finite length by the minimality of N, and hence N itself is of finite length by Proposition 7.44 above. ❑

7.47 Be aware that the base ring A is a serious part of the game and can have a decisive effect on the length of a module. If $A \to B$ is a map of rings and M a B-module which is of finite length over both A and B, there is in general no reason that $\ell_A(M)$ and $\ell_B(M)$ should agree. Already when $k \subseteq K$ is a finite non-trivial extension of fields the two lengths differ in that $\dim_K V = [K;k] \cdot \dim_k V$ for vector spaces over K. You will find a simple but slightly more subtle example in Example 7.10 below. And of course there are stupid examples like $\mathbb{Q} \subseteq \mathbb{R}$ with $\mathbb{R}$ being of length over itself, but as a module over $\mathbb{Q}$ its length is infinite (even uncountable!)

However, when the map $A \to B$ is surjective, the two lengths agree since then the B-submodules and the A-submodules of M coincide.

7.48 Unlike what is true for vector spaces, module of the same length need not be isomorphic. A simple example are the $\mathbb{Z}$-modules $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. They are all of length one but not two are isomorphic!

Examples

7.7 *(Vector spaces)* Over fields, of course the length of modules coincide with their vector space dimensions. In a similar fashion, if the A-module M is killed by a maximal ideal $\mathfrak{m}$ in A, and therefore is a vector space over the field $A/\mathfrak{m}$, one has $\ell_A(M) = \dim_{A/\mathfrak{m}} M$.

7.8 *(Finite groups)* The only abelian groups that are of finite length are the finite groups. They are all direct sums of cyclic groups of shape $\mathbb{Z}/p^\nu\mathbb{Z}$ where p is a prime and ν a natural number; that is such a group M enjoys a direct sum decomposition

$$M = \bigoplus_i \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}.$$

We contend that $\ell_{\mathbb{Z}}(M) = \sum_i \nu_i$. By additivity of the length it suffices to show that for a each prime p the length of $\mathbb{Z}/p^\nu\mathbb{Z}$ is given as $\ell_A(\mathbb{Z}/p^v\mathbb{Z}) = v$, and this one does by an induction argument based on the standard[4] mod p^ν. short exact sequences

$$0 \longrightarrow \mathbb{Z}/p^{\nu-1}\mathbb{Z} \xrightarrow{\ p\ } \mathbb{Z}/p^v\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

[4] The map p is close to being a "multiplication-by- p-map"; it sends a class $[x]_{p^{\nu-1}}$ mod $p^{\nu-1}$ to the class $[px]_{p^\nu}$

Since $\ell_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) = 1$, the length $\ell_A(\mathbb{Z}/p^\nu\mathbb{Z})$ increases by one when ν increases by one, and we are done.

7.9 Let $A = k[x, y]$ and $M_n = k[x, y]/\mathfrak{m}^n$. Then there are exact sequences like

$$0 \longrightarrow \mathfrak{m}^{n-1}/\mathfrak{m}^n \longrightarrow M_n \longrightarrow M_{n-1} \longrightarrow 0$$

so that $\ell_A(M_n) = \ell_A(M_{n-1}) + \dim_k \mathfrak{m}^{n-1}/\mathfrak{m}^n = \ell_A(M_n) + n$ and by induction one finds

$$\ell_A(M_n) = \sum_{i=1}^{n} i = \binom{n+1}{2}$$

7.10 We let $A = \mathbb{Z}$ and $B = \mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$ and let $M = \mathbb{Z}[i]/(105)\mathbb{Z}[i]$. The prime factorization of 105 is $105 = 3 \cdot 5 \cdot 7$, and one checks easily that $x^2 + 1$ is irreducible mod 3 and 7 but decomposes over $\mathbb{F}_5$; hence the Chinese remainder theorem gives a decomposition

$$M = \mathbb{F}_3(i) \oplus \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_7(i),$$

and we conclude that $\ell_{\mathbb{Z}}(M) = 6$ but $\ell_{\mathbb{Z}[i]}(M) = 4$. (The primes 3 and 7 persist being primes in $\mathbb{Z}[i]$, but 5 splits up in the product $5 = (2+i)(2-i)$.)

☆

Problems

7.15 A frequently met situation in algebraic geometry is that a ring A is a k-algebra; that is, it contains a ground field k (for instance, algebras like $k[x_1, \dots, x_r]/\mathfrak{a}$ are of this type). Then any A-module is a vector space over k. Assume that A in addition to being a k-algebra is local ring. Denote the maximal ideal by $\mathfrak{m}$ and let $k(\mathfrak{m}) = A/\mathfrak{m}$ be the residue class field. ✲

a) Assume that k maps isomorphically onto $k(\mathfrak{m})$. Prove that a module M is of finite length over A if and only if is of finite dimension over k and in case it holds true that $\dim_k M = \ell_A(M)$.

b) Assume merely that $k(\mathfrak{m})$ is finite extension of the image of k. Prove that $\dim_k M = [k(\mathfrak{m}) : k] \cdot \ell_A(M)$.

7.16 *(Modules of finite length over finite product of fields.)* Let $A = \prod_{1 \leqslant i \leqslant r} k_i$ be a finite product of fields. Show that an A-module $V = \bigoplus_{1 \leqslant i \leqslant r} V_i$, where V_i is a vector space over k_i, is of finite length if and only if V_i is of finite dimension over k_i, and in case it holds true that ✲

$$\ell_A(\bigoplus_i V_i) = \sum_i \dim_{k_i} V_i.$$

7.17 Show that the the length $\ell_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})$ equals the number of prime factors of n (counted with multiplicity). ✲

7.18 *(Modules of finite length over PID's.)* Let A be PID and let $f \in A$ be an element. Show that $\ell_A(A/(f)A)$ is the number of prime factors in f (counted with multiplicity).

7.19 Assume that M is an A-module of finite length and that $\mathfrak{a}$ is an ideal contained in the Jacobson radical of A. Show that for some integer n it holds true that $\mathfrak{a}^n M = 0$. HINT: Consider the descending chain $\mathfrak{a}^i M$ and remember Nakayama's lemma.

Finite length and support

7.49 We finish of the story about modules of finite length with a criterion for a module being of finite length in terms of the support of the module, and a structure theorem, essentially saying that a module is of finite length is just a finite direct sum of "local contributions"—but of course, it says nothing about how the local contributions are shaped.

PROPOSITION 7.50 *A finitely generated module M over a Noetherian ring is of finite length if and only if its support* Supp M *is a finite union of closed points.*

Recall that the closed points in Spec A are precisely the maximal ideals. It may well happen that a subset of Spec A is closed and finite without all points being closed; for instance, Spec $\mathbb{Z}_{(p)}$ is finite.

PROOF: Assume to begin with that M is of finite length and let $\{M_i\}$ be a composition series. Then citing Proposition 6.69 on page 146 we infer that $\operatorname{Supp} M = \bigcup_i \operatorname{Supp} M_i/M_{i+1} = \bigcup_i \{\mathfrak{m}_i\}$ where $M_i/M_{i+1} \simeq A/\mathfrak{m}_i$ are the subquotients of the composition series $\{M_i\}$. So the support is a finite union of closed points.

For the other implication we resort to the Structure Theorem 7.21 on page 158 assuring there is a descending chain $\{M_i\}$ of submodules in M whose subquotients are shaped like $A/\mathfrak{p}_i$ with $\mathfrak{p}_i$ being prime. Again by Proposition 6.69 on page 146 it holds that $\operatorname{Supp} M = \bigcup_i V(\mathfrak{p}_i)$. Now, if M is of finite length, the the subquotients $A/\mathfrak{p}_i$'s will be as well, and by the lemma below, all the $\mathfrak{p}_i$'s must be maximal. Hence Supp M is finite. ❑

LEMMA 7.51 *Assume that an integral domain A is Artinian, then A is a field.*

PROOF: Let $f \in A$ be a non-zero member of A. The principal ideals (f^i) form a descending chain and is ultimately constant since A is artinian; *i.e.* $(f^{\nu+1}) = (f^\nu)$ for some ν. Then $f^\nu = af^{\nu+1}$ for some $a \in A$, and cancelling f^ν, which is permissible as A is a domain, we find $1 = af$; *i.e.* f is invertible. ❑

COROLLARY 7.52 (STRUCTURE OF FINITE LENGTH MODULES) *Assume that M is of finite length over the ring A. Then there is a canonical isomorphism*

$$M \simeq \bigoplus_{\mathfrak{m} \in \operatorname{Supp} M} M_{\mathfrak{m}}.$$

PROOF: The localization maps $M \to M_{\mathfrak{m}}$ combine to a map $\Phi\colon M \to \bigoplus_{\mathfrak{m}\in\operatorname{Supp} M} M_{\mathfrak{m}}$, which fits in the exact sequence

$$0 \longrightarrow \ker\Phi \longrightarrow M \longrightarrow \bigoplus_{\mathfrak{m}\in\operatorname{Supp} M} M_{\mathfrak{m}} \longrightarrow \operatorname{coker}\Phi \longrightarrow 0.$$

Given a prime ideal $\mathfrak{p}$ there are two outcomes when the sequence is localized at $\mathfrak{p}$. Either $\mathfrak{p}$ does not contain any of the $\mathfrak{m}_i$'s, and then all terms of the sequence become zero when localized, or $\mathfrak{p}$ is one of the maximal ideals in $\operatorname{Supp} M$; say $\mathfrak{p} = \mathfrak{m}$. If $\mathfrak{m}' \neq \mathfrak{m}$ is another member of $\operatorname{Supp} M$, there are elements in $\mathfrak{m}'$ not belonging to $\mathfrak{m}$, and hence $(M_{\mathfrak{m}'})_{\mathfrak{m}} = 0$. Therefore the only term in the sum that survives being localized at $\mathfrak{m}$ is $M_{\mathfrak{m}}$, and the sum localises to $M_{\mathfrak{m}}$. But of course M localises to $M_{\mathfrak{m}}$ as well, and the localization map localizes to the identity! It follows that $\ker\Phi$ and $\operatorname{coker}\Phi$ localizes to zero everywhere, and hence they are zero by the"The Localness of Being Zero" principle (Proposition 6.62 on page 144). ❑

7.5 *Artinian ring*

We now turn to the rings whose ideals satisfy the descending chain condition; that is, rings being Artinian modules over themselves. Even though the definitions may appear symmetric, the class of Artinian rings is astonishingly different from the class of Noetherian rings. The latter is a large class encompassing almost all rings one meets in algebraic geometry, whereas the Artinian ones merely serve special (but important) purposes. They are the tiny, little brothers among the Noetherian rings—but they carry a great lot of subtleties.

Yasuo Akizuki
(1902–1984)
Japanese mathematician

7.53 It turns out that, as we shorty shall see, that Artinian rings are Noetherian. This is specific for rings, but far from true for modules. The Artinian rings are characterized among the Noetherian ones by the property that all their prime ideals are maximal and that the maximal ideals are finite in number. In geometric terms, their spectra are finite sets and the Zariski topology is discrete.

The theorem we are about to prove is due to the Japanese mathematician Yasuo Akizuki. There is an analogue version valid for non-commutative rings, proved about at the same time as Akizuki proved his theorem, which usually is contributed to Charles Hopkins and Jacob Levitzki, but the the commutative version is Akizuki's:

THEOREM 7.54 (AKIZUKI'S THEOREM) *An Artinian ring is Noetherian and all its prime deals are maximal and they are finite in number.*

7.55 Recall that a module which is both Noetherian and Artinian is of finite length. Hence Artinian rings are of finite length (regarded as modules over themselves) and hence come with a natural numerical invariant, the length $l(A)$; that is, the number of (simple) subquotients in a composition series.

The proof of Akizuki's theorem ⟹

The proof of Akizuki's theorem will be done in series of two lemmas. We begin with proving the second statement in the theorem, the one about prime ideals being maximal and finite in number. This is the easy piece, that A is noetherian, is deeper.

LEMMA 7.56 *Every prime ideal in an Artinian ring A is maximal and they are finite in number. Hence if J is the radical of A, the quotient A/J is a finite product of fields.*

PROOF: We have already established the first assertion, if $\mathfrak{p}$ is a prime in A, the quotient $A/\mathfrak{p}$ is an Artinian domain, hence a field by Lemma 7.51 above.

As to the second statement, assume that $\{\mathfrak{m}_i\}_{i\in\mathbb{N}}$ is a countable set of different maximal ideals in A. For each natural number r consider the ideal $N_r = \bigcap_{i\leqslant r} \mathfrak{m}_i$. They form a descending chain, and A being Artinian it holds true that $N_n = N_{n+1}$ for some n. This means that $\bigcap_{i\leqslant r} \mathfrak{m}_i \subseteq \mathfrak{m}_{n+1}$, and by the Prime Avoidance Lemma (Lemma 2.28 on page 33), one of the $\mathfrak{m}_i$'s must lie within $\mathfrak{m}_{n+1}$, contradicting the assumption that the $\mathfrak{m}_i$'s are different.

The last assertion ensues from the Chinese remainder theorem. If $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are the prime ideals in A, the radical J equals $J = \bigcap_i \mathfrak{m}_i$, and since all the $\mathfrak{m}_i$'s are maximal, they are pair-wise comaximal. Hence the Chinese Remainder Theorem gives an isomorphism $A/J \simeq \prod_i A/\mathfrak{m}_i$. ❑

The preceding lemma implies that the radical J of A coincides with intersection of the maximal ideals in A. The elements are nilpotent, but A is not *a priori* Noetherian, so J is not *a priori* a nilpotent ideal. However, our next lemma says it is.

LEMMA 7.57 *The radical J of an Artinian ring A is nilpotent; that is, $J^n = 0$ for some n. Moreover, J is Noetherian.*

This lemma concludes the proof of Akizuki's theorem. Since A/J, being the product of finite number of fields is Noetherian, we infer that A is Noetherian.
PROOF: Consider the set of powers J^r that are not finitely generated. If J is not finitely generated, that set is non-empty and since A is Artinian it has a a minimal element, say J^m. In any case, there is an m so that J^v is finitely generated for $v \geqslant m$.

The descending chain of powers J^r becomes stationary at a certain stage as well, that is, there is an m such that $J^{\nu+1} = J^\nu$ whenever $\nu \geqslant m$.

Altogether, we infer there is an r so that J^r is finitely generated and satisfies $J^{r+1} = J^r$ and we are thence in the position to apply Nakayama's lemma to the J^r, and may conclude that $J^r = 0$. ❑

The final step of the proof of Akizuki's theorem is an induction argument to show that J is Noetherian. For ν sufficiently big, we saw in the previous lemma that $J^\nu = 0$, and for each ν there is a short sequence:

$$0 \longrightarrow J^{v+1} \longrightarrow J^\nu \longrightarrow J^\nu/J^{\nu+1} \longrightarrow 0.$$

Submodules and quotients of Artinian modules are Artinian (Proposition 7.8 on page 153), so it follows that J^ν, and therefore also $J^\nu/j^{\nu+1}$, is Artinian. But $J^\nu/J^{\nu+1}$ is a module over A/J which we just proved is a finite product of fields, and over such rings any Artinian module is Noetherian (Example 7.2 on page 154); and we are through by descending induction on ν.

The structure of Artinian rings

Since Artinian rings are of finite length over themselves, we may apply the Structure Theorems (Proposition 7.50 and Theorem 7.52 both on page 169) to obtain the following description

THEOREM 7.58 *Let A be an Artinian ring. Then* Spec A *is finite and discrete, and the localisation maps $A \to A_{\mathfrak{m}}$ induce an isomorphism*

$$A \simeq \prod_{\mathfrak{m} \in \operatorname{Spec} A} A_{\mathfrak{m}}.$$

If A is Noetherian and Spec A *is finite and discrete, then A is Artinian.*

Saying Spec A is finite and discrete is just another way of saying that all prime ideals in A are maximal and finite in number. Anticipating the notion of *Krull dimension*, a ring all whose prime ideals are maximal is said to be of Krull dimension zero. Hence a Noetherien ring A is Atinian if and only if its Krull dimension equals zero.

The theorem says nothing about local Artinian rings, even if they might appear small and innocuous, they can be extremely intricate creatures.

Problems

7.20 Let n and m be two natural numbers and let $\mathfrak{a}$ be the ideal $\mathfrak{a} = (x^m, y^n)$ in $k[x, y]$. Show that $A = k[x, y]/\mathfrak{a}$ is Artinian and compute its length.

7.21 Let n, m and r be three natural numbers and let $A = k[x, y, z]/(x^n, y^m, z^r)$. Prove that A is Artinian and compute its length.

Lecture 8

Primary decomposition

Preliminary version 1.0 as of 2018-11-15 at 11:29:54 (typeset 3rd December 2018 at 10:03am)—Much work remaining. Prone to misprints and errors and will change.
2018-11-15 Added exercise 6.20, corrected exercises 8.9 and **??**

The beginning of the story about primary decomposition is the Fundamental Theorem of Arithmetic which states that any integer has a representation as a product of prime numbers unambiguous up to order. The early 19$^{\text{th}}$ century mathematicians discovered however that algebraic integers do not share this property unconditionally, there are rings of algebraic numbers for which the analogue of the Fundamental Theorem does not hold; where irreducible factors are not always unique.

However, for a large class rings appearing in algebraic number theory—the so-called Dedekind domains—the situation could be saved by using prime ideals instead of prime numbers; any non-zero and proper ideal in a Dedekind domain is a product of powers of prime ideals in an unambiguous ways.

Dedekind domains are special, and the question arose quickly what is generally true. Emanuel Lasker[1] was one of the first to give a partial answer, he established the primary decomposition for ideals in rings finitely generated over fields. The final breakthrough came in Emmy Noether's famous 1921-paper. Her results were profoundly more general and her proofs enormously easier and more translucent than the previous.

In a general decomposition products are replaced by intersections and powers of prime ideals by so-called primary ideals. Every ideal $\mathfrak{a}$ in a Noetherian ring has a such a primary decomposition. One may write $\mathfrak{a}$ as an intersection $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ of primary ideals, but the uniqueness of the intervening ideals are only partially true.

There is also a geometric interpretation of this decomposition. The closed subset $X = V(\mathfrak{a})$ of the spectrum Spec A—or the variety $X = V(\mathfrak{a})$ in $\mathbb{A}^n$ if one prefer working with ideals in a polynomial ring—can be decomposed in a union of closed, irreducible[2] subsets called the *irreducible components* of X. For instance, the subset given by $xyz = 0$ in $\mathbb{C}^3$ has the thee coordinate planes as components.

The road map of this chapter is as follows: We begin with introducing the

[1] In addition to be an eminent mathematician, Lasker was World Chess Champion for 27 years

Emanuel Lasker (1868–1941) German mathematician

[2] A topological space is *irreducible* if it is not the union of two proper, closed subsets.

new important players, the primary ideals, and establish their basic properties. Next follows the announcement of the main theorem and a discussion around it, and finally the main theorem is proven through a series of lemmas.

8.1 *Primary ideals*

As alluded to in the introduction to this chapter, one needs a notion of *primary ideals* which generalizes the notion of "prime powers" we have for integers. The naive try would be to just use powers of prime ideals, but this is in fact too naive and doesn't work—the issue is certainly of a more subtle character.

8.1 The property of an ideal $\mathfrak{q}$ being being primary is best introduced as a property of the quotient $A/\mathfrak{q}$. To motivate the definition, consider the multiplication-by-n-map $\mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}/p^r\mathbb{Z}$. It is either bijective or nilpotent[3], and the salient point is that this characterises prime powers. If an integer m has different primes p and q as factors, multiplication by p (or by q) in $\mathbb{Z}/m\mathbb{Z}$ is neither bijective nor nilpotent.

[3] When n is prime to p it is bijective, and when n has p as factor, it will be nilpotent.

Inspired by this exquisite property of prime powers, we call a proper ideal $\mathfrak{q}$ a *primary ideal* if the following condition is satisfied:

As for prime ideals, we insist on primary ideals being proper.

Primary ideals (*primæridealer*)

- For every element $x \in A$ the multiplication map $A/\mathfrak{q} \to A/\mathfrak{q}$ that sends an element y to $x \cdot y$ is either injective or nilpotent.

The "multiplication-by-x-map" is frequently called by a more scientific name, namely the *homothety* by x Since the radical $\sqrt{\mathfrak{q}}$ consists of ring elements with a power lying in $\mathfrak{q}$, the condition may be reformulated as

Homotheties (*homotetier*)

- If $xy \in \mathfrak{q}$, then either $y \in \mathfrak{q}$ or $x \in \sqrt{\mathfrak{q}}$.

Basic properties of primary ideals

In this section a series of four small propositions we shall establish four basic properties of primary ideal. We shall see that their radicals are prime ideals (as would be expected from offshoots of prime powers), that they behave well with respect to intersections, localizations and quotient formation.

8.2 The first property of primary ideals we discuss is that their radicals are prime ideals. Once this is established, it follows that $\sqrt{\mathfrak{q}}$ is minimal among the prime prime ideals containing $\mathfrak{q}$. Indeed, as for any ideal, the radical of $\mathfrak{q}$ equals the intersection of the prime ideals containing $\mathfrak{q}$ (see Proposition 2.59 on page 42). In other words, the ring $A/\mathfrak{q}$ has just one minimal prime ideal, which is formed by the nilpotent elements.

PROPOSITION 8.3 *If $\mathfrak{q}$ is a primary ideal in the ring A, the radical $\sqrt{\mathfrak{q}}$ is a prime ideal, and it is the smallest prime ideal containing $\mathfrak{q}$.*

PROOF: Assume that $xy \in \sqrt{\mathfrak{q}}$, but $y \notin \sqrt{\mathfrak{q}}$; then $x^n y^n$ lies in $\mathfrak{q}$ for some n, but $y^n \notin \mathfrak{q}$, so some power of x^n lies there. Hence $x \in \sqrt{\mathfrak{q}}$. ❑

It is customary to say that a primary ideal $\mathfrak{q}$ is $\mathfrak{p}$-*primary* when $\mathfrak{p} = \sqrt{\mathfrak{q}}$, or one also says that $\mathfrak{p}$ *belongs to* $\mathfrak{q}$. The converse of Proposition 8.3 does not hold in general; the radical being prime is not sufficient for an ideal to be primary. Example 8.1 below is an easy and concrete instance of this, and more elaborate example in a polynomial ring is found in Exercise 8.4 below. However, if the radical of $\mathfrak{q}$ is maximal, $\mathfrak{q}$ is primary:

$\mathfrak{p}$-*primary ideals* ($\mathfrak{p}$-*primære idealer*)

PROPOSITION 8.4 *An ideal $\mathfrak{q}$ whose radical is maximal, is primary.*

PROOF: Assume that the radical $\sqrt{\mathfrak{q}}$ is maximal and write $\mathfrak{m} = \sqrt{\mathfrak{q}}$. Because $\mathfrak{m}$ is both maximal and the smallest prime containing $\mathfrak{q}$, the ring $A/\mathfrak{q}$ is a local ring with maximal ideal $\mathfrak{m}/\mathfrak{q}$ as the only prime ideal. Therefore the elements of $\mathfrak{m}/\mathfrak{q}$ are nilpotent while those not in $\mathfrak{m}/\mathfrak{q}$ are invertible. ❑

COROLLARY 8.5 *The powers $\mathfrak{m}^n$ of a maximal ideal $\mathfrak{m}$ are $\mathfrak{m}$-primary.*

PROOF: The radical of $\mathfrak{m}^n$ equals $\mathfrak{m}$. ❑

Examples

8.1 The ideal $\mathfrak{a} = (x^2, xy)$ in the polynomial ring $k[x, y]$ has a radical that is prime, but $\mathfrak{a}$ is not primary. Clearly the radical of (x^2, xy) equals (x) which is prime, but in the quotient $k[x, y]/(x^2, xy)$ multiplication by y is neither injective nor nilpotent (y kills the class of x, but no power of y lies in (x^2, xy)). One decomposition of (x^2, xy) as an intersection of primary ideals is

$$(x^2, xy) = (x) \cap (x^2, y).$$

Checking the equality is a nice little exercise: A relation $z = ax = bx^2 + cy$ entails that $x|c$ (the polynomial ring is UFD), and hence $z \in (x^2, xy)$. Notice that both ideals in the intersections are primary; (x) since it is prime and (x^2, y) because the radical equals (x, y) which is maximal. One also has the decomposition

$$(x^2, xy) = (x) \cap (x, y)^2,$$

indeed, the polynomials in (x^2, xy) are those with x as factor that vanish at least to the second order at the origin. This gives an example of the primary decomposition not being unique.

8.2 A standard example of a prime ideal whose square is not primary is as follows. Let $A = k[X, Y, Z]/(X^2 - YZ)$ and, by the usual convention, x, y and z are the classes of the variables in A. The ideal $\mathfrak{p} = (x, y)$ is prime, but $\mathfrak{p}^2$ is not primary; indeed, yz lies there, but neither does y lie in $\mathfrak{p}^2$ nor does z lie in $\mathfrak{p}$. A decomposition into primary ideals of $\mathfrak{p}^2$ is shaped like

$$(x, y)^2 = (x^2, xy, y^2) = (yz, yx, y^2) = (x, y, z) \cap (y).$$

Obviously the ideal (x, y, z) being maximal is primary. The ideal (y) is more interesting. Killing y, we obtain the ring $A/(y) = k[X, Z]/(X^2)$, whose elements are either non-zero divisors or nilpotent[4] and (y) is a primary ideal. It's radical equals (x, y).

[4] The elements are of the form $a(z) + b(z)x$ with $a, b \in k[z]$, and one easily sees that this is a non-zero divisor unless $a = 0$, but then the square is zero.

☆

8.6 The intersection of finitely many $\mathfrak{p}$-primary ideals persist being $\mathfrak{p}$-primary. In the analogy with the integers, this reflects the simple fact that the greatest common divisor of some powers of the same prime number is a power of that prime.

PROPOSITION 8.7 *If $\{q_i\}$ is a finite collection of $\mathfrak{p}$-primary ideals, then the intersection $\bigcap_i \mathfrak{q}_i$ is $\mathfrak{p}$-primary.*

PROOF: Taking radicals commutes with taking finite intersection (Lemma 2.63 on page 43), and therefore one has $\sqrt{\bigcap_i \mathfrak{q}_i} = \bigcap_i \sqrt{\mathfrak{q}_i} = \mathfrak{p}$. Assume next that $xy \in \bigcap_i \mathfrak{q}_i$, but $y \notin \bigcap_i \mathfrak{q}_i$; that is, $xy \in \mathfrak{q}_i$ for each i, but $y \notin \mathfrak{q}_\nu$ for some ν. Since $\mathfrak{q}_\nu$ is $\mathfrak{p}$-primary x lies in the radical $\sqrt{\mathfrak{q}_\nu}$ of $\mathfrak{q}_\nu$, which equals $\mathfrak{p}$, but as we just checked, $\mathfrak{p}$ is as well the radical of the intersection $\bigcap_i \mathfrak{q}_i$. ❑

The hypothesis that the intersection be finite cannot be discarded. Powers $\mathfrak{m}^i$ of a maximal ideal are all primary and have the same radical, namley $\mathfrak{m}$, but but at least when A is Noetherian, their intersection equals the zero ideal (0) by Krull's intersection theorem— which might be primary, but certainly not $\mathfrak{m}$-primary (in most cases). There are however instances when infinite intersection of primary ideals are primary.

Problems

8.1 With notation as in Example 8.2 on the previous page, show that $\mathfrak{p}^n$ is not primary for any $n \geqslant 2$. HINT: Show that $zy^{n-1} \in \mathfrak{p}^n$ but $y^{n-1} \notin \mathfrak{p}^n$. ✲

8.2 Let $\{\mathfrak{q}_i\}_{i \in I}$ be a collection of primary ideals (of any cardinality) all with the same radical $\mathfrak{p}$. Assume that there is a natural number n so that $\mathfrak{p}^n \subseteq \mathfrak{q}_i$ for all i. Prove that the intersection $\bigcap_{i \in I} \mathfrak{q}_i$ is primary with $\mathfrak{p}$ as radical. ✲

8.3 Let the group G act[5] on the Noetherian ring A and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Assume that $\mathfrak{p}$ is invariant under G. Prove that $\bigcap_{g \in G} \mathfrak{q}^g$ is $\mathfrak{p}$-primary and invariant under G. ✲

[5] The action induces an action on the ideals by setting $\mathfrak{a}^g = \{ ga \mid g \in G, a \in \mathfrak{a} \}$

★

8.8 The property of being primary is compatible with localizations, at least when these are performed with respect to multiplicative sets disjoint from the radical.

PROPOSITION 8.9 *Let S a multiplicative set in the ring A and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Assume that $S \cap \mathfrak{p} = \varnothing$. Then $\mathfrak{q}A_S$ is $\mathfrak{p}A_S$-primary and it holds true that $\iota_S^{-1}(\mathfrak{q}A_S) = \mathfrak{q}$.*

PROOF: Localizing commutes with forming radicals (Proposition 6.23 on page 130) so the radical of $\mathfrak{q}A_S$ equals $\mathfrak{p}A_S$. Assume that $x/s \cdot y/s' \in \mathfrak{q}A_S$, but that $y/s' \notin \mathfrak{q}A_S$. Then $txy \in \mathfrak{q}$ for some $t \in S$, and obviously it holds that $y \notin \mathfrak{q}$. Hence tx lies in the radical $\mathfrak{p}$ of $\mathfrak{q}$, and since $t \notin \mathfrak{p}$, we conclude that $x \in \mathfrak{p}$; in other words x/s lies in $\mathfrak{p}A_S$.

To verify that $\iota_S^{-1}(\mathfrak{q}A_S) = \mathfrak{q}$ let $x \in A$ be such that $\iota_S(x) \in \mathfrak{q}A_S$. This means that $sx \in \mathfrak{q}$ for some $s \in S$, but by hypothesis $\mathfrak{p} \cap S = \varnothing$ so that $s \notin \mathfrak{p}$; thence $x \in \mathfrak{q}$ because $\mathfrak{q}$ is primary. ❑

8.10 The fourth property permits us to replace A by $A/\mathfrak{q}$ and $\mathfrak{q}$ by the zero ideal, which makes some arguments cleaner and notationally simpler.

PROPOSITION 8.11 *Let $\phi\colon A \to B$ be a surjective map of rings with kernel $\mathfrak{a}$. Assume that $\mathfrak{q}$ is an ideal in A containing the kernel $\mathfrak{a}$. Then the image $\mathfrak{q}B = \mathfrak{q}/\mathfrak{a}$ of $\mathfrak{q}$ in B is primary if and only if $\mathfrak{q}$ is. The radical of the image equals the image of the radical; or in symbols, $\sqrt{(\mathfrak{q}/\mathfrak{a})} = (\sqrt{\mathfrak{q}})/\mathfrak{a}$.*

PROOF: This is pretty obvious because by the ISOMORPHISM THEOREM (Theorem 2.18 on page 30) it holds that $A/\mathfrak{q} = B/\mathfrak{q}B$, so the multiplication-by-whatever-maps are the same. ❑

In particular, we observe that the ideal $\mathfrak{q}$ is primary if and only if the zero ideal (0) is a primary ideal in the quotient $A/\mathfrak{q}$.

PROBLEM 8.4 This problem is meant to illustrate that even in a polynomial ring powers of prime ideals are not always primary. The polynomial ring $R = k[x, y, z]$ is given a grading by assigning the following degrees to the variables: $\deg x = 3$, $\deg y = 4$ and $\deg z = 5$.

Consider the map $\phi\colon k[x, y, z] \to k[t]$ defined by $x \mapsto t^3$, $y \mapsto t^4$ and $z \mapsto t^5$. It preserves the degrees (when $k[t]$ is given the usual grading with the degree of t being one) hence the kernel $\mathfrak{p}$ is a homogeneous prime ideal. The image of ϕ is the ring $k[t^3, t^4, t^5]$.

a) Show that the polynomials $f = xz - y^2$, $g = x^3 - yz$ and $h = yx^2 - z^2$ all lie in $\mathfrak{p}$.

b) Verify that the homogeneous polynomials of degree less than 8 in R are x, x^2 and xy, and prove that no element of $\mathfrak{p}$ is of degree less than 8.

c) Show that $g^2 - fh$ is divisible by x and that $u = (g^2 - fh)x^{-1}$ is homogeneous of degree 15.

d) Conclude that $\mathfrak{p}^2$ is not a primary ideal. HINT: $xu \in \mathfrak{p}^2$ but neither u nor any power of x lies in $\mathfrak{p}^2$. ★

8.2 The Lasker-Noether theorem

Minimal primary decompositions

8.12 Given a collection $\{S_i\}$ of set. It might very well happen that the intersection $\bigcap_i S_i$ does not change if one throws away one or more of the S_i's (for instance, if $S_1 \subseteq S_2$, one stupidly has $S_1 \cap S_2 = S_1$) and in that case one says that intersection is *redundant*. In the opposite case, that all the S_i contribute to the intersection, or in other words, when $\bigcap_i S_i \subsetneq \bigcap_{i\neq j} S_i$ for all j, the intersection is called *irredundant*.

Redundant intersections (*redundant snitt*)

Irredundant intersections (*irreduntante snitt*)

The superfluous sets of an intersection are precisely those S_j such that $\bigcap_{i\neq j} S_i \subseteq S_j$, and one may render the intersection irredundant by just discarding those sets.

8.13 Now, let $\mathfrak{a}$ be an ideal in the ring A, a *primary decomposition* is an expression of $\mathfrak{a}$ as a finite intersection of primary ideals; that is an equality like

Primary decomposition (*primær dekomposisjon*)

$$\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \mathfrak{q}_r \tag{8.1}$$

where $\mathfrak{q}_i$'s are primary ideals. We have already seen several examples (examples 8.1 and 8.2 above).

Without further constraints there are several trivial[6] ways such a decomposition can be ambiguous. First of all, it can be an irredundant intersection. Secondly a $\mathfrak{p}$-primary ideal can be the intersections of other $\mathfrak{p}$-primary ideals in infinitely many different ways (see the upcoming example 8.3). The first type of ambiguity is coped with by just discarding superfluous ideals, and Proposition 8.7 above helps us coping with the second. We just group those $\mathfrak{q}_i$'s with the same radical together, and replace them by their intersection, which will be primary with the same radical.

[6] And it can be in non-trivial ways too; we shortly return to those.

The primary decomposition (8.1) is called *minimal* or *reduced* if all the radicals $\sqrt{\mathfrak{q}_i}$ are different and the intersection is irredundant.

Minimal or reduced primary decompositions (*minimale eller reduserte primærdekomposisjoner*)

LEMMA 8.14 *Any primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ can be rendered a minimal one; that is, an irredundant intersection with the radicals $\sqrt{\mathfrak{q}_i}$ being distinct.*

EXAMPLE 8.3 Consider $\mathfrak{m}^2 = (x^2, xy, y^2)$ in $k[x, y]$ (where $\mathfrak{m} = (x, y)$). For all scalars α and β with $\alpha \neq 0$ one has the equality

$$(x^2, xy, y^2) = (x^2, y) \cap (y^2, \alpha x + \beta y).$$

Indeed, this amounts to the two lines generated by the class of y and the class of $\alpha x + \beta y$ in the two dimensional vector space $\mathfrak{m}/\mathfrak{m}^2$ intersecting in 0. ☆

EXAMPLE 8.4 If the ring A is a PID, there is nothing much new. The prime ideals are the principal ideals (p) generated by an irreducible p. The (p)-primary ideals are those generated by powers of p; that is, those on the form (p^v). In

general, if $f = p_1^{\nu_1} \dots p_r^{\nu}$ is a factorisation of f into a product of irreducible elements, the primary decomposition of (f) is unambiguous and it is given as

$$(f) = (p_1)^{\nu_1} \cap \dots \cap (p_r)^{\nu_r}.$$

The same applies to *principal* ideals in any UFD; but be warned that not all ideals are principal! ☆

Finally in this paragraph, we notice that by Proposition 8.9 a primary decomposition localises well:

PROPOSITION 8.15 *Assume that S is a multiplicatively closed subset of A and that $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r$ is a primary decomposition of $\mathfrak{a}$ with radicals $\mathfrak{p}_i$. Then $\mathfrak{a}A_S = \mathfrak{q}_1 A_S \cap \dots \cap \mathfrak{q}_r A_s$, and either $\mathfrak{q}_i A_S$ is primary with radical $\mathfrak{p}_i A_S$ or $\mathfrak{q}_i A_S = AS$*

The resulting decomposition of $\mathfrak{a}A_S$ is by no means always irredundant even if the one of $\mathfrak{a}$ one starts with is. The primes $\mathfrak{p}_i$ meeting S blow up to the entire ring A_S. They will not contribute to the intersection and can be discarded, and thus one may write

$$\mathfrak{a}A_S = \bigcap_{S \cap \mathfrak{p}_i = \varnothing} \mathfrak{q}_i A_S.$$

A particularily interesting case is to take S to be the complement of one of the $\mathfrak{p}_i$'s, say $\mathfrak{p}_\nu$. Then $\mathfrak{a}A_S = \mathfrak{q}_v A_S$, and $\mathfrak{a}A_S$ is primary in A_S!

Existence of Primary Decompositions

In rings that are not Noetherian, ideals may or may not have a finite primary decomposition; but in Noetherian rings they always have. The proof is application of Noetherian induction (the principle of attacking a maximal crook!)

PROPOSITION 8.16 *In a Noetherian ring A any ideal $\mathfrak{a}$ is the intersection of finitely many primary ideals.*

PROOF: Since the ring A is assumed to be Noetherian, the set of ideals for which the conclusion fails, if non-empty, has a maximal element $\mathfrak{a}$. Replacing A by $A/\mathfrak{a}$ we may assume that the zero ideal is not the intersection of finitely many primary ideals (in particular it is not primary), but that all non-zero ideals in A are.

In A there will be two elements x and y such that $xy = 0$, but with $x \neq 0$ and y not nilpotent. The different annihilators $\operatorname{Ann} y^i$ form an ascending chain of ideals, hence $\operatorname{Ann} y^\nu = \operatorname{Ann} y^{\nu+1}$ for some ν. We contend that $(0) = \operatorname{Ann} y \cap (y^\nu)$. Indeed, if $a = by^\nu$ is an element in (y^ν) that lies in $\operatorname{Ann} y$, one has $ay = by^{\nu+1} = 0$ and therefore $b \in \operatorname{Ann} y^{\nu+1} = \operatorname{Ann} y^\nu$, and it follows that $a = by^\nu = 0$. Now, $x \in \operatorname{Ann} y$ is a non-zero element, and since y is not nilpotent, both ideals (y^ν) and $\operatorname{Ann} y$ are non-zero and are therefore finite intersections of primary ideals; the same is thus true for (0). ❑

THEOREM 8.17 (THE LASKER-NOETHER THEOREM) *Every ideal in a Noetherian ring has a minimal primary decomposition.*

PROOF: Start with any decomposition of an ideal $\mathfrak{a}$ into primary ideals (there is at least one according to the proposition above). By Lemma 8.14 on page 178 it can be made minimal by regrouping ideals with the same radical and discarding redundant ones. ❑

The First Uniqueness Theorem

There are two main uniqueness issues concerning primary decompositions. One may ask if the radicals of the components are unique, or ask if the primary components themselves are unique. The first question is answered by an unconditionally yes (well, the ring must be Noetherian), but to the second the answer is no in general (also in Noetherian rings), although being a partial yes.

8.18 A way to show that the radicals of the primary components of an ideal $\mathfrak{a}$ are invariants of the ideal, is to characterize them without referring to any of the decompositions. The idea is to consider the collection of *transporter ideals* $(\mathfrak{a} : x)$ when x varies in A, and it turns out that the radicals of the primary components of $\mathfrak{a}$ are precisely the prime ideals among these.

PROPOSITION 8.19 *Let $\mathfrak{a}$ be an ideal in a Noetherian ring A. The radicals that occur in an irredundant primary decomposition of $\mathfrak{a}$, are precisely the prime ideals among the transporter ideals $(\mathfrak{a} : x)$ with x in A.*

Passing to the quotient $A/\mathfrak{a}$ and observing that $(\mathfrak{a} : x)/\mathfrak{a}$ equals the annihilator $(0 : [x])$ of the class $[x]$ in $A/\mathfrak{a}$, the theorem has the equivalent formulation (remember Proposition 8.11 on page 177) which is the one we shall prove:

PROPOSITION 8.20 (PRINCIPLE OF ANNIHILATORS) *The radicals occurring in an irredundant primary decomposition of the zero ideal (0) in a Noetherian ring A, are those ideals among the annihilators $\operatorname{Ann} x$ that are prime.*

PROOF: Fix an irredundant primary decomposition of the zero ideal (0). There are two implications to prove. We begin with letting $\mathfrak{q}$ be one of the components and letting $\mathfrak{p} = \sqrt{\mathfrak{q}}$ denote the radical, and we aim at exhibiting an x such that $\mathfrak{p} = \operatorname{Ann} x$. Denote by $\mathfrak{c}$ the intersection of the other primary components in the decomposition. Then $\mathfrak{c} \cap \mathfrak{q} = 0$, but $\mathfrak{c} \neq 0$ since the decomposition is irredundant.

Let $x \in \mathfrak{c}$ be a non-zero element such $\operatorname{Ann} x$ is maximal among the annihilators of non-zero elements of $\mathfrak{c}$. We contend that $\operatorname{Ann} x = \mathfrak{p}$, and begin with showing the inclusion $\operatorname{Ann} x \subseteq \mathfrak{p}$. Because $x \neq 0$, it holds that $x \notin \mathfrak{q}$, and hence $xy = 0$ implies that $y \in \mathfrak{p}$ as $\mathfrak{q}$ is $\mathfrak{p}$-primary.

In order to show the other inclusion pick an $y \in \mathfrak{p}$ and assume that $xy \neq 0$. Some power of y lies in $\mathfrak{q}$ and therefore kills x. Hence there is a natural number n so that $y^n x = 0$, but $y^{n-1}x \neq 0$. By the maximality of $\operatorname{Ann} x$ it holds true that $\operatorname{Ann} x = \operatorname{Ann} y^{n-1}x$, and consequently $y \in \operatorname{Ann} x$, which contradicts the assumption that $xy \neq 0$.

For the reverse implication, assume that $\operatorname{Ann} x$ is a prime ideal. Let I be the set of indices such that $\mathfrak{q}_i$ does not contain x. Then $\bigcap_{i\in I} \mathfrak{q}_i \subseteq \operatorname{Ann} x$, because

$$x \cdot \bigcap_{i\in I} \mathfrak{q}_i \subseteq \bigcap_{i\notin I} \mathfrak{q}_i \cdot \bigcap_{i\in I} \mathfrak{q}_i \subseteq \bigcap_{i\notin I} \mathfrak{q}_i \cap \bigcap_{i\in I} \mathfrak{q}_i = (0).$$

Consequently it holds true that the product of appropriate powers of the corresponding radicals $\mathfrak{p}_i$ is contained in $\operatorname{Ann} x$. Since $\operatorname{Ann} x$ is supposed to be prime, it follows that $\mathfrak{p}_\nu \subseteq \operatorname{Ann} x$ for one $\nu \in I$. On the other hand, it holds true that $(0) = x \cdot \operatorname{Ann} x \subseteq \mathfrak{q}_\nu$ from which ensues that $\operatorname{Ann} x \subseteq \mathfrak{p}_\nu$ because $\mathfrak{q}_\nu$ is $\mathfrak{p}_\nu$-primary and $x \notin \mathfrak{p}_\nu$. ❑

THEOREM 8.21 (THE FIRST UNIQUENESS THEOREM) *The radicals occurring in an irredundant primary decomposition of an ideal in a Noetherian ring are unambiguously determined by the ideal.*

8.22 The radicals of the primary components are of course tightly related to the ideal, vaguely analogous to the prime factors of an integer, and they merit a proper name. They are called the *associated prime ideals* of $\mathfrak{a}$, and the set they constitute is denoted by $\operatorname{Ass} A/\mathfrak{a}$. In particular, $\operatorname{Ass} A$ will be the set of prime ideals associated to zero.

Associated prime ideals (*assosierte primidealer*)

8.23 There are no inclusion relations between the components of an irredundant primary decomposition (irredundant means precisely this), but that does not exclude inclusion relations between the associated primes. In Example 8.1, for instance, we found that $(x^2, xy) = (x) \cap (x, y)^2$ with the associated primes being (x) and (x, y). One distinguish between *isolated* and *embedded* associated primes. The former are those being minimal in $\operatorname{Ass} A$; that is, they do not contain any other associated prime, whereas the latter are those that do. In the example above, (x) is an isolated prime whilst (x, y) is embedded[7].

Isolated associated primes (*isolerte assosierte primidealer*)

Embedded associated primes (*embeddede assosierte primidealer*)

Primary components with an isolated radical are called *isolated components* and those with an embedded radical are called *embedded components*.

8.24 Early in the course, when discussing the radical of an ideal, we proved that the radical $\sqrt{0}$ of A equals the intersection of all minimal primes in A (Paragraph 2.61 on page 2.61); that is, $\sqrt{0} = \bigcap \mathfrak{p}$, the intersection extending over the minimal elements of $\operatorname{Spec} A$.

On the other hand, we just expressed the radical $\sqrt{0}$ as the intersection of the prime ideals minimal in $\operatorname{Ass} A$ so that $\sqrt{0} = \bigcap \mathfrak{p}$ where the intersection extends over the minimal elements in $\operatorname{Ass} A$. When the intersections of two families of prime ideals are equal and there are no (non-trivial) inclusion

[7] You might wonder why t *embedded* components since they are not contained in, but on the contrary contain other associated primes. The usage stems from geometry since inclusions between varieties are the reversed of those between ideals.

Isolated components (*isolerte komponenter*)

Embedded components (*embeddede komponenter*)

relations between members of either family, the families coincide (Lemma 2.31 on page 34). Hence the sets Spec A and Ass A have the same minimal primes. We have proved:

PROPOSITION 8.25 *In a Noetherian ring A the sets* Spec A *and* Ass A *have the same minimal elements; in other words, the minimal primes of A are precisely the isolated associated primes. In particular, there are finitely many minimal primes.*

8.26 We have seen the intersection of the associated primes of A is the set of nilpotent elements, and their union turns out to be the set of zero divisors:

PROPOSITION 8.27 *The set of zero-divisors in a Noetherian ring A equals the union $\bigcup_{\mathfrak{p}\in \operatorname{Ass} A} \mathfrak{p}$ of the associated primes.*

PROOF: Let $\operatorname{Ann} z$ be maximal among the annihilators of non-zero elements in A. Then $\operatorname{Ann} z$ is prime and hence an associated prime of A. Indeed, if $xyz = 0$ and $xz \neq 0$, it it ensues from the maximality of $\operatorname{Ann} z$ that $\operatorname{Ann} z = \operatorname{Ann} xz$ because obviously $\operatorname{Ann} z \subseteq \operatorname{Ann} xz$. Hence $y \in \operatorname{Ann} z$, and as any annihilator ideal is contained in a maximal one, we are through. ❑

EXAMPLE 8.5 We offer one more example and consider the ideal

$$\mathfrak{a} = (x^2y, y^2z, z^2x).$$

in the polynomial ring $\mathbb{C}[x, y, z]$ and aim at determining a primary decomposition.

To get an idea of where to start we resort to geometry, and take a look at the zero-locus $V(\mathfrak{a})$ inside $\mathbb{C}^3$. It is given by $x^2y = y^2z = z^2x = 0$, and is easily seen to be the union of the three coordinate-axes. This means that there must be some components supported along each axis, and no component can be supported elsewhere. So let us consider the x-axis. Localizing at x, *i.e.* passing to $A_x = \mathbb{C}[x, x^{-1}, y, z]$ and eliminating the two other axes, we see that $\mathfrak{a}A_x = (y, y^2z, z^2)$; so we suspect this to be one of the components; by symmetry we find two more suspects, and in fact, it holds true that

$$(x^2y, y^2z, z^2x) \subseteq (y, y^2z, z^2) \cap (x, x^2y, y^2) \cap (z, z^2x, x^2).$$

This is however not the whole story. The element xyz lies in the intersection to the right, but not in $\mathfrak{a}$. Now, clearly $(x, y, z) \subseteq (\mathfrak{a} : xyz)$ and (x, y, z) being maximal, it holds that $(\mathfrak{a} : xyz) = (x, y, z)$, so there must be an (x, y, z)-primary component. After a few tries (and a more failures) one finds the equality

$$(x^2y, y^2z, z^2x) = (y, y^2z, z^2) \cap (x, x^2y, y^2) \cap (z, z^2x, x^2) \cap (x^2, y^2, z^2).$$

The associated primes are (z, y), (x, y), (z, x) and (x, y, z). Once one has guessed correctly, it is relatively easy to check the answer. All involved ideals are generated by monomials, and such ideals have the nice property that they

have a polynomial as member if and only if all the monomial terms of the polynomial are members. Hence it suffices to check that every monomial lying in the ideal to the right lies in the one to the left as well. But monomials in (x^2, y^2, z^2) have either x^2, y^2 or z^2 as a factor, and by symmetry we may assume it is y^2. Lying in (z, z^2x, x^2) too, our monomial must have either z or x^2 as a factor and thereby also zy^2 or x^2y^2; but these two both lie in $\mathfrak{a}$, and we are done. ☆

The second uniqueness theorem

We have now to come the uniqueness issue for the primary component. Already our first example (Exampe 8.1 on page 175) showed that they are not unique. We found that

$$(x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x, y)^2.$$

and both (x^2, y) and $(x, y)^2$ are primary components. Notice that they have the same radical (they must!) and that they are embedded components. Now, the bad news are that (x^2, xy), have infinitely many different primary decomposition (Example 8.6 below), but the good news are that merely the embedded components differ. This is generally true. The Second Uniqueness Theorem we are about to prove, states that isolated components are unique. The point is that the isolated components may be expressed in terms of the corresponding associated primes which are independent of the decomposition. We shall see that if $\mathfrak{q}$ is the component and $\sqrt{\mathfrak{q}} = \mathfrak{p}$ it holds that $\mathfrak{q} = \iota^{-1}(\mathfrak{a}A_\mathfrak{p})$ where $\iota\colon A \to A_\mathfrak{p} \to$ is the localization map, or simply that $\mathfrak{q} = A \cap \mathfrak{a}A_\mathfrak{p}$ when ι is injective and suppressed from the notation.

THEOREM 8.28 (THE SECOND UNIQUENESS THEOREM) *The isolated components of an ideal $\mathfrak{a}$ in a Noetherian ring A are unambiguously defined by $\mathfrak{a}$.*

PROOF: We shall concentrate on one of the isolated associated prime ideals $\mathfrak{p}$ of $\mathfrak{a}$, but the main player will be a component $\mathfrak{q}$ that belongs to one of the minimal primary decompositions of $\mathfrak{a}$ and has radical $\mathfrak{p}$.

The salient point is the equality

$$\mathfrak{q} = \iota^{-1}(\mathfrak{a}A_\mathfrak{p}), \tag{8.2}$$

from which the theorem ensues since the isolated components are invariants of $\mathfrak{a}$.

To establish (8.2) express the decomposition of $\mathfrak{a}$ as $\mathfrak{a} = \mathfrak{q} \cap \bigcap_i \mathfrak{q}_i$ where the intersection extends over the primary components different from $\mathfrak{q}$. Localizing at $\mathfrak{p}$ one finds

$$\mathfrak{a}A_\mathfrak{p} = \mathfrak{q}A_\mathfrak{p} \cap \bigcap_i \mathfrak{q}_i A_\mathfrak{p} = \mathfrak{q}A_\mathfrak{q} \tag{8.3}$$

since the $\mathfrak{q}_i$'s blow up when localized; that is, $\mathfrak{q}_i A_\mathfrak{p} = A_\mathfrak{p}$. Indeed, since $\mathfrak{p}$ is

isolated, $\mathfrak{p}_i \nsubseteq \mathfrak{p}$ holds for all i. In each $\mathfrak{p}_i$ we may therefore find elements s not belonging to $\mathfrak{p}$, and as a power of s lies in $\mathfrak{q}_i$, we infer $\mathfrak{q}_i$ blows up. Taking inverse images on both sides of (8.3) and citing Proposition 8.9 on page 177 we conclude that $\iota^{-1}(\mathfrak{a}A_\mathfrak{p}) = \mathfrak{q}$.

EXAMPLE 8.6 The equality

$$(x^2, xy) = (x) \cap (x^2, xy, y^n)$$

holds true in the polynomial ring $k[x, y]$ for any natural number n, and is an example of infinitely many different minimal primary decompositions. Indeed, the $\subseteq$-inclusion is obvious, and to check the other, assume that a belongs to the right side. Then

$$a = p \cdot x = q \cdot x^2 + r \cdot y^n + sxy$$

with p, q r and s polynomials in $k[x, y]$. It follows that x divides r, and hence that $f \in (x^2, xy)$. ☆

EXAMPLE 8.7 So far all our examples have merely involved monomial ideals, but of course most idelas are not shaped like that. Primary decompositions are notoriously strenuous to lay hands on, and the monomial ideals are among the easiest to handle, hence their tendency to appear in texts. However, we are obliged to give at least one example of a more mainstream situation. It illustrates as well that the decomposition is largely of a geometric nature; that is, at least the isolated associated prime ideals are; the primary components may conceal subtler structures.

We shall analyse the familiar case of the intersection of two quadratic curves; the unit circle centred at $(0, 1)$ and a standard parabola. So let $\mathfrak{a} = (x^2 + (y-1)^2 - 1, y - x^2)$ in $k[x, y]$, where k is any field of characteristic different from 2. A standard manipulation shows that the common zeros of the two polynomials are the points $(1, 1)$, $(-1, 1)$ and $(0, 0)$, and the same manipulations give

$$\mathfrak{a} = (x^2 + (y-1)^2 - 1, y - x^2) = (x^2(x^2 - 1), y - x^2).$$

Any prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ must contain either x, $x - 1$ or $x + 1$. It contains y if x lies in it, and because $y - x^2 = y - (x + 1)(x - 1) - 1$, one has $y - 1 \in \mathfrak{p}$ in the two other cases. We conclude that the (x, y), $(x - 1, y - 1)$ and $(x + 1, y - 1)$ are the only prime ideals containing $\mathfrak{a}$; and since they all three are maximal, the associated primes are found among them, and there can be no embedded component.

To determine the primary components of $\mathfrak{a}$, we localize (as in Theorem 8.28 on the previous page). In the local ring $A = k[x, y]_{(x+1,y-1)}$ where both x and $x - 1$ are invertible, we obtain the equality

$$\mathfrak{a}A = (x^2 - 1, y - x^2) = (x + 1, y - x^2) = (x + 1, y - 1).$$

In similar fashion, in $B = \mathbb{C}[x,y]_{(x-1,y-1)}$ both x and $x+1$ are invertible and one has

$$\mathfrak{a}B = (x^2(x^2-1), y-x^2) = (x-1, y-1).$$

Finally, in $C = k[x,y]_(x,y)$ both $x+1$ and $x-1$ have inverses, and we see that

$$\mathfrak{a}C = (x^2, y).$$

Since there are no embedded components, we conclude that

$$\mathfrak{a} = (x-1, y-1) \cap (x+1, y-1) \cap (x^2, y).$$

When the characteristic of k equals two, there things evolve in a slighty different manner. In that case, then two ideals $(x-1, y-1)$ and $(x+1, u-1)$ conicide and $x^2+1 = (x+1)^2$. We find

$$\mathfrak{a} = ((x+1)^2, y-1) \cap (x^2, y).$$

☆

Problems

8.5 Show that for any scalar $a \in k$ it holds true that ⁂

$$(x^2, xy) = (x) \cap (x^2, y + ax)$$

and that this is a minimal primary decomposition. Show that different scalars a give different decompositions.

8.6 Determine a minimal primary decomposition of (x^3, y^2x^2, y^3x). ⁂

8.7 Let $\mathfrak{a}$ be the ideal in the polynomial ring $k[x,y,z]$ given as $\mathfrak{a} = (yz, xz, xy)$. ⁂ Show that the minimal primary decomposition of $\mathfrak{a}$ is shaped like

$$(yz, xz, xy) = (y,z) \cap (x,z) \cap (x,y).$$

Show that the maximal ideal (x,y,z) is associated to $\mathfrak{a}^2$ and determine a minimal primary decomposition of $\mathfrak{a}^2$. HINT: Consider $(\mathfrak{a} : xyz)$.

8.8 Let $\mathfrak{p}$ be the ideal in the polynomial ring $k[x_1, \ldots, x_n]$ over a field k generated by the r first variables; that is, $\mathfrak{p} = (x_1, \ldots, x_r)$. Show that every power $\mathfrak{p}^m$ is $\mathfrak{p}$-primary. HINT: Consider $\mathfrak{p}^m K[x_1, \ldots, x_r]$ where $K = k(x_{r+1}, \ldots, x_n)$ and show that $\mathfrak{p}^m K[x_1, \ldots, x_r] \cap k[x_1, \ldots, x_n] = \mathfrak{p}^m$. ⁂

8.9 Let k be a field. Let $\mathfrak{p}_s = (x_1, \ldots, x_s)$ in $k[x_1, \ldots, x_n]$ be the ideal generated by the s first variables. Consider ⁂

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \ldots \mathfrak{p}_r = (x_1)(x_1, x_2)(x_1, x_3, x_3) \ldots (x_1, \ldots, x_r).$$

Prove that the following equality holds true

$$\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2 \cap \ldots \cap \mathfrak{p}_{r-1}^{r-1} \cap \mathfrak{p}_r^r$$

and is a minimal primary decomposition of $\mathfrak{a}$. HINT: Show that if $\mathfrak{c}$ is any ideal generated by monomials of degree $s-1$ in $x_1, \ldots, x_s$, then $\mathfrak{c}\mathfrak{p}_s = \mathfrak{c} \cap \mathfrak{p}_s^s$; then use induction on r.

8.10 *(Symbolic powers.)* We have seen that the powers $\mathfrak{p}^n$ of a prime ideal $\mathfrak{p}$ in A are not necessarily $\mathfrak{p}$-primary (unless $\mathfrak{p}$ is maximal). But there is an in some sense canonical primary ideal associated to the powers $\mathfrak{p}^n$; the so-called *symbolic power* $\mathfrak{p}^{(n)}$. They arise in the following way. The ideal $\mathfrak{p}A_\mathfrak{p}$ is maximal in the local ring $A_\mathfrak{p}$ and its powers are therefore primary by Proposition 8.4 on page 175. Pulling primary ideals back along the localization map ι results in primary ideals (Proposition 8.9 on page 177), the ideal $\mathfrak{p}^{(n)} = \iota^{-1}\mathfrak{p}^n A_\mathfrak{p}$ (or when ι is injective $\mathfrak{p}^{(n)} = A \cap \mathfrak{p}^n A_\mathfrak{p}$) will be primary, and this is the n-th symbolic power of $\mathfrak{p}$.

Symbolic powers (symbolske potenser)

a) Show that if n and m are natural numbers it holds that $\mathfrak{p}^{(n)} \cdot \mathfrak{p}^{(m)} \subseteq \mathfrak{p}^{n+m}$

b) Show that $\mathfrak{p}^n = \mathfrak{p}^{(n)}$ if and only if $\mathfrak{p}^n$ has no embedded component.

c) With the notation as in Example 8.2 on page 175, let $\mathfrak{p} = (x, y)$ and determine the symbolic square $\mathfrak{p}^{(2)}$.

8.3 *The homogeneous case*

It is of great interest to know that the subsidiary ideals of a homogeneous ideal arising from a minimal primary decomposition are homogeneous. This not so much because of most ideals one meets in examples or exercises being homogeneous, but because the so-called *projective varieties*, which are ubiquitous in algebraic geometry, are defined by homogeneous ideals.

In what follows, we shall se that the associated primes and the isolated component of homogeneous ideals are homogeneous. When it comes to the more elusive embedded components, all we can hope for is that they may be chosen to be homogeneous, and fortunatly this is the case as well, and the Lasker–Noether theorem is fully valid in a grade context.

Preparitions

8.29 We start with a little lemma (in fact, we already met a version of it in Exercise 1.15 as early as on page 17).

LEMMA 8.30 *Let R be a graded ring and assume that x and y are two elements such that $x \cdot y = 0$. Let x_e be the lowest homogeneous term of x. Then $x_e^\nu y = 0$ for some ν. In particular $x_e^\nu y_i = 0$ for each graded part y_i of y.*

PROOF: Let $x = x_e + \ldots + x_n$ and $y = y_f + \ldots + y_m$ respectively be the expansions of x and y in homogeneous components. We shall show that $x_e^{\nu+1} \cdot y_{f+\nu} = 0$, and letting $\nu = m - f$ we see that the proposition ensues from this. As $x_e y_f$ is the term of xy of lowest degree, it holds that $x_e y_f = 0$, and the induction can start. Expanding the product xy one finds that the homogeneous component of degree $e + f + \nu$ is given as

$$x_e \cdot y_{f+\nu} + x_{e+1} \cdot y_{f+\nu-1} + \ldots + x_{e+j} \cdot y_{f+\nu-j} + \ldots + x_{e+\nu} \cdot y_f = 0.$$

Multiplying through by $x_e^{\nu+1}$ gives $x_e^{\nu+1} \cdot y_{f+\nu} = 0$ because by induction it holds true that

$$x_e^{\nu+1} \cdot y_{f+\nu-j} = x_e^j \cdot x_e^{\nu-j+1} \cdot y_{f+\nu-j} = 0.$$

❑

8.31 The first step in establishing the graded Noether–Lasker Theorem is to see that associated primes to homogeneous ideals are homogeneous.

PROPOSITION 8.32 *Let R be a graded ring and let $\mathfrak{p}$ be a prime ideal associated to the homogeneous ideal $\mathfrak{a}$. Then $\mathfrak{p}$ is homogeneous.*

PROOF: Replacing R by $R/\mathfrak{a}$, we may assume that $\mathfrak{a} = 0$. Let $\mathfrak{p} = (0 : a)$ and assume that $x \in (0 : a)$. If x_e is the homogeneous part of x of lowest degree, the lemma tells us that x_e^ν kills a. Hence $x_e^\nu \in (0 : \mathfrak{a})$ and by consequence $x_e \in (0 : \mathfrak{a})$ as $(0 : a)$ is a prime ideal. Noticing that $x - x_e$ also lies in $(0 : a)$, we may finish off the proof by induction on the degree of the lowest non-vanishing term of x.

❑

8.33 Next step is to treat the primary components, and as alluded to, a embedded components are not unique they are therefore not forced to be homogeneous, but they can be chosen to be homogeneous.For any ideal $\mathfrak{a}$, we shall denote by $\mathfrak{a}^\sharp$ the largest homogeneous ideal contained in $\mathfrak{a}$; that is, the one generated by all homogeneous elements belonging to $\mathfrak{a}$.

LEMMA 8.34 *Let $\mathfrak{q}$ be primary ideal in the graded ring R whose radical is homogeneous. Then $\mathfrak{q}^\sharp$ is primary and $\sqrt{\mathfrak{q}^\sharp} = \sqrt{\mathfrak{q}}$.*

PROOF: We start out by proving that $\mathfrak{q}^\sharp$ has $\sqrt{\mathfrak{q}}$ as its radical. Obviously $\sqrt{\mathfrak{q}^\sharp} \subseteq \sqrt{\mathfrak{q}}$. Attacking the other inclusion, we pick a member $x \in \sqrt{\mathfrak{q}}$. Since $\sqrt{\mathfrak{q}}$ is homogeneous all the homogeneous parts of x lie in $\sqrt{\mathfrak{q}}$, and we can safely assume x to be homogeneous. Since $x^\nu \in \mathfrak{q}$ for some ν, and any homogeneous member of $\mathfrak{q}$ belongs to $\mathfrak{q}^\sharp$, it follows for free that $x^\nu \in \mathfrak{q}^\sharp$ and we are through.

Next, suppose that $xy \in \mathfrak{q}^\sharp$ but that $y \notin \mathfrak{q}^\sharp$. The task is to show that $x \in \sqrt{\mathfrak{q}^\sharp}$; that is, $x \in \sqrt{\mathfrak{q}}$ since the two radicals coincide. If y_f is the homogeneous term in y of lowest degree, we may assume that $y_f \notin \mathfrak{q}^\sharp$, since if y_f lay in $\mathfrak{q}^\sharp$, we might replace y by $y - y_f$, and repeating this procedure if need was, we would

finally end up with an element whose term of lowest degree does not belong to $\mathfrak{q}^\sharp$. With y_f in place outside $\mathfrak{q}^\sharp$, it follows that y_f does not belong to $\mathfrak{q}$, hence $x \in \sqrt{\mathfrak{q}} = \sqrt{\mathfrak{q}^\sharp}$. ❑

8.35 Finally we have come to the graded version of the Lasker–Noether theorem; needless to say, the two uniqueness theorem persist unchanged, they can of course be applied to any minimal primary decompositions.

PROPOSITION 8.36 (GRADED LASKER–NOETHER THEOREM) *A homogeneous ideal in a Noetherian graded ring has a minimal primary decomposition with all components being homogeneous, and all its associated primes are homogeneous.*

PROOF: Observe first that all prime ideals associated to a homogeneous ideals are homogeneous. (Proposition 8.32 above).

It is fairly clear that $(\mathfrak{a} \cap \mathfrak{b})^\sharp = \mathfrak{a}^\sharp \cap \mathfrak{b}^\sharp$ (the homogeneous elements in $\mathfrak{a} \cap \mathfrak{b}$ are the honogenous elements the lie in both $\mathfrak{a}$ and $\mathfrak{b}$!!) so starting out with a minimal primary decomposition $\mathfrak{a} = \bigcap_i \mathfrak{q}_i$ and applying the $\sharp$-construction to it, one arrives at a decomposition

$$\mathfrak{a} = \mathfrak{a}^\sharp = \bigcap_i \mathfrak{q}_i^\sharp, \tag{8.4}$$

and according to Lemma 8.34 on the preceding page, this is a primary decomposition. Moreover, the radicals of the sharpened ideals $\mathfrak{q}_i^\sharp$ are the same as the radicals of the $\mathfrak{q}_i$'s, and we can conclude that (8.4) is a minimal primary decomposition. ❑

Arriving by group actions

The stage in this paragraph is confined to ideals in the polynomial ring over the complex numbers $\mathbb{C}$. The r-dimensional torus $\mathbb{C}^*)^r$ acts on $x = (x_1, \dots, x_r)$ by homothety in the variables; that is $x^t = (t_1 x_1, \dots, t_r x_r)$ and this action induces an action on the polynomial ring $f^t(x) = f(tx)$.

Recall we saw in xxx that an ideal $\mathfrak{a}$ was homogenous if and only if it is invariant under this action. Obviously $\mathfrak{q}^t$ is $\mathfrak{p}^t$-primary if and only if $\mathfrak{q}$ is $\mathfrak{p}$-primary. Hence

$$\mathfrak{a} = \mathfrak{a}^t = \bigcap_i \mathfrak{q}_i^t$$

is a primary decomposition, and $\mathfrak{p}^t$ is obviously the radical of $\mathfrak{q}^t$. We conclude that the associated primes are permuted by G, bu they are finite in number and as G has no finite quotient, each is is invariant under G and hence is homogeneous. Since the isolated components are unique, each of those is invariant as well and is homogenous. As to the embedded components, let $\mathfrak{q}$ be one. After exercise xxx , the intersection $\bigcup_{t \in G} \mathfrak{q}^t$ is $\mathfrak{p}$-primary, and hence a component of $\mathfrak{a}$.

8.4 *Primary decomposition of modules*

The primary decomposition of ideals is easily generalised to modules. In a Noetherian module, any submodule has a primary decomposition, with analogous uniqueness properties as in the ideal case. The proofs are basically the same but with the necessary changes. In this we sketch the development but leave most of the details to the students.

Associated prime ideals

Prime ideals associated to modules (*primidealer assosiert til moduler*)

Generalizing the concept of associated primes for rings, we say that a prime ideal $\mathfrak{p}$ is *associated* to the module M if it is the annihilator of an element x in the M; that is $\mathfrak{p} = (0 : x)$, and in concordance with the notation for rings we denote the the set of associated primes of M by $\operatorname{Ass} M$. We proved in chapter 7 that the ideals maximal among the annihilators of non-zero elements from M are prime ideals (Proposition 7.18 on page 157), so for Noetherian modules we infer that $\operatorname{Ass} M$ is non empty.

PROPOSITION 8.37 *Let A be a ring and M a Noetherian A-module. Then* $\operatorname{Ass} M$ *is finite and non-empty. The minimal primes in* $\operatorname{Ass} M$ *and* $\operatorname{Supp} M$ *coincide.*

PROOF: This follows from The structure theorem on page 158. ❑

The radical $\sqrt{(0)} = \{ x \in A \mid \ x \text{ acts nilpotently on } M \ \}$ is an ideal, and is a prime ideal if M is primary. Indeed, if $(xy)^\nu$ kills M and no power of y does, there is a $z \in M$ so that $y^n z \neq 0$; and since $x^n(y^n z) = 0$, it follows that x is nilpotent as M is primary

PROPOSITION 8.38 *Every Noetherian module has a primary decomposition*

PROOF: Let N be the maximal rascal, and replace M by M/N. That is M is not primary. Hence $xz = 0$ but the homothety by x is not nilpotent. Let $\ker[x^i] \subseteq \ker[x^{i+1}]$ is an ascending chain, hence stabilizes at certain point, say ν. We contend that $(0) = \ker[x] \cap x^\nu M$. Indeed, if $xz = 0$ and $z = x^v w$ it follows that $w \in \ker[x]^{v+1}$, hence in $\ker[x]^v$. By consequence $z = x^{\nu+1} w = 0$. We ❑

Primary modules

Given a submodule N of the module M, one has the transporter ideal $(N : M)$ consisting of ring elements that multiply M into N; that is

$$(N : M) = \{ x \in A \mid xM \subseteq N \},$$

and the radical $\sqrt{(N : M)}$ is called the radical of N relative to M. The elements are the ring elements such a power multiplies M into M. If $N = 0$, they consist of the ring elements inducing a nilpotent homothety on M.

and one extends the notion of primary ideals to modules in the following fashion:

- The homothety by x on M/N is either injective or nilpotent.

Or in other words

- if $xz \in N$ then either $z \in N$ or $xN \in (N : M)$ for some n

PROPOSITION 8.39 *Let $N \subseteq M$ be a module and a submodule.*

- *If N is primary, the radical $(N : M)$ is a primary ideal and the consequently the radical $\mathfrak{p} = \sqrt{(N : M)}$ is a prime ideal. One says that N is $\mathfrak{p}$-primary.*
- *Finite intersections of $\mathfrak{p}$-primary submodules are $\mathfrak{p}$-primary.*
- *If N is $\mathfrak{p}$-primary and $S \cap \mathfrak{p} = \varnothing$, then N_S is $\mathfrak{p}A_S$-primary submodule of M_S.*
- *Assume that $L \subseteq N$. Then N is $\mathfrak{p}$-primary, then N/L is a $\mathfrak{p}$-primary submodule of M/L.*

Lecture 9

Integral extensions

Preliminary version 1.1 as of 2018-11-19 at 16:45 (typeset 3rd December 2018 at 10:03am)—For the moment nothing here!! Prone to misprints and errors and will change.

Completely rewritten and extended a lot. For the moment not many exercises or examples—hopefully this will follow soon. Also probably peppered with misprints and impressions (sorry, improvements will shortly follow) and organisation will also be better soon.

19/11/2018 Corrected som mistakes and imoroved the text many places.

From an algebraic point of view there is a huge difference between the ring of integers $\mathbb{Z}$ and the field of rationals $\mathbb{Q}$; we need only mention the primes. They are visible in $\mathbb{Z}$ as generators of the prime ideals, but in $\mathbb{Q}$ they are, at least from an algebraic point of view, on an equal footing with the other units. When the exploration of number fields[1] begun, an immediate want arose to have subrings playing the role of the integers and where the deep secrets of the field could be revealed. These rings was made up of the "integral elements" in the field, or more precisely those being integral over $\mathbb{Z}$.

[1] That is, finite field extensions of the rationals

In algebraic geometry these rings give rise to what is called normal varieties where the geometry of the codimension one subvarieties strongly influence the geometry of the entire space.

9.1 Definition and basic properties

Throughout this section the setting will be an extension of rings $A \subseteq B$; that is, a pair of a ring and subring. An element $x \in B$ is said to *integral* over A if it satisfies a monic relation as

Integral elements (*hele elementer*)

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, \tag{9.1}$$

where the coefficients a_i are members of A. It is all-important that the leading coefficient be one, so there is heavy stress on the word *monic*. This distinguishes integral elements from their cousins the algebraic elements, which satisfy similar equations, but without constraints on the leadings coefficient; of course, if the leading coefficient is invertible in A it goes for the same. A relation like (9.1) is called an *integral dependence relation* for x over A.

Integral dependence relation (*helavhenighetsrelasjon*)

9.1 If all the elements in B are integral over A one says that B is *integral over* A or that B is an *integral extension* of A. The subset of B consisting of the elements integral over A is called the *integral closure* of A in B and is denotes by $\bar{A}$. Of course it depends on B, but to keep notation simple, we do not include a reference to B in the notation—the context will make it clear where the integral closure is taken.

Integral extension (*hel utvidlese*)
Integral closure (*helavslutningen*)

It is a basic, but subtle fact that the integral closure is ring, which we shortly shall prove. Finally, one says that A is *integrally closed* in B if $A = \bar{A}$; that is, every element which is integral over A belongs to A.

Integrally closed (*helavsluttet*)

9.2 Both in algebraic geometry and algebraic number theory the integral closure of a domain A in its field of fractions is a frequently used construction and we shall use the notation $\widetilde{A}$ for it to distinguish it from all the crowd. Domains being integrally closed in their field of fractions; that is, those satisfying $A = \widetilde{A}$, are called *normal*, and for general domians $\widetilde{A}$ is sometimes called the *normalization* of A.

Normal rings (*normale ringer*)
Normalization (*normalisering*)

9.3 To illustrate the difference between algebraic an integral dependence relation consider the two simple equations

$$y^2 - z = 0$$
$$(z-1)y^2 - z = 0$$

over the complex numbers. The first one "has $\sqrt{z}$ as a solution", but due to the ambiguity of the square root, it is impossible to find a continuous (yet alone analytic) solution in the entire plane Only in simply connected domain not containing the origin can a continuous solution be found. The solutions of the second equation suffer the same defect, but additionally they acquire a pole at $z = 1$. The difference between solutions of algebraic and integral relations is precisely the occurrence of poles in the former.

EXAMPLE 9.1 The golden section $(1+\sqrt{5})/2$ is integral over $\mathbb{Z}$ as it satisfies the equation

$$x^2 - x - 1 = 0.$$

The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{5})$ equals $\mathbb{Z}[(1+\sqrt{5})/2]$. Indeed, a number $a + b\sqrt{5}$ has the minimal equation

$$x^2 - 2ax + (a^2 - 5b^2) = 0,$$

and if it is integral over $\mathbb{Z}$, the coefficients are integral by Gauss lemma (Exercise 3.1 on page 64). Then $n = 2a \in \mathbb{Z}$ and $20b^2 \in \mathbb{Z}$, and hence $m = 2b \in \mathbb{Z}$ as well. Substituting back, gives $0 \equiv (n^2 - 5m^2) \equiv (n^2 - m^2) \mod 4$, which holds if and only if m and n have the same parity. ☆

EXAMPLE 9.2 The ring of integers in the number field $\mathbb{Q}(i\sqrt{5})$ equals $\mathbb{Z}[i\sqrt{5}]$. Indeed, the minimal equation of an element $a + ib\sqrt{5} \in \mathbb{Q}(i\sqrt{5})$ is

$$x^2 - 2ax + a^2 + 5b^2 = 0.$$

If x is integral over $\mathbb{Z}$, the coefficients are integral, and as in the previous example, this entails that $n = 2a$ and $m = 2b$ are integral. Substituting back gives $0 \equiv n^2 + 5m^2 \equiv m^2 + n^2 \mod 4$, which occurs only if both n and m are even (squares are either equal to 1 or 0 $\mod 4$). Hence a and b are integers.

The difference between the ring of integers in these two example illustrates a general phenomenon. If d square free, the ring of integers in $\mathbb{Q}(\sqrt{d})$ equals $\mathbb{Z}[(1+\sqrt{d})/2]$ when $d \equiv 1 \mod 4$ and equals $\mathbb{Z}[\sqrt{d}]$ else. ☆

The basic properties

9.4 If x is an element of B which is integral over A, the subring $A[x]$ of B obtained by adjoining the element x to A is a *finitely generated* A-module. An integral dependence relation as (9.1) above, entails that

$$x^n = -(a_{n-1}x^{n-1} + \ldots + a_1 x + a_0),$$

and a straightforward induction yields that $A[x]$ is generated by the n first powers of x. The converse is also true, as shown in the next proposition. When the A-module $A[x]$ is Noetherian, this comes almost for free; one just considers the ascending chain $M_i = (1, x, x^2, \ldots, x^i)$ of submodules of $A[x]$, and at the point where it stabilises; that is, when $M_{\nu+1} = M_\nu$, one obtains an integral dependence relation for x since $x^{\nu+1} \in M_\nu$. For the general proof a little twist is needed.

PROPOSITION 9.5 (BASIC CHARACTERISATION) *Let $A \subseteq B$ be an extension of rings and $x \in B$ an element. The following three statements are equivalent:*

- ❏ *The element x is integral over A;*
- ❏ *$A[x]$ is a finite A-module;*
- ❏ *There is faithful $A[x]$-module which is finite over A.*

PROOF: The only implication that shows any substantial resistance is that the last statement entails the first. So let M be a module as in the last assertion and let $m_1, \ldots, m_n$ be generators for M over A. One may express each element $x \cdot m_i$ in terms of the m_j's, and this gives relations

$$x \cdot m_i = f_{ij}m_1 + \ldots f_{in}m_n$$

for $1 \leqslant i \leqslant n$ where each $f_{ij} \in A$. We introduce an $n \times n$-matrix Φ by letting $\Phi = x \cdot I_n - (f_{ij})_{ij}$ where I_n is the identity matrix[2]. The equations above then translate into $\Phi \cdot m = 0$ with $m = (m_1, \ldots, m_n)$. Hence $\det \Phi = 0$ by the determinantal trick (Lemma 9.47 on page 209). But developing the determinant shows that $\det(x \cdot I_n - (f_{ij}))$ is a monic polynomial in x whose coefficients lie in A; that is, $\det \Phi = 0$ is an integral dependence relation for x over A. ❏

[2] For $n = 3$ the matrix Φ is shaped like
$$\begin{pmatrix} x - f_{11} & f_{12} & f_{13} \\ f_{21} & x - f_{22} & f_{23} \\ f_{31} & f_{32} & x - f_{33} \end{pmatrix}$$

We notice the immediate corollary—which may also easily be proven *ad hoc*—that all elements in $A[x]$ are integral over A when x is. An $A[x]$ module M which is finite over A, will be faithful over any subring of $A[x]$, in particular over $A[z]$ for any $z \in A[x]$.

COROLLARY 9.6 *If x is integral over A, all elements in $A[x]$ are integral over A.*

9.7 There is a close relationship between integral and finite extensions as was unveiled in the previous proposition. Finite extensions are integral, but in general the converse is not true. There are even examples of Noetherian domains whose normalizasion $\widetilde{A}$ is not a finite module over A; they are however, rather exotic creatures, and the lions share of the rings appearing in mainstream algebraic geometry—that is, domains finitely generated over field and their localizations—have normalizations which are finitely generated as modules.

9.8 The first conclusion to be drawn from the Basic Characterization is that finitely generated algebras which are integral, are finitely generated modules; an important observations since the integral closure being finite over A or not, is an issue. One has

PROPOSITION 9.9 *Let B be an integral ring-extension of A. Any subalgebra C of B which is a finitely generated algebra over A, is a finite A-module.*

PROOF: The poof goes by induction on the number of generators of C. So let $C' \subseteq C$ be a subalgebra generated over A by the same elements as C but one. By induction C' is finite over A, and $C = C'[x]$ with $x \in C$ the last generator. The element x being integral over A is even so more over C'. Hence C is finite over C' by Proposition 9.5, and because the property of being a finite extension is transitive in towers (Lemma 9.48 on page 209 in the appendix), it holds that C is finite over A. ❑

COROLLARY 9.10 (TRANSITIVITY) *Assume that $A \subseteq B \subseteq C$ are ring-extension and that B is integral over A. Then every element in C which is integral over B is integral over A.*

PROOF: Let x be an element in C which is integral over B and satisfies the dependence relation

$$x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n = 0. \tag{9.2}$$

with the coefficients b_i lying in B. We let D be the sub A-algebra of B the b_i's generate. Then x is integral over D (the relation (9.2) has coefficients in D) and consequently $D[x]$ is a finite module over D. Now, D is a finite module over A after the Proposition and therefore $D[x]$ is finite over A as well. Hence we can conclude by the Basic Characterization of integral elements. ❑

9.11 It is by no means obvious how to deduce a dependence relation for a product (or for a sum) from a dependence relation for the factors (or the addends); that the integral closure is a ring, is a slightly subtle property. However, once the Basic Characterisation (Proposition 9.5 on page 193) is in place, it follows readily. For a different approach, see Problem 9.4 on the following page.

PROPOSITION 9.12 (THE INTEGRAL CLOSURE IS A RING) *If x and y are elements in B both integral over A, then their sum and product are integral over A as well. The integral closure $\bar{A}$ of A in B is a subring of B. The integral closure $\bar{A}$ is integrally closed in B.*

PROOF: This is just a combination of Corollary 9.6 and the transitivity property (Corollary 9.10). Indeed, let x and y be integral over A. The ring A[x] is an integral extension of A and y being integral over A, the extension $A[x,y]$ is integral over $A[x]$. Hence $A[x,y]$ is integral over A by the transitivity. In particular, this applies to both the product $x \cdot y$ and the sum $x + y$.

The last statement of the proposition might appear as a tautology, but an argument is in fact needed. We have to see that elements integral over $\bar{A}$ are integral over A, which is exactly what Corollary 9.10 above tells us since $\bar{A}$ is integral over A. ❑

Integral extensions, localization and quotients

Integral extensions are well behaved and compatible with the formation of localizations and quotients.

9.13 We treat the loacalizations first:

PROPOSITION 9.14 *Let $S \subseteq A$ be a multiplicatively closed subset and assume that B is an integral extension of A. Then B_S is an integral extension of A_S. Forming the integral closure commutes with localization; i.e. holds that $\overline{(A_S)} = (\bar{A})_S$.*

PROOF: Let xs^{-1} be an element in B with $x \in A$ and $s \in S$. All elements of B are integral over A, so x satisfies an integral dependence relation shaped like

$$x^n + a_{n-1}x^{n-1} + \ldots + a_i x^i + \ldots + a_0 = 0$$

with the a_i's lying in A. Multiplying through by s^{-n} we find the relation

$$(xs^{-1})^n + a_{n-1}s^{-1}x^{n-1}s^{-(n-1)} + \ldots + a_i s^{-n+i}(xs^{-1})^i + \ldots + a_0 s^{-n} = 0, \quad (9.3)$$

which is a monic equation whose coefficients lie in A_S and hence is an integral dependence relation for xs^{-1} over A_S.

For the second statement, the inclusion $(\bar{A})_S \subseteq \overline{(A)_S}$ ensues from the first claim, and it suffices to prove that $\overline{(A)_S} \subseteq (\bar{A})_S$. To that end, assume that $xs^{-1} \in \overline{(A)_S}$. It satisfies an integral dependence relation as

$$(xs^{-1})^n + b_{n-1}(xs^{-1})^{n-1} + \ldots + b_i(xs^{-1})^i + \ldots + b_0 = 0, \quad (9.4)$$

where each b_i lies in A_S and hence may be written as $b_i = a_i t^{-1}$ with $a_i \in A$ and $t \in S$ (extending the fractions, we may use a common denominator for all the b_i's). Multiplying (9.5) through by t^n yields the relation

$$(txs^{-1})^n + ta_{n-1}(txs^{-1})^{-(n-1)} + \ldots + t^{n-i-1}a_i(txs^{-1})^i + \ldots + t^{n-1}a_0 = 0, \quad (9.5)$$

and it follows that tx is integral over A. We conclude that $xs^{-1} = (tx)s^{-1}t^{-1} \in (\bar{A})_S$. ❑

9.15 Next comes the quotients, and in addition to the usual the staging of this chapter with an integral extension $A \subseteq B$, an ideal $\mathfrak{b}$ in B is given. We let $\mathfrak{a}$ be the ideal $\mathfrak{b}$ induces in A; that is, $\mathfrak{a} = A \cap \mathfrak{b}$. Then $A/\mathfrak{a} \subseteq B/\mathfrak{b}$ is an extension, and it persits being integral.

PROPOSITION 9.16 *Let $\mathfrak{b} \subseteq B$ be an ideal and let $\mathfrak{a} = \mathfrak{b} \cap A$. If B is integral over A, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.*

PROOF: Let $x \in B/\mathfrak{b}$ and let $y \in B$ be an element that maps to x. By assumption it is integral over A and there is therefore a relation

$$y^n + a_{n-1}y^{n-1} + \ldots + a_1 y + a_0 = 0$$

with the a_i's from A. Reducing that relation modulo $\mathfrak{b}$ gives the relation

$$x^n + [a_{n-1}]x^{n-1} + \ldots [a_1]x + [a_0] = 0,$$

where $[a_i]$ as usual denotes the classes of a_i in $A/\mathfrak{a}$. Hence x is integral over $A/\mathfrak{a}$. ❑

Problems

9.1 Let B be a ring and $\{B_i\}_{i\in I}$ a family of subrings of B. If each B_i is integrally closed in B, then the intersection $\bigcap_{i\in I} B_i$ is integrally closed as well.

9.2 Assume that $\{B_i\}_{i\in I}$ is a family of subrings of a field K. Prove that if each B_i is integrally closed in K, then the intersection $\bigcap_{i\in I} B_i$ is as well.

9.3 Show that x is integral over A if and only if there is a square matrix with coefficients in A having x as an eigenvalue.

9.4 Show that if x and y are eigenvalues for Φ and Ψ then $x \cdot y$ is and eigenvalue for the Kronecker product $\Phi \otimes \Psi$ and that $x + y$ is one for the matrix $\Phi \otimes I_m + I_n \otimes \Psi$ where the I_n are I_m are identity matrices of appropriate size. Conclude that the integral closure is a ring.

★

Being normal is a local property

As mention in the introduction to this section, a particular important situation is when A is a domain and $B = K(A)$ is the field of fractions of A. Recall that the integral closure of A in $K(A)$ is called *normalization* of A, and in case A is integrally closed in $K(A)$, one says that A is a *normal domain*.

Normalizations (*normaliseringer*)
Normal domains (*normale områder*)

9.17 Being normal is a local property.

PROPOSITION 9.18 (BEING NORMAL IS LOCAL) *Assume that A is a domain. Then A is normal if and only if $A_{\mathfrak{m}}$ is normal for all maximal ideals $\mathfrak{m}$ in A. It is also equivalent to $A_{\mathfrak{p}}$ being normal for all prime ideals $\mathfrak{p}$ in A.*

PROOF:

Notice first, that all the localization $A_{\mathfrak{m}}$ have K as fraction field as well. Consider the inclusion $A \hookrightarrow \widetilde{A}$, which fits into the short exact sequence

$$0 \longrightarrow A \longrightarrow \widetilde{A} \longrightarrow \widetilde{A}/A \longrightarrow 0$$

of A-modules. Because localization is an exact functor, it gives rise to the following short exact sequence

$$0 \longrightarrow A_{\mathfrak{m}} \longrightarrow (\widetilde{A})_{\mathfrak{m}} \longrightarrow (\widetilde{A}/A)_{\mathfrak{m}} \longrightarrow 0$$

when localized at a maximal ideal $\mathfrak{m}$. According to Proposition 9.14, forming integral closures commute with localization, so it holds that $(\widetilde{A})_{\mathfrak{m}} = (\widetilde{A}_{\mathfrak{m}})$. Thence $(\widetilde{A}/A)_{\mathfrak{m}} = (\widetilde{A}_{\mathfrak{m}})/A_{\mathfrak{m}}$, and the claim follows by the Localness of Being Zero (Proposition 6.62 on page 144). ❑

9.19 In the case $\widetilde{A}$ is finite over A, the quotient $\widetilde{A}/A$ is finitely generated over A as well, and it ensues that Supp $A/\widetilde{A}$ is a closed subset of Spec A equal to $V(\text{Ann}\, A/\widetilde{A})$. And localizing at (0), or equivalently tensorizing by K, we see that $\widetilde{A}/A \otimes_A K = 0$ because A and $\widetilde{A}$ both have K as fraction field. Hence $\widetilde{A}/A$ is not of global support. So in that good case, when $\widetilde{A}$ is finite over A, for "most" primes $\mathfrak{p}$ the local ring $A_{\mathfrak{p}}$ is normal;that is, for primes in an open non-empty subset of Spec A.

9.2 *Examples*

We indulge ourselves in two examples of rather large classes of rings that are normal. Firstly, the unique factorization domains are always normal, and secondly, there is a principle that rings of invariant of the actions of a finite groups are normal, at least when the ring upon which the group act is normal. This class includes the so-call "quotient singularities". We shall treate a few simple examples in detail but leave the general case to the zealous students in the form of a guided exercise.

9.20 We start out with the UFD-case.

PROPOSITION 9.21 *If the domain A is a* UFD*, then A is normal.*

PROOF: Let K be the fraction field of A, and let $z = x/y \in K$ be an element which is integral over A, and we may assume that x and y are without common factors. The element z being integral means there is a relation

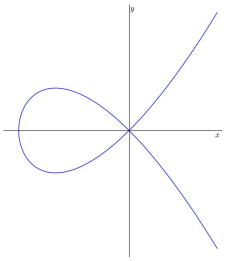
$$z^n + a_{n-1}z^{n-1} + \ldots + a_i z^i + \ldots + a_0 = 0$$

with the a_i's lying in A. Multiplying through by y^n and moving the leading term to the left, gives

$$-x^n = a_{n-1}x^{n-1}y + \ldots + a_i x^i y^{n-i} + \ldots + a_0 y^n.$$

Every irreducible factor of y divides the right side, hence it divides the left side and consequently also x. Contradiction. ❑

EXAMPLE 9.3 Integral closures and normalizations play an important role in algebraic geometry which is particularly accentuated in the theory of curves. To illustrate this, we let $C \subseteq \mathbb{C}^2$ be the plane curve parametrized by $x = t^2 - 1$ and $y = t(t^2 - 1)$. It is easily seen to satisfy the equation $y^2 = x^2(x + 1)$; indeed, $(y/x)^2 = t^2 = x + 1$.



The real points of the curve is depicted in the margin. For points on C with $x \neq 0$ the corresponding parameter value is uniquely defined, and the parametrization is one-to-one away from the origin. However, the two parameter values $t = \pm 1$ both give the origin, and the curve has a double point there.

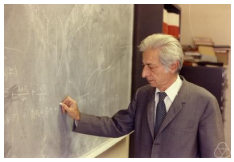
The parametrization may be though of as the map $\operatorname{Spec} \mathbb{C}[t] \to \operatorname{Spec} \mathbb{C}[x, y]$ induced by the ring-map $\mathbb{C}[x, y] \to \mathbb{C}[t]$ that sends $x \to t^2 - 1$ and $y \to t(t^2 - 1)$; or in the language of varieties, it is the the map $\mathbb{C} \to C = V(y^2 - x^2(x - 1)) \subseteq \mathbb{C}^2$ sending t to the point $(t^2 - 1, t(t^2 - 1))$.

This leads to considering the subring $A = \mathbb{C}[t^2 - 1, t(t^2 - 1)] \subseteq \mathbb{C}[t]$. The point of the example is that t is integral over A; indeed, almost tautologically it satisfies the equation

$$X^2 - t^2 = 0,$$

and $t^2 = (t^2 - 1) + 1 \in A$.

Moreover, the ratio between the two generators of A equals t, so that its fraction field is $\mathbb{C}(t)$. Now, the polynomial ring $\mathbb{C}[t]$ being a UFD is normal, and we can conclude that $\mathbb{C}[t]$ equals the normalization of A. It is typical for curves that their normalisation "resolves the singularities"; that is, it separates the different branches of the curve passing through the double points (or points of of higher multiplicity). ☆



Abraham Seidenberg
(1916–1988)
American mathematician

Rings of invariants

9.22 Now comes the promised result on rings of invariants, and as promised, we shall proceed rather in relaxed way merely treating the simples possible case. That is, the case of a cyclic group of order two acting on a normal domain B. Such an action is just given by an *involution* on B; in other words, a ring map $\sigma\colon B \to B$ with $\sigma^2 = \mathrm{id}_B$. The map σ extends to an involution of the fraction field K of B by the obvious assignment $\sigma(xy^{-1}) = \sigma(x)\sigma(y)^{-1}$. Furthermore, we let $A = B^\sigma = \{\, x \in B \mid \sigma(x) = x \,\}$ be the ring of invariants and L its field of fractions. In this setting we have

Involutions (*involusjoner*)

PROPOSITION 9.23 *It holds true that $L = K^\sigma = \{\, z \in K \mid \sigma(z) = z \,\}$. Moreover B is integral over A and if B is normal, A will be normal.*

PROOF: Clearly $L \subseteq K^\sigma$. If $\sigma(x)/\sigma(y) = x/y$ it holds that $y\sigma(x) = x\sigma(y)$, and we may write $x/y = \sigma(x)x/\sigma(x)y$ with both $\sigma(x)x$ and $\sigma(x)y$ being invariant. Hence $L = K^\sigma$.

Any $x \in B$ satisfies the relation

$$x^2 - (\sigma(x) + x)x + \sigma(x)x = 0. \tag{9.6}$$

$$\begin{array}{ccccc} K^\sigma = & L & \subseteq & K \\ & \cup\!| & & \cup\!| \\ B^\sigma = & A & \subseteq & B \end{array}$$

Both $\sigma(x) + x$ and $x\sigma(x)$ are invariant under σ and belong therefore to A, hence (9.6) is an integral dependence relation for x over A.

Finally, as B is integral over A, the integral closure of A in K equals $\widetilde{B}$ by transitivity, and hence $\widetilde{A} = \widetilde{B} \cap L$. From this ensues that $A = B \cap L = \widetilde{A}$ in case $B = \widetilde{B}$. ❑

9.3 *The Cohen–Seidenberg Theorems*

There is cluster of results proven by I. S. Cohen and A. Seidenberg dubbed "going–up", "going–down" and "lying–over" by Cohen and Seidenberg. They all relate prime ideals in one ring to prime ideals in another ring which is integral over the first. So let $A \subseteq B$ be the two rings. Every prime ideal $\mathfrak{q} \subseteq B$ intersects A in a prime ideal $\phi = A \cap \mathfrak{q}$, and this is sets up the canonical map Spec $B \to$ Spec A. We call π. The results are basically about this map and he proofs hinge on a basic lemma which is first we prove.

Basic lemma—the case of fields

9.24 The basic lemma treats the special case of fields:

LEMMA 9.25 *Let $A \subseteq B$ be an integral extension of domains. If one of the rings is a field the other one is as well.*

PROOF: Assume first that B is a field. If $y \in A$ is an element, the inverse y^{-1} is integral over A and satisfies a dependence relation

$$y^{-n} + a_{n-1}y^{-(n-1)} + \ldots + a_1 y^{-1} + a_0 = 0.$$

Multiplying through by y^n gives

$$1 + y(a_{n-1} + \ldots + a_1 y^{n-2} + a_0 y^{n-2}) = 0$$

which shows that y is invertible in A. Next assume that A is a field, and let $x \in B$ be given. It satisfies a relation

$$x^n + a_1 x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

and assuming that the degree n is minimal, it holds that $a_0 \neq 0$. Then a_0 is invertible and we have

$$x \cdot a_0^{-1}(x^{n-1} + a_1 x^{n-2} + \ldots + a_1) + 1 = 0.$$

❑

COROLLARY 9.26 *Assume that $A \subseteq B$ is an integral extension. A prime ideal $\mathfrak{n}$ in B is maximal if and only if $\mathfrak{n} \cap A$ is maximal.*

PROOF: The extension

$$A/\mathfrak{n} \cap A \subseteq B/\mathfrak{n}$$

is integral by Proposition 9.16 on page 196, and the corollary ensues since the quotient by an ideal is a field if and only if the ideal is maximal. ❑

The Lying–Over Theorem

the Lying-over Theorem (*Lying–over-teoremet*)

The first theorem we shall treat—*the Lying-over Theorem*—gives the structure of the fibres of the map π; that is, it gives a qualitative description of the set of prime ideals in B intersecting A in a given fixed prime ideal. The fibres are not empty, or in other words, all prime ideals $\mathfrak{p}$ in A are of the form $\mathfrak{p} = \mathfrak{q} \cap A$, and moreover, there are no inclusion relations between the members of the fibres. In topological terms this means that the fibres of π are discrete topological spaces.

9.27 Here it comes:

PROPOSITION 9.28 (LYING-OVER) *The map π is surjective, and the fibres are discrete. In other words, for each $\mathfrak{p} \subseteq A$ there is at least one $\mathfrak{q} \subseteq B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. Moreover, if $\mathfrak{q}$ and $\mathfrak{q}'$ are prime ideals in B with $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$ and $q \subseteq \mathfrak{q}'$, then $\mathfrak{q} = \mathfrak{q}'$.*

PROOF: We begin with treating the local case; the rest of the proof is a reduction to that case.

Assume then that A is local with maximal ideal $\mathfrak{m}$. Let $\mathfrak{n}$ be any maximal ideal in B which exists according to the Basic Existence Theorem (Theorem 2.50 on page 40). By Corollary 9.26 $\mathfrak{n} \cap A$ is maximal, hence equal to $\mathfrak{m}$ since $\mathfrak{m}$ is the only maximal ideal in A.

To see that no ideal in the fibre is contained in another, assume that $\mathfrak{q} \subseteq \mathfrak{q}'$ and that both intersect A in $\mathfrak{m}$ (we are still in the local situation). Again by Corollary 9.26 both $\mathfrak{q}$ and $\mathfrak{q}'$ are maximal and must be equal since $\mathfrak{q} \subseteq \mathfrak{q}'$.

Let $\mathfrak{p}$ be a prime ideal in A. In order to reduce the general case to a local situation we pass to the localized $A_\mathfrak{p} \subseteq B_\mathfrak{p}$ extension, which persists being integral in view of Proposition 9.14. According to what we established in the local case, there is an ideal in $B_\mathfrak{p}$, which as all ideals in $B_\mathfrak{p}$ is of the form $qB_\mathfrak{p}$, such that $\mathfrak{q}B_\mathfrak{p} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. But then $\mathfrak{q} \cap A = \mathfrak{p}$, this follows *e.g.* as

$$(A_\mathfrak{p} \cap \mathfrak{q}B_\mathfrak{q}) \cap A = A \cap \mathfrak{q}A_\mathfrak{p} = a \cap (B \cap \mathfrak{q}B_\mathfrak{p}) = A \cap \mathfrak{q}$$

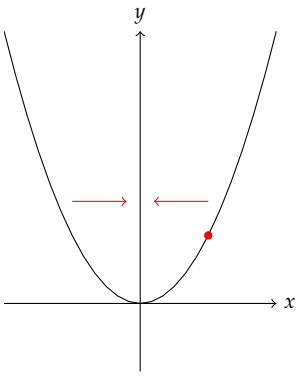
.

If $q \cap A = q' \cap A = \mathfrak{p}$ for two prime ideals in B, one included in the other, it holds by the local case that $\mathfrak{q}B_\mathfrak{p} = \mathfrak{q}'B_\mathfrak{p}$, and hence $\mathfrak{q}$ and $\mathfrak{q}'$ are equal. ❑

EXAMPLE 9.4 It might well happen that π is surjective and has finite fibres without B being integral over A. An example can be the extension

$$A = k[x^2] \subseteq k[x, (x-1)^{-1}] = B$$

where we assume that k is algebraically closed and not of characteristic two. The geometric interpretation of the example is the parabola X given as $y = x^2$ with a hole punched in it; that is, the point $(1, 1)$ is removed. The map π is just projection $X \backslash \{(1, 1)\}$ to the y-axis.



The ring $k[x^2]$ is isomorphic to the polynomial ring $k[y]$ (rebaptize x^2 to y). Every maximal ideal $\mathfrak{m}$ in A is of therefore the form $x^2 - a^2$ (all elements in k have a square-root) with $a \neq 0$, and it holds true that $(x-a)B \cap A = (x^2 - a^2)A$ since $x^2 - a^2 = (x+a)(x-a)$. However $(x-1)^{-1}$ is not integral over A; indeed, if it were, multiplying an integral dependence relation of degree n by $(x-1)^n$, would yield a relation

$$1 + p_{n-1}(x-1) + \ldots + p_1(x-1)^{n-1} + p_0(x-1)^n = 0,$$

where the coefficients p_i's are elements on $k[x^2]$; that is, they are polynomials $p_i(x^2)$ in x^2. Putting $x = 1$ gives an obvious contradiction.

As of the fibres, it is a nice exercise to check that if $a \neq 1$, the two prime ideals (x-a)B and $(x+a)B$ are the ones lying over $(x^2 - a^2)A$, but the sole prime ideal lying over $(x-1)A$ is $(x+1)B$. ☆

PROBLEM 9.5 Let $A \subseteq B$ be an integral extension. Show that the map $\pi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ is a closed map, by showing that $\pi(V(\mathfrak{a})) = V(\mathfrak{a} \cap A)$ for any ideal $\mathfrak{a}$ in A. HINT: Apply Lying–Over to the extension $A/\mathfrak{a} \cap A \subseteq B/\mathfrak{a}$. ★

Going–Up

The Going–Up Theorem (*Going–Up teoremet*)

The *Going–Up Theorem* is about extending, or lifting as one also says, ascending chains of prime ideals in A to chains in B by climbing them; contrary to the Going–Down Theorem where chains are lifted by a downwards "move ment". If a one-step chain in A can be lifted, an easy induction ensures that any finite ascending chain $\{\mathfrak{p}_i\}$ of prime ideals in A can be lifted ; that is, there is an ascending chain $\{\mathfrak{q}_i\}$ of prime ideals in B so that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.

$$\begin{array}{ccccc} \mathfrak{q}_0 & \subseteq & \mathfrak{q}_1 & \subseteq & B \\ \cup| & & \cup| & & \cup| \\ \mathfrak{p}_0 & \subseteq & \mathfrak{p}_1 & \subseteq & A \end{array}$$

9.29 The one step case is what is usually called the Going–Up Theorem

Theorem 9.30 (Going–Up) *Let $A \subseteq B$ is an integral extension of rings, and let $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$ be two prime ideals in A. Furthermore assume that $\mathfrak{q}_0$ is a prime ideal in B lying over $\mathfrak{p}_0$. Then there is a prime ideal $\mathfrak{q}_1$ in B containing $\mathfrak{q}_0$ and lying over $\mathfrak{p}_1$.*

Proof: Consider the extension $A/\mathfrak{p}_0 \subseteq B/\mathfrak{q}_0$ which is integral by Proposition 9.16. By the Lying-Over Theorem, there is a prime ideal in $B/\mathfrak{q}_0$ lying over $\mathfrak{p}_1/\mathfrak{p}_0$. As all prime ideals in $B/\mathfrak{q}_0$ are, it is shaped like $\mathfrak{q}_1/\mathfrak{q}_0$ for some $\mathfrak{q}_1$ in B. Then $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. ❑

Corollary 9.31 (Going–Up II) *Any finite chain $\{\mathfrak{p}_i\}$ of prime ideals in A has a chain $\{\mathfrak{q}_i\}$ of prime ideals in B lying over it.*

Proof: The proof goes by induction on the number of prime ideals in the chain A, and one should find it completely transparent pondering the following display:

$$\begin{array}{ccccccccc} \mathfrak{q}_0 & \subset & \mathfrak{q}_1 & \subset & \dots & \subset & \mathfrak{q}_{n-1} & & \\ \cup| & & \cup| & & & & \cup| & & \\ \mathfrak{p}_0 & \subset & \mathfrak{p}_1 & \subset & \dots & \subset & \mathfrak{p}_{n-1} & \subset & \mathfrak{p}_n \end{array}$$

The upper chain exists by induction, an one just fils in the upper right corner citing the Going–Up Theorem. ❑

9.32 A chain $\{\mathfrak{q}_i\}$ in B that lifts the chain $\{\mathfrak{p}_i\}$, will be saturated whenever $\{\mathfrak{p}_i\}$ is; indeed, any prime strictly in between $\mathfrak{q}_i$ and $\mathfrak{q}_{i+1}$ would either meet A in $\mathfrak{p}_i$ or $\mathfrak{p}_{i+1}$ since $\{\mathfrak{p}_i\}$ is saturated, but this can not happen since Lying–Over guarantees there are no inclusions among primes in the fibres. We conclude that the suprema of the lengths of chains in the two rings coincide, and hence we have

Corollary 9.33 *If $A \subseteq B$ is an integral extension, then A and B have the same Krull-dimension, or in symboles* $\dim B = \dim A$.

Going–Down

The Going–Down property (*Going–Down-egenskapen*)

The *Going–Down Theorem* the version for descending along chains. One says that *Going–Down* property holds for an extension $A \subseteq B$ if for any pair $\mathfrak{p}_1 \subseteq \mathfrak{p}_0$ of prime ideals in A and any prime ideal $\mathfrak{q}_0$ in B lying over $\mathfrak{p}_0$ there is a prime

ideal $\mathfrak{q}_1$ contained in $\mathfrak{q}_0$ and lying over $\mathfrak{p}_1$; in other words lifted chains may be continued downwards. When A and B domains and A integrally closed in its fraction field the Going-Down property holds for te extension $A \subseteq B$, but it is significantly more subtle to establish than Going-Up.

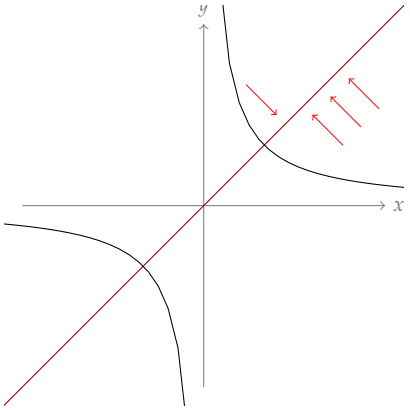
9.34 As indicated we content ourself by formulating the Going–Down theorem.

THEOREM 9.35 *Let $A \subseteq B$ be an extension of interal domains and assume that A is normal. Given two prime ideals $\mathfrak{p}_1 \subseteq \mathfrak{p}_0$ in A and one $\mathfrak{q}_0$ in B luing over $\mathfrak{p}_0$. Then there exists a prime ideal B contained in $\mathfrak{q}_0$ and lying over $\mathfrak{p}_1$.*

PROOF: Not yet here! ❑

9.4 *Noether's normalization lemma*

Once more a lemma that has become a theorem and once more an important result due to Emmy Noether.



The Normalization lemma

The Normalization Lemma is a result about domains that are finitely generated algebras over fields; typical examples being coordinate rings of affine varieties, which are shaped like $k[x_1, \ldots, x_r]/\mathfrak{a}$. It states that such a domain A can be realized as a finite module over a polynomial ring. That is, one may find elements $w_1, \ldots, w_n$ in A such that $k[w_1, \ldots, w_n]$ is isomorphic to a polynomials ring (the w_i's corresponding to the variables) and such that A a finite module over $k[w_1, \ldots, w_n]$.

The w_i's will be algebraically independent, and since A is a finite module over $k[w_1, \ldots, w_n]$, they form a transcendence basis for the fraction field K of A. So the number n will be the transcendence degree $\operatorname{trdeg}_k K$.

The standard proof, which is close to Noether's original and is the one we offer, works over any infinite field, but a slightly less translucent proof, due to Nagata, works over finite field as well.

9.36 Starting out with $k \subseteq A$ and adjoining elements, one will sooner or later exhaust the entire ring A since A is finitely generated over k. In the beginning one may add new elements which are algebraically independent of those already added, but at a certain point, when the maximal number of algebraically independent elements is reached, new elements are forced to be algebraically dependent on the previous. If a new element is *integrally dependent* on the old, we are happy, if not, we have to go back and perturb the already added elements to make the new-comer integral.

EXAMPLE 9.5 A non-integral new-comer will typically have a pole, and to illustrate the perturbation process, we consider the simplest way of adding

a function with a pole, namely the extension $k[x, 1/x]$ of $k[x]$. The geometric counterpart is the projection of the classical hyperbola, $xy = 1$ onto the x-axis, the hyperbola just being the graph of the function $1/x$.

The ring $k[x, 1/x]$ is not finite over $k[x]$, but perturbing x slightly, we obtain a subring over which $k[x, 1/x]$ is finite. The subring $k[x + 1/x]$ will do the job; indeed, $k[x, 1/x] = k[x, x + 1/x]$ is generated by x over $k[x + 1/x]$ and one has the integral dependence relation

$$x^2 - x(x + 1/x) + 1 = 0.$$

It is remarkable that almost *any* perturbation of x will work; that is, $k[x, 1/x]$ is finite over $k[ax + b/x]$ as long as both the scalars a and b are non-zero. ☆

PROBLEM 9.6 Show that $k[x, 1/x]$ is a finite module over $k[ax + b/x]$ for any scalars a b both being different from zero. ★

9.37 The proof of Noether's Normalization Lemma goes by induction of the number of generators A requires as an algebra over k, and the basic ingredient in the induction step is the following lemma:

LEMMA 9.38 *Let k be an infinite field and let $A = k[X_1, \ldots, X_m]/\mathfrak{a}$. Assume that A is a domain whose fraction field K has transcendence degree at most $m - 1$ over k. Then there are elements $y_1, \ldots, y_{m-1}$ in A such that A is a finite module over $k[y_1, \ldots, y_{m-1}]$.*

PROOF: Following our usual convention, we let x_i denote the image of the variable X_i in A. Since the transcendence degree of K over k is less than m, the m elements $x_1, \ldots, x_m$ can not be algebraically independent and must satisfy and equation

$$p(x_1, \ldots, x_m) = 0,$$

where p is a non-zero polynomial with coefficients in k. Let d be the degree of p and let p_d be the homogenous component of degree d. Now, perturbe the x_i's by putting $y_i = x_i - \alpha_i x_m$ for $i \leqslant m - 1$ where the α_i's are scalars to be chosen. This gives[3]

$$\begin{aligned} 0 = p(x_1, \ldots, x_m) = p(y_1 + \alpha_1 x_m, \ldots, y_{m-1} + \alpha_{m-1} x_m, x_m) = \\ = p_d(\alpha_1 x_m, \alpha_2 x_m, \ldots, \alpha_{m-1} x_{m-1}, x_m) + q(x_m, y_1, \ldots, \ldots, y_{m-1}) = \\ = p_d(\alpha_1, \ldots, \alpha_{m-1}, 1) x_m^d + q(x_m, y_1, \ldots, \ldots, y_{m-1}) \end{aligned}$$

where q is a polynomial of degree less that d in the last variable x_m. Now, since the ground field is infinite, for a generic choice of the scalars α_i it holds true that $p_d(\alpha_1, \ldots, \alpha_{m-1}, 1) \neq 0$ (see Exercise 9.9 below). Hence the element x_m is integral over $k[y_1, \ldots, y_{m-1}]$ and by consequence, A is a finite module over the algebra $k[y_1, \ldots, y_{m-1}]$. ❑

[3] Recall that for any polynomial $p(x)$ it holds true that $p(x + y) = p(x) + yq(x, y)$ where q is a polynomial of total degree less than the degree of p. Apply this to p_d.

9.39 By induction on m one obtains the full version of the normalization lemma:

THEOREM 9.40 (NOETHER'S NORMALIZATION LEMMA) *Let k be an infinite field and let $A = k[X_1, \ldots, X_m]/\mathfrak{a}$. Assume that A is a domain whose fraction field K has transcendence degree n over k. Then there are algebraically independent elements $w_1, \ldots, w_n$ in A such that A is a finite module over $k[w_1, \ldots, w_n]$.*

THEOREM 9.41 (NOETHER'S NORMALIZATION LEMMA) *Let k be an infinite field and let $A = k[X_1, \ldots, X_m]/\mathfrak{a}$. Assume that A is a domain whose fraction field K has transcendence degree n over k. Then there are algebraically independent elements $w_1, \ldots, w_n$ in A such that A is a finite module over $k[w_1, \ldots, w_n]$.*

PROOF: We fix the transcendence degree n and proceed by induction on m. If $m \leqslant n$, the elements $x_1, \ldots, x_m$ must be algebraically independent since they generate the field K over k. But any non-zero polynomial in $\mathfrak{a}$ would give a dependence relation between them, so we infer that $\mathfrak{a} = 0$, and hence that $A = k[X_1, \ldots, X_m]$.

Suppose then that $m > n$. By Lemma 9.38 above, there are elements $y_1, \ldots, y_{m-1}$ such that A is finite over $k[y_1, \ldots, y_{m-1}]$. Now, K is algebraic over the fraction field of $B = k[y_1, \ldots, y_{m-1}]$ since A is finite over B, and the latter is therefore of transcendence degree n over k. By induction there are algebraically independent elements $w_1, \ldots, w_n$ in B so that B is finite over $k[w_1, \ldots, w_n]$. But then also A is finite over $k[w_1, \ldots, w_n]$, and we are through. ❑

Problems

9.7 Let k be an infinite field and $f(x_1, \ldots, x_m)$ a non-zero polynomial with coefficients from k. Show that $f(a_1, \ldots, a_m) \neq 0$ for infinitely many choices of a_i from k. HINT: Use induction on n and expand f as $f(x_1, \ldots, x_m) = \sum_i g_i(x_1, \ldots, x_{m-i}) x_m^i$.

9.8 Prove the formula in Footnote number 3. HINT: Use the binomiall theorem to check it for the polynomials $(x + y)^\nu$.

9.9 In stead of the linear change of variables $y_i = x_i - \alpha_i x_1$, show that the proof of Lemma 9.38 goes through over any field with the change $y_i = x_i + x_1^{n_i}$ when n_i are chosen sufficiently large.

★

Corollaries

9.5 The Nullstellensatz

Let $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ be an ideal. Remember the the zero locus of $V(\mathfrak{a})$ of $\mathfrak{a}$. It is the set $a = (a_1, \ldots, a_n)$ so that $f(a) = 0$ for all members f of $\mathfrak{a}$. For every subset $S \subseteq k^n$ one may als consider the ideal $I(S)$ consisting of polynomials in $k[X_1, \ldots, X_n]$ that vanish on S. In general there is no reason that $V(I(S))$ should be eqaue to S, but when S *a priori* is known to be an algebraically closed subset one has equality. That is $V(I(V(\mathfrak{a}))) = V(\mathfrak{a})$.

The Nullstellensatz

Hilbert's Nullstellensatz is about the composition of I and V the other way around, namely about $I(V(\mathfrak{a}))$. Polynomials in the radical $\sqrt{\mathfrak{a}}$ vanish along $V(\mathfrak{a})$ and therefore $\sqrt{\mathfrak{a}} \subseteq I(V(\mathfrak{a}))$, and the Nullstellensatz tells us that this inclusion is an equality. We formulate the Nullstellensatz here, together with two of its weak avatars, but shall come back with a thorough discussion of the proof(s) a little later.

THEOREM 9.42 (HILBERT'S NULLSTELLENSATZ) *Assume that k is an algebraically closed field, and that $\mathfrak{a}$ is an ideal in $k[x_1, \ldots, x_n]$. Then one has $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*

Notice that the ground field must be algebraically closed. Without this assumption the result is not true. The simplest example of an ideal in a polynomial ring with empty zero locus is the ideal $(x^2 + 1)$ in $\mathbb{R}[x]$.

THEOREM 9.43 (WEAK NULLSTELLENSATZ I) *Let A be a finitely generated algebra over the field k and let $\mathfrak{m}$ be a maximal ideal in A. Then $A/\mathfrak{m}$ is a finite field extension of k.*

PROOF: The field $K = A/\mathfrak{m}$ is finitely generated as an k-algebra since A is. If it not algebraic, it has transcendence degree at least one oveer k and by Noether's Normalization Lemma it is a finite module over a polynomial ring $k[w_1, \ldots, w_r]$. By Lemma 9.25 it ensues that $k[w_1, \ldots, w_n]$ is field which is a contradiction since polynomial ring are not fields (if w is a variable $1/w$ is certainly not a polynomial). Hence K is finite over the ground field k. ❑

THEOREM 9.44 (WEAK NULLSTELLENSATZ II) *Let k be an algebraically closed and $\mathfrak{m}$ a maximal ideal in the polynomial ring $k[x_1, \ldots, x_n]$. Then $\mathfrak{m}$ is of the form $\mathfrak{a} = (x_1 - a_1, \ldots, x_n - a_n)$.*

PROOF: By version I, the field $k[x_1, \ldots, x_r]/\mathfrak{m}$ is algebraic over k hence equa to since k is assumed to algebraically closed. The ensuing homomorphism $k[x_1, \ldots, x_n] \to k$ has $x_i - a_i$ in its kernel $\mathfrak{m}$, and since we already know that

$(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal it must be equal to $\mathfrak{m}$, and we are through. ❑

The Rabinowitsch trick

9.45 We proceed to present the J.L. Rabinowitsch trick proving that the weak version of the Nullstellensatz (Theorem **??** on page ??) implies the strong. That is, we need to demonstrate that $I(Z(\mathfrak{a})) \subseteq \sqrt{\mathfrak{a}}$ for any proper ideal $\mathfrak{a}$ in $k[x_1, \ldots, x_n]$.

The crux of the trick is to introduce a new auxiliary variable x_{n+1} and for each $g \in I(Z(\mathfrak{a}))$ to consider the ideal $\mathfrak{b}$ in the polynomial ring $k[x_1, \ldots, x_{n+1}]$ given by

$$\mathfrak{b} = \mathfrak{a} \cdot k[x_1, \ldots, x_{n+1}] + (1 - x_{n+1} \cdot g).$$

In geometric terms $Z(\mathfrak{b}) \subseteq \mathbb{A}^{n+1}$ is the intersection of the the subset $Z = Z(1 - x_{n+1} \cdot g)$ and the inverse image $\pi^{-1}Z(\mathfrak{a})$ of $Z(\mathfrak{a})$ under the projection $\pi\colon \mathbb{A}^{n+1} \to \mathbb{A}^n$ that forgets the last and auxiliary coordinate. This intersection is empty, since obviously g does not vanish along Z, but vanishes identically on $\pi^{-1}Z(\mathfrak{a})$.

The weak Nullstellensatz therefore gives that $1 \in \mathfrak{b}$, and hence there are polynomials f_i in $\mathfrak{a}$ and h_i and h in $k[x_1, \ldots, x_{n+1}]$ satisfying a relation like

$$1 = \sum f_i(x_1, \ldots, x_n) h_i(x_1, \ldots, x_{n+1}) + h \cdot (1 - x_{n+1} \cdot g).$$

We substitute $x_{n+1} = 1/g$ and multiply through by a sufficiently[4] high power g^N of g to obtain

$$g^N = \sum f(x_1, \ldots, x_n) H_i(x_1, \ldots, x_n),$$

where $H_i(x_1, \ldots, x_n) = g^N \cdot h_i(x_1, \ldots, x_n, g^{-1})$. Hence $g \in \sqrt{\mathfrak{a}}$.

[4] For instance the highest power of x_{n+1} that occurs in any of the h_i's.

9.6 *Appendix—skirmishes*

We have relegated a few simple results of preparatory character to this appendix. They do not take part in the main battle, but are merely skirmishes on the flanks, though of significant importance for the progress. At least the two firsts are easy and elementary. The concept of transcendence degree might be a little more involved, but should be known to mosts students from earlier courses.

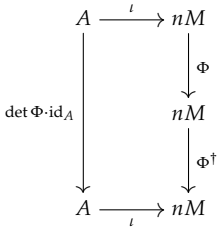
The determinantal trick

The determinantal trick (so named by Miles Reid), is a little lemma from linear algebra adapted to modules. It is just a reformulation of the arch-classical fact

that a square matrix with a non-trivial kernel has a vanishing determinant—which is the *raison d'être* for determinants and the reason for their name.

We start by recalling that the good old matrix multiplication may be extended to modules. Indeed, if $\Phi = (f_{ij})$ is an $n \times n$-matrix with entries from a ring A and $m = (m_1, \dots, m_n)$ a string of elements from an A-module M, the expression $\Phi \cdot m$ is meaningful. It is the string of elements from M given as $(\sum f_{ij} m_j)_{1 \leqslant i \leqslant n}$; or expressed in a fancy functorial fashion, the map $m \mapsto \Phi \cdot m$ is just the map $\mathrm{id}_M \otimes \Phi \colon M \otimes_A nA \to M \otimes_A nA$.

LEMMA 9.46 (THE DETERMINENTAL TRICK) *Let Φ be an $n \times n$-matrix with entries in the ring A, and let M be an A-module. Assume that M has generators $m_1, \dots, m_n$ such that $\Phi \cdot (m_1, \dots, m_n) = 0$. Then the determinant $\det \Phi$ kills M.*



PROOF: Consider the A-linear map $\iota \colon A \to nM$ sending x to $(x \cdot m_1, \dots, x \cdot m_n)$. Then the hypothesis of the lemma translates into the relation $\Phi \circ \iota = 0$. Citing the adjunction formula from linear that states $\Phi^\dagger \cdot \Phi = \det \Phi \cdot I$, we find

$$\det \phi \cdot \iota = \Phi^\dagger \circ \Phi \circ \iota = 0.$$

This means that $(\det \Phi \cdot m_1, \dots, \det \Phi \cdot m_n) = \det \Phi \cdot \iota(1) = 0$; hence $\det \Phi$ kills M as the m_i's generate M. ❑

Finite generation in towers

The next preparation is an utterly simple lemma which we give for the benefit of the students: Two successive finite ring extension gives a finite extension having generators the products of the generators of the two.

LEMMA 9.47 *Let $A \subseteq B \subseteq C$ be a tower of rings and assume that C i finite over B and B is finite over A, then C is a finite over A.*

PROOF: Let $x_1, \dots, x_r$ be a generating set for B as an A-module and $y_1, \dots, y_s$ one for C over B. Then the products $x_i y_j$ will generated C over A. This is elementary indeed, if $z = \sum b_j y_j$ with $b_j \in B$, write each coefficient b_j as $b_j = \sum_j a_{ij} x_i$ to obtain

$$z = \textstyle\sum_j b_j y_j = \sum_j (\sum_i a_{ij} x_i) y_j = \sum_{i,j} a_{ij} x_i y_j.$$

❑

Transcendence degree

9.48 Let $k \subseteq K$ be a field extension and let $x \in K$ be an element not lying in k. The elements in K can be parted in to classes, the algebraic elements and the transcendental ones. The algebraic ones are those x that satisfies a relation like

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 \tag{9.7}$$

where the a_i's are elements form k and $a_n \neq 0$[5], and the transcendental ones are the rest; that is, those for which $p(x) \neq 0$ for any non-zero-polynomial in $k[X]$.

[5] Since K is field we may as well assume that $a_n = 1$

More generally a collection $x_1, \ldots, x_r$ of element from the bigger field K is said to be *algebraically dependent* over k if for some non-zero polynomial p in r variables and coefficients from k it holds true that $p(x_1, \ldots, x_r) = 0$, and of course, if no such polynomial can be found, the collection is called *algebraically independent* over k.

Algebraically dependent elements (*algebraisk avhengige elementer*)

A collection of algebraically independent elements $x_1, \ldots, x_r$ is a *transcendence basis* of K over k if it is maximal; that is firstly, it is algebraically independent and secondly, adding any new element to it will make it algebraically dependent. In terms of the field K that $x_1, \ldots, x_r$ is a transcendence basis means that the field K is an algebraic extension of $k(x_1, \ldots, x_r)$, and that $k(x_1, \ldots, x_r)$ is isomorphic to the rational function field over k in r variables..

Algebraically independent elements (*algebraisk uavhengige elementer*)

transcendence basis (*transcendence basis*)

We cite the following result but refrain from giving a proof:

PROPOSITION 9.49 *Every field extension K of k that is not algebraic, has a transcendence basis. All transcendent bases for K over k have the same number elements.*

That common number is called the *transcendence degree* of K over k and denoted by $\mathrm{trdeg}_k(K)$.

Transcendence degree (*transcendensgrad*)

9.50 In linear algebra The Tietze's Extension Lemma is used to show that bases of vector spaces have the same number of elements. An analoguous result will give that different transcendence bases of fiels extension have same cardinality.

LEMMA 9.51 (EXCHANGE EMMA) *Let $k \subseteq L \subseteq K$ be a tower of fields and let a and b be two elements of K. Assume that b is transcendent over L but algebraic over $L(a)$, then a is algebraic over $L(b)$.*

PROOF: Since b is algebraic over $L(a)$, there is a polynomial $f(x, y)$ with coefficients from L such that $f(a, y) \neq 0$ but $f(a, b) = 0$. Expandingh f in powers of x yields

$$0 = f(a, b) = \sum q_i(b) a^i,$$

wehere $q_i(y) \in L[y]$. This looks very much like a dependence relation for a over $L(b)$, it only remains to see that $f(x, b)$ is not identically zero, but since b is trancsendent over L and at least one of the polynomials $q_i(y)$'s is non-zero, this holds true. ❑

PROOF OF TRANCENDENCE BASES: We only treate the case of finite bases. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ be two transcendence bases for K over k. ❑

Lecture 10

Krull dimension

Very preliminary version 0.01 as of 2018-12-03 at 10:01 (typeset 3rd December 2018 at 10:03am)—Prone to misprints and errors and will change.

03/12/2018 Several changes, still unfinished.

Dimension is in general a complicated and subtle notion. In a few good cases it is well defined. Vector spaces have a dimension as do manifolds of course (or at least each connected component has). They are locally isomorphic to open sets in some euclidean space, and the dimension of that euclidean space is constant along connected components, and is the dimension of the component.

There is another and naive approach to the conception of dimension. For example, in three dimensional geometric gadgets, called threefolds, we may imagine increasing chains of subgadgets of length three; points in curves, curves in surfaces and surfaces in the threefold. This may be formalized by using closed and irreducible subsets as "subgadgets", and the dimension will be the maximal of length of chains such, or rather the supremum of the lengths as the lengths might be bounded. This definition works for any topological space, but the ensuing dimension does not carry much information unless the topology is "Zariski-like". Translated into algebra, where prime ideals correspond to closed irreducible subsets, this leads to the consept of Krull dimension of a ring; the supremum of the length of chains of prime ideals.

For varieties there is another good candidate for the dimension, namely the transcendence degree of the fraction field $K(X)$ over the ground field. This may be motivated by the fact the Krull dimension of the polynomial ring $k[x_1, \dots, x_n]$ equals n (which is not obvious at all but follows from the Principal Ideal Theorem), and obviously the transcendence degree of $k(x_1, \dots, x_n)$ is n. That the two coincide, follows from the Normalization lemma which states that every variety is a finite cover of an affine space.

The definiton

10.1 Let A be a ring. The point is to consider strictly ascending and finite chains $\{\mathfrak{p}_i\}$ of prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_\nu.$$

Recall that ν is called *the length* of the chain; it is one less than the number of prime ideals, or if you want, the number of inclusions. The *Krull dimension* of A be the supremum of the length of all such chains in A. It is denoted by $\dim A$. We shall say that a chain is *saturated* if there are no prime ideals of A lying strictly between two of the terms, and it is *maximal* if additionally it neither can be lengthened upwards nor downwards.

Krull dimension (*Krull dimensjon*)

saturated chains (*mettede kjeder*)

Maximal chains (*maksimale kjeder*)

10.2 Even if each chain is finite, there might be arbitrary long chain, and the Krull dimension will in that case be infinite. It is easy to find examples among non-noetherian rings whose Krull dimension is infinite; Example10.1 below is an obvious example of one with an infinite ascending chain. Even Noetherian rings might have infinite Krull dimension. However, these examples live on the fringe of the Noetherian society, and rings met in mainstream algebraic geometry will all have finite dimension. When $\dim A < \infty$, there are saturated chains of maximal length, that is of length $\dim A$. We shall also see that local Noetherian rings have finite Krull dimension.

EXAMPLE 10.1 The polynomial ring in $A = k[x_1, \ldots, x_r, \ldots]$ in infinite many variables is of inifinite Krulll dimension. Each of the ideals $\mathfrak{p}_r = (x_1, \ldots, x_r)$ is a prime ideal, and they form an infinite ascending chain.

There is also an infinite descending chain of prime ideals in A whose members are the ideals $\mathfrak{q}_r = (x_r, x_{r+1}, \ldots)$. ☆

EXAMPLE 10.2 *(Rings of dimension zero)* A ring A is zero-dimensional when there are no chains of prime ideals with two or more terms; or in other words, when all its prime ideals are both minimal and maximal. If A in addition is Noetherian, there are according to the Lasker-Noether Theorem (Teorem 8.17 on page 180) only finitely many minimal prime ideals, and we may characterise Artinian rings as those having finitely many prime ideals all being maximal (Theorem 7.58 on page 172). Hence a Noetherian ring is of dimension zero if and only if it is Artinian. In particular, fields are of dimension zero. ☆

EXAMPLE 10.3 *(Domains of dimension one)* It is worth while contemplate one-dimensional rings as well. In a one-dimensional domain the zero ideal is a prime ideal so the saturated chains are all of the form $(0) \subset \mathfrak{p}$. All non-zero prime ideal are therefore maximal, and they are as well minimal over the zero ideal. Examples are PID's; in particular polynomial rings $k[X]$ in one variable over fields and, of course, the integers $\mathbb{Z}$ will all be one-dimensional.

If A is not a domain, there may as well be saturated chains of length one; in other words, some of the minimal prime ideals might also be maximal (see Example 10.4 below). ☆

10.3 If A has several minimal prime ideals, the space Spec A will have several irreducible components, as in the example above with $(0,1)$ and the x-axis being the components. The dimension of A will we the largest of the dimensions of the components, or if there are infinitely many, the supremum. In algebraic terms this translates as:

PROPOSITION 10.4 *If $\{\mathfrak{p}_i\}$ are the minimal primes of A, then* $\dim A = \sup_i \dim A/\mathfrak{p}_i$.

PROOF: The intersection of the prime ideals of a chain being prime, any maximal chain starts at minimal prime (see also Paragraph 2.61 on page 43 and Exercise 2.23 on page 43). ❑

10.5 It is common usage to call $\dim A_\mathfrak{p}$ the *the height* of $\mathfrak{p}$, or more generally for any ideal $\mathfrak{a}$ in A the heigh is the least height of any prime ideal containing $\mathfrak{a}$; that is

Height of ideals (høyden til idealer)

$$\operatorname{ht}\mathfrak{a} = \min_{\mathfrak{a}\subseteq\mathfrak{p}} \operatorname{ht}\mathfrak{p}.$$

A useful inequality

10.6 Any chain $\{\mathfrak{p}_i\}_i$ of prime ideals in A may be broken in two at any stage, say at term $\mathfrak{p} = \mathfrak{p}_\nu$. It is the concatenation of a lower chain, formed by the members of the chain contained in $\mathfrak{p}$, and an upper chain, the one formed by those containing $\mathfrak{p}$. And of course, one may as well splice two chains provided one ends at the prime where the other one begins.

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_{\nu-1} \subset \mathfrak{p}_\nu \subset \mathfrak{p}_{\nu+1} \subset \ldots \subset \mathfrak{p}_n$$

Now, the primes contained in $\mathfrak{p}$ are in a one-to-one correspondence with the prime ideals in $A_\mathfrak{p}$, hence the lower chains correspond to chains in the localization $A_\mathfrak{p}$. This means that $\dim A_\mathfrak{p}$.

In similar way, prime ideals containing $\mathfrak{p}$ correspond to prime ideals in the quotient $A/\mathfrak{p}$ and hence the upper chains correspond to chains in $A/\mathfrak{p}$. When considering the suprema of the lengths of such splices, we arrive at the following formula:

PROPOSITION 10.7 *Let A be a ring and $\mathfrak{p}$ a prime ideal. Then*

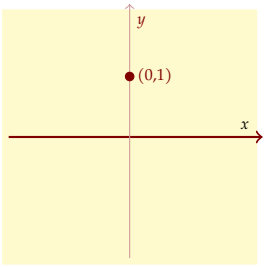
$$\dim A_\mathfrak{p} + \dim A/\mathfrak{p} \leqslant \dim A.$$

Notice that the proposition is still valid if one or more of the dimensions are infinite, with the usual intepretation that $n + \infty$ equals ∞.

In some rings there are maximal chains—that is, saturated chains which cannot be lengthened—of different lengths, and the Krull dimension is of course the length of the longest. For any prime ideal in a shorter chain, the inequality as in the proposition will be strict. It is easy to give such examples when the ring A is not a domain, one simply takes an A with components

of different dimension (see Example 10.4) below). However, there are also examples when A is a Noetherian domain, but these are again rather exotic constructs you don't tumble over in algebraic geometry.

EXAMPLE 10.4 Let $A = k[X,Y]/\mathfrak{a}$ where $\mathfrak{a} = (XY, Y(Y-1))$, and as usual, we let lower case letters denote the classes of their upper case versions. Geometrically $V(\mathfrak{a})$ is the subset of k^2 being the union of X-axis and the point $(0,1)$. The primary decomposition of (0) in A is $(0) = (y) \cap (x, y-1)$. Hence (y) and $(x, y-1)$ are the minimal prime ideals in A. Now, $(x-a, y)$ is a maximal ideal for any $a \in k$, so A possesses saturated chains



$$(y) \subset (x-a),$$

and therefore $\dim A = 1$. On other hand $(x, y-1)$ is clearly a maximal ideal, and hence is both maximal and minimal. ☆

EXAMPLE 10.5 If you want an example that is a local ring consider the ideal $\mathfrak{a} = (Z) \cap (X,Y) = (ZX, ZY)$ in $k[X,Y,Z]$ and let A be the localization at (x,y,z) of the quotient $k[X,Y,Z]/\mathfrak{a}$. Then $(0) = (z) \cap (x,y)$ is the primary decomposition of (0) and (z) and (y,x) are minimal prime ideals in A; but there maximal chains $(z) \subset (x,z) \subset (x,y,z)$ and $(x,y) \subset (x,y,z)$ in A. ☆

Going–Up again

A most useful consequence of the Going–Up Theorem is that any chain in an integral extension B of a ring A, when intersected with A becomes a chain in A; this ensures that the dimension is preserved in integral extensions. We have

PROPOSITION 10.8 *Let $A \subseteq B$ be an integral extension of domains. Then* $\dim A = \dim B$.

PROOF: This is a direct consequence of the Going-Up theorem as formulated in Going–Up II*. Indeed, let $\{\mathfrak{q}\}_i$ be a chain of length d in B and consider the prime ideals $\mathfrak{p}_i = \mathfrak{q}_i \cap A$. They form a chain in A whose length is d since no two $\mathfrak{q}_i$'s intersect A in the same ideal according to Lying–Over*. This shows that $\dim B \leqslant \dim A$. On the other hand by Going–Up II, every chain in A has a chain in B lyinig over it which means that $\dim B \leqslant \dim A$. ❑

*Corollary 9.31 on page 203

*Proposition 9.28 on page 201

10.9 For example if $\mathbb{Q} \subseteq K$ is any field extension (finite or not) the ring of integers in K, that is the integral closure A of $\mathbb{Z}$ in K, is of course integral over $\mathbb{Z}$ and consequently is of dimension one. In particular this applies to the quadratic extensions $K = \mathbb{Q}(\sqrt{d})$ we have seen, but also to the more impressive extension $K = \bar{\mathbb{Q}}$, the field of algebraic numbers. The ring of algebraic integers $\bar{\mathbb{Z}}$ is therefore of dimension one, but recall, it is not a Noetherian ring.

Cutting out a hypersurface

Cutting a varity X with a hypersurface is a rather common technique in geometry, which on the level of algebras corresponds to passing to a quotient $A/(f)A$ of A by a principal ideal. One suspects the dimension to go down, but it might happen that the hypersurface contains one of the components of X, and in that case the dimension might stay the same (if the component is one of maximal dimension). To avoid such an accidental behaviour, one must assumes that f does not lie in any of the minimal prime ideals of A; then one has:

PROPOSITION 10.10 *Let A be ring of finite Krull dimension and let $f \in A$ is an element not belonging to any minimal prime ideal in A, then* $\dim A/(f)A < \dim A$.

PROOF: Chains of prime ideals in $A/(f)A$ are in one-to-one correspondence with chains in A containing f. Moreover, a prime ideal $\mathfrak{p}$ that is minimal over (f), properly contains a minimal prime $\mathfrak{q}$ of A, and consequently any chain in A starting upwards from $\mathfrak{p}$ can be lengthened downwards by joining $\mathfrak{q}$ to it. ❑

The dimension of polynomial rings

There is an obvious chain of prime ideals in the polynomial ring $k[x_1, \ldots, x_n]$ over a field k corresponding to a chain of linear subspaces in k^n with the dimension jumping by one between two consecutive. The terms of the ideal chain are the ideals generated by the variables, and the length is n:

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, \ldots, x_n). \tag{10.1}$$

This shows that the Krull dimension of $k[x_1, \ldots, x_n]$ is at least n. To see it equals n, is a subtler matter which asks for some bigger artillery; it hinges on the Normalization Lemma*.

*Th. 9.40 on page 205

PROPOSITION 10.11 (DIMESION OF POLYNOMIAL RING) *Let k be a field and let $k[x_1, \ldots, x_n]$ be the ring of polynomials in the variables $x_1, \ldots, x_n$. Then one has* $\dim k[x_1, \ldots, x_n] = n$.

PROOF: Assume that

$$(0) \subset \mathfrak{p}_1 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_d \tag{10.2}$$

is a chain with $\mathfrak{p}_1$ minimal over (0). Pick a non-zero irreducible element f in $\mathfrak{p}_1$; then (f) is a prime ideal and $(f) = \mathfrak{p}_1$. Consider the quotient algebra $A = k[x_1, \ldots, x_n]/(f)$. It is a domain, and since we have imposed a non-trival condition on the variables, its fraction field is of transcendence degree at most $n - 1$. By Noether's Normalization Lemma it follows that A is finite over a polynomial ring in at most $n - 1$ variables, and hence by the Going–Up Theorem the dimension of A is at most $n - 1$ as well.

Now, the chain (10.2) induces a chain in A shaped like

$$(0) \subset \mathfrak{p}_2/\mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_d/\mathfrak{p}_1,$$

and it follows that $n-1 \geqslant \dim A \geqslant d-1$, and consequently it holds true that $\dim k[x_1,\ldots,x_n] \leqslant n$. ❑

COROLLARY 10.12 *Let A be a domain finitely generated over the field k whose field of fractions is K. Then* $\dim A = \operatorname{trdeg}_k K$

PROOF: Let $n = \operatorname{trdeg}_k K$. By Noteher's Normalization Lemma* there is a polynomial ring $k[x_1,\ldots,x_n] \subseteq A$ over which A is finite, hence $\dim A = \dim k[x_1,\ldots,x_n] = n$. ❑

* 9.40 on page 205

10.1 Krull's Principal Ideal Theorem

This important theorem is also known under its German name Krull's Hauptidealsatz. It lies at the bottom of the dimension theory in commutative algebra and algebraic geometry, and in his book[1] Irving Kaplansky refers to it as "may be the most important single theorem in the theory of Noetherian rings". There is however a rather simple underlying intuition that the dimension of a solution space goes down by at most one when an additional equation is introduced. We recongnize this from theory of linear equations, but the principle has a much wider scope (as shows *e.g.* the Hauptidealsatz).

[1]

10.13 The scene is a ring A with the two main players, a prime ideal $\mathfrak{p}$ and an element x over which $\mathfrak{p}$ is minimal; in other words, there is no prime ideal properly lying between (x) and $\mathfrak{p}$. And the conclusion is that $\operatorname{ht}\mathfrak{p}$ is at most one. Of course, the prime ideal $\mathfrak{p}$ might be a minimal one and then the height would be equal to zero, but if A is a domain and x is non-zero, the height will be one.

THEOREM 10.14 (KRULL'S PRINICIPAL IDEAL THEOREM) *Let A be a Noetherian ring and x an element from A. Assume that $\mathfrak{p}$ is a prime ideal in A which is minimal over (x). Then* $\operatorname{ht}\mathfrak{p} \leqslant 1$.

PROOF: We are to show that there are no chain of prime ideals of length two as $\mathfrak{q}' \subset \mathfrak{q} \subset \mathfrak{p}$. By passing to the quotient $A/\mathfrak{q}'$ and subsequently localizing in $\mathfrak{q}/\mathfrak{q}'$, we may assume that A is a local domain with maximal ideal $\mathfrak{p}$, and we our task is to prove that if $\mathfrak{q} \subset \mathfrak{p}$, then $\mathfrak{q} = 0$.

$$\begin{array}{ccc} (x) & \subseteq & \mathfrak{p} \\ & & \cup \\ & & \mathfrak{q} \\ & & \cup \\ & & \mathfrak{q}' \end{array}$$

The first observation is that, since $\mathfrak{p}$ is minimal over (x), the ring A/xA has only one prime ideal and being Noetherian, it is Artinian, and we shall have the opportunity to activate the descending chain condition. The chain we shall exploit, is the descending chain $\{(x)+\mathfrak{q}^{(n)}\}_n$, where $\mathfrak{q}^{(n)}$ is the n-th symbolic[2] power of $\mathfrak{q}$, that is, $\mathfrak{q}^{(n)} = A \cap \mathfrak{q}^n A_{\mathfrak{q}}$. The chain $\{(x)+\mathfrak{q}^{(n)}\}$ corresponds to the

[2] Don't panic! We would rather have used the powers $\mathfrak{q}^n$. But powers of prime ideals can be unruly, and at a later point in the proof they will not serve our purpose.

descending chain $\{\big((x)+\mathfrak{q}^{(n)}\big)/(x)\}$ in A/xA and must eventually be stable, as A/xA is Artinian. Hence there is an n so that

$$(x)+\mathfrak{q}^{(n+1)} = (x)+\mathfrak{q}^{(n)}.$$

This entails that if $a \in \mathfrak{q}^{(n)}$, one may write $a = b + cx$ with $b \in \mathfrak{q}^{(n+1)}$, so that $cx \in \mathfrak{q}^{(n)}$. This entails[3] that $c \in \mathfrak{q}^{(n)}$, and consequently that $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n)}$ Nakayama's lemma yields that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$; this gives $\mathfrak{q}^n A_\mathfrak{q} = \mathfrak{q}^{n+1} A_\mathfrak{q}$, and appealing once more to Nakayama's lemma, we may conclude that $\mathfrak{q}A_\mathfrak{q} = 0$; that is, $\mathfrak{q} = 0$. ❑

[3] This is where we use the symbolic power; since $x \notin \mathfrak{q}$, it is invertible in $A_\mathfrak{q}$, and $c \in A \cap \mathfrak{q}^n A_\mathfrak{q}$

The general version of The Principal Ideal Theorem

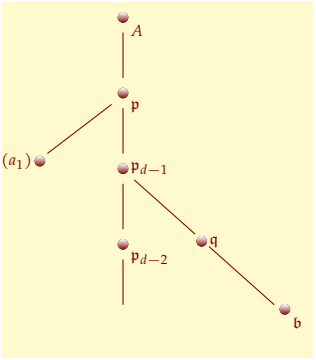
This result, ofen called "The height theorem", is the natural generalisation of the Principal Ideal theorem which applies to minimal primes over ideals with more than one generator. The natural guess that the height is at most the number of generators is actually true, and in agreement with the naive intuition that imposing r constraints on a system should at most lower the dimension of the solution space by r, reasoning that it diminishes at most with one for each new condition imposed. This points to an induction argument, but one which will be slightly more subtle than the naive intuitive version.

THEOREM 10.15 (THE HEIGHT THEOREM) *Let A be a Noetherian ring and let $\mathfrak{p}$ be a prime ideal minial over an ideal $\mathfrak{a}$ generated by r elements. Then* $\operatorname{ht}\mathfrak{p} \leqslant r$.

PROOF: Let $\mathfrak{a} = (a_1, \dots, a_r)$. As indicated above the proof goes by inductuion on r, and heading for a contradiction, we assume that there is a chain $\{\mathfrak{p}_i\}$ in A of length $d > r$ ending at $\mathfrak{p}$. We may assume that a_1 is not in $\mathfrak{p}_{d-1}$, and so there is no prime lying properly bewteen $(a_1)+\mathfrak{p}_{d-1}$ and $\mathfrak{p}$. The radical of $(a_1)+\mathfrak{p}_{d-1}$ therefore equals $\mathfrak{p}$, and a power of $\mathfrak{p}$ is contained in $(a_1)+\mathfrak{p}_1$. Write

$$a_i^t = c_i a_1 + b_i$$

with $b_i \in \mathfrak{p}_{d-1}$, and let $\mathfrak{b} = (b_2, \dots, b_r)$. Then $\mathfrak{b}$ is contained in $\mathfrak{p}_{d-1}$. We contend that there is prime ideal $\mathfrak{q}$ lying between $\mathfrak{b}$ and $\mathfrak{p}_{d-1}$, properly contained in $\mathfrak{p}_{d-1}$; indeed, if $\mathfrak{p}_{d-1}$ were minimal over $\mathfrak{b}$, the height of $\mathfrak{p}_{d-1}$ would be at most $r-1$ by induction, but being next to the top in a chain of length d, the ideal $\mathfrak{p}_{d-1}$ is of height at least $d-1$, and $r-1 < d-1$.



Now, the idea is to pass to the ring $A/\mathfrak{q}$. The ideal $\mathfrak{q}+(a_1)$ contains a power of $\mathfrak{a}$, hence there is no prime ideal between $\mathfrak{q}+(a_1)$ and $\mathfrak{p}$, which means that the $\mathfrak{p}/\mathfrak{q}$ is minimal over the principal ideal $\mathfrak{q}+(a_1)/\mathfrak{q}$, and therefore of height one after the Principal Ideal Theorem, but there is also the chain $0 \subset \mathfrak{p}_{d-1}/\mathfrak{q} \subset \mathfrak{p}/\mathfrak{q}$. Contradiction. ❑

10.16 It ensues from the Height Theorem that any local Noetherian ring A has a finite Krull dimension. Indeed, the maximal ideal $\mathfrak{m}$ is finitely generated,

and by the Height Theorem the height of $\mathfrak{m}$, which is the same as $\dim A$, is bounded by the number of generators. Similarily, Noetherian rings enjoy a descending chain condition for the prime ideals. Any term in a chain is finitely generated and hence is of finite height.

PROPOSITION 10.17 *A local Noetherian ring is of finite Krull dimension. Noetherian rings satisfy the* DDC *for prime ideals.*

10.18 Among the different numbers associated with a ring having some flavour of a dimension, is the so-called *embedding dimension* of a local ring A. If $\mathfrak{m}$ denotes maximal ideal of A, embedding dimension of A is defined as the vector space dimension $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ (the module $\mathfrak{m}/\mathfrak{m}^2$ is killed by $\mathfrak{m}$ and therefore is a vector space over $A/\mathfrak{m}$). Any vector space basis of $\mathfrak{m}/\mathfrak{m}^2$ is of the form $[x_1], \ldots, [x_r]$ for members x_i of $\mathfrak{m}$. Nakayama's lemma implies that the x_i's generate $\mathfrak{m}$, and in its turn The Height Theorem yields that $\dim A \leqslant r$. We have thus proved

Embedding dimension (*embeddingsdimensjon*)

PROPOSITION 10.19 *Assume that A is a Noetherian ring with maximal ideal $\mathfrak{m}$. Then $\dim A \leqslant \dim \mathfrak{m}/\mathfrak{m}^2$.*

UFD*'s once more*

In Lecture 3 we showed a criterion of Kaplansky's (Proposition 3.11 on page 61) which tells us that a domain A is a UDF if and only if "every prime contains a prime". When A is a Noetherian domain, this criterion can be improved. Citing Proposition 10.17 above which asserts that prime ideals in a Noetherian ring satisfy the descending chain condition, we infer that any prime ideal in A contains a prime ideal of height one (if this is not true, one easily constructs a descending chain that does not terminate). To ensure that A is a UFD it therefore suffices that prime ideals of height one contain prime elements, but of course in that case, since prime elements generate prime ideals, the height one ideal is itself generted by the prime element. This leads to

THEOREM 10.20 *A Noetherian domain A is a* UFD *if and only if every prime ideal of height one is principal.*

10.2 *System of parameters*

10.21 Let A be a local ring with maximal ideal $\mathfrak{m}$ whose Krull dimension is n. A sequence $x_1, \ldots, x_n$ of n elements in A is called a *system of parameters* if the ideal $\mathfrak{a}$ they generate is $\mathfrak{m}$-primary. Since $\mathfrak{m}$ is maximal, this amount to the radical being equal to $\mathfrak{m}$ (Proposition 8.4 on page 175), or if A is Noetherian that $\mathfrak{a}$ contains some power of $\mathfrak{m}$.

System of parameters (*parmetersystemer*)

PROPOSITION 10.22 *Every local Noetherian ring has a system of parameters.*

PROOF: Let A be the ring, let $\mathfrak{m}$ the maximal ideal, and let $n = \dim A$. We shall, by a recursive construction, exhibit a sequence $x_1, \dots, x_n$ of elements in $\mathfrak{m}$ so that the ideal $\mathfrak{a}_i = (x_1, \dots, x_i)$ generated by the i first has all its minimal primes of height i. Assume that $\mathfrak{a}_\nu$ has been constructed and consider the prime ideals $\{\mathfrak{p}_j\}$ minimal over $\mathfrak{a}_\nu$. They all have height ν so if $\nu < n$, none of them equals $\mathfrak{m}$. Hence their union is not equal to $\mathfrak{m}$ by Prime Avoidance (Lemma 2.28 on page 33), and we may pick an element $x_{\nu+1}$ from A so that $x_{\nu+1} \in \mathfrak{m}$, but $x_{\nu+1} \notin \bigcup_i \mathfrak{p}_i$. Then any prime ideal minimal over $\mathfrak{a}_{\nu+1} = (x_1, \dots, x_{\nu+1})$ has height $\nu + 1$; indeed, let $\mathfrak{p}$ be one of them. It is not among the minimal prime ideals $\mathfrak{p}_i$ of $\mathfrak{a}_\nu$, and therefore must contain one of $\mathfrak{p}_i$'s properly, say $\mathfrak{p}_j$, and we infer that $\operatorname{ht}\mathfrak{p} > \operatorname{ht}\mathfrak{p}_j = \nu$. The other inequality; that is $\operatorname{ht}\mathfrak{p} \leqslant \nu + 1$, ensues from the Height Theorem. ❑

10.23 The geometric counterpart of a system of parameters is, given a variety X and point P on X, a sequence of hypersurfaces that intersect the given variety in just the point P, or more precisely since we talk about a local concept, intersect a neighbourhood of P just in P.

10.24 One cannot in general hope that the maximal ideal itself is generated by $\dim A$ elements. The plane cusp $A = k[X, Y]/(Y^2 - X^3)$ gives a simple example. The maximal ideal $\mathfrak{m} = (x, y)$ requires both x and y as generators since no linear combination $\alpha X + \beta Y$ with $\alpha, \beta \in k$ for degree reasons can lie in $(Y^2 - X^3)$, and therefore x and y are linearly independent modulo $\mathfrak{m}^2 = (x^2, xy, y^2)$.

The corresponding geometric situation is like this. Both the x-axis and the y-axis intersect the curve $C = V(Y^2 - X^3)$ only at the origin, but because C has a double point there, there will always be an intersection multiplicity; indeed, any line through the origin intersects C only at the origin, but with a multiplicity.

Noetherian local rings whose maximal ideal needs no more generators than the Krull dimension are said to *regular*. A general Noetherian ring is regular if the local rings $A_\mathfrak{p}$ are regular for all prime ideals $\mathfrak{p}$ in A.

Regular local rings
(regulære lokale ringer)

PROBLEM 10.1 With notations as above, show that $\ell_{A_\mathfrak{p}}(A_\mathfrak{p}/(X - \alpha Y)A_\mathfrak{p}) = 2$ when α is a scalar and that $\ell_{A_\mathfrak{p}}(A_\mathfrak{p}/(Y)A_\mathfrak{p}) = 3$. The excess length in the latter case is explain by the x-axis, that is the line $Y = 0$, being tangent C at the origin in some sense. Show that $\ell_A(A/(\beta X - \alpha Y)) = 3$ for all linear forms $\beta X - \alpha Y$. ★

Dimension and fibres

10.25 From linear algebra we know that for a given linear map $\phi\colon V \to W$ one has the formula

$$\dim \operatorname{im}\phi + \dim \ker \phi = \dim V + \dim W,$$

or using that $\dim \operatorname{im} \phi \leqslant \dim V$, it yields the inequality $\dim V \leqslant \dim + \dim \phi^{-1}(0)$. For a smooth map $\phi\colon X \to Y$ between manifolds there is a similar inequality

$$\dim Y \leqslant \dim X + \dim \phi^{-1}(y),$$

for $y \in \phi(X)$, which in fact is just the inequality from linear algebra applied to the derivative of ϕ. If now, $\phi\colon X \to Y$ is a map of varieties, or between spectra of rings, there is a similar formula, however we confine ourselves to an algebraic version valid for maps of local rings.

10.26 Recall that *map of local rings* is map of rings between two local rings which sends the maximal ideal into the maximal ideal.

Maps of local rings (lokale ringavbildning)

PROPOSITION 10.27 *Let A and B be the two local rings having maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$ respectively, and assume that $\phi\colon A \to B$ is a map of local rings. Then it holds true that*

$$\dim B \leqslant \dim A + \dim B/\mathfrak{m}B.$$

PROOF: We begin with choosing two systems of parameters. One is a system of parameters $x_1, \ldots, x_r$ for the maximal ideal $\mathfrak{m}$, and the other is one for the ideal $\mathfrak{n}/\mathfrak{m}B$ in the ring $B/\mathfrak{m}B$, and let $y_1, \ldots, y_s$ be liftings to B of the members of the latter. We contend that the ideal $\mathfrak{a} = (\phi(x_1), \ldots, \phi(x_r), y_1, \ldots, y_s)$ the two systems generate in B is $\mathfrak{n}$-primary; indeed, some power $\mathfrak{n}^\nu$ is contained in $(y_1, \ldots, y_s) + \phi(\mathfrak{m})$, and consequently some higher power lies in $\mathfrak{a}$ since high powers of $\mathfrak{m}$ lie in $(x_1, \ldots, x_r)$. ❑

EXAMPLE 10.6 *(Strict inequality may occur)* Consider the map $\psi\colon \mathbb{C}^2 \to \mathbb{C}^2$ sending a point (u, v) to (u, uv). The fibre over $(0, 0)$ is the entire line $u = 0$, and thus of dimension strictly larger than the difference between the dimensions of the source and the target.

Transcribing this into local algebra we consider the map of rings $\phi\colon k[u, v] \to k[x, y]$ that sends $u \mapsto x$ and $v \mapsto xy$. The appropriates localizations are $A = k[u, v]_{(u,v)}$ with $\mathfrak{m} = (u, v)A$ and $B = k[x, y]_{(x,y)}$ with $\mathfrak{n} = (x, y)B$. Then $\mathfrak{m}B = (x, xy)$ and the "fibre" $B/(x, y)B = (k[x, y]/(x, xy))_{(x,y)} = k[y]_{(y)}$ is of dimension one, whereas of course, $\dim B - \dim A = 0$. ☆

10.28

10.29 As an example connecting up with the geometric situation, assume that $A \to B$ is a mp of rings, not necessarily local, and that $\mathfrak{m}$ is a maximal ideal in A. Furthermore, assume that $\mathfrak{n}$ is maximal ideal so that $\phi^{-1}\mathfrak{n} = \mathfrak{m}$. Then the proposition yields

$$\dim B_{\mathfrak{n}} \leqslant \dim A_{\mathfrak{m}} + \dim B/\mathfrak{m}B.$$

The number $\dim A_{\mathfrak{m}}$ is the dimension of the component of $Y = \operatorname{Spec} X$ that passes through $\mathfrak{m}$ and $\dim B_{\mathfrak{n}}$ that of the component passing through $\mathfrak{n}$, and finally, $\operatorname{Spec} B/\mathfrak{m}B$ is identified with the fibre of ϕ.

Examples

10.7 *(A polynomial ring of excess dimension)* The following example of Krull's illustrates that non-Noetherian rings may show a pathological behaviour when it comes to forming polynomial rings. We shall exhibit a one-dimensional local ring R such that the Krull dimension of the polynomial ring $R[T]$ equals three; that is $\dim R[T] = \dim R + 2$.

The ring R is no more exotic than the ring of rational functions $f(x, y)$ in two variables over a field k which are defined and constant on the y-axis. The elements of R when written in lowest terms have thus a denominator not divisible by x, and $f(0, y)$, which then is meaningful, lies in k.

The ring R is not Noetherian, for instance the ideals (xy^{-i}) with $i \in \mathbb{N}$ form an ascending chain which does not stabilize (very much like in Example 7.4 on page 156). The elements $f \in R$ such that $f(0, y) = 0$ clearly form a maximal ideal $\mathfrak{m}$, and in fact, it is the only prime ideal in R. Indeed, if $f(x, y) = p(x, y)/q(x, y)$ and $f(0, y) \neq 0$, the numerator $p(x, y)$ cannot have x as a factor and $q(x, y)/p(x, y)$ lies in R as well. Hence R is a local one-dimensional ring.

Consider now the polynomial ring $R[T]$. It has the prime ideals 0, $\mathfrak{m}R[T]$ and $(T) + \mathfrak{m}R[T]$, but there is forth one, namely the ideal $\mathfrak{q}$ of polynomial $F(T)$ such that $F(y) = 0$. This in not equal to zero as $xT - xy$ lies there, and it is contained in $\mathfrak{m}R[T]$. Assume namely that $F(T) = \sum_i r_i(x, y)T^i \in \mathfrak{q}$. Then substituting y for T, gives $0 = F(y) = \sum_i r_i(x, y)y^i = 0$, which with $x = 0$ yields $\sum_i r_i(0, y)y^i$. By definition of R the functions $r_i(0, y)$ belongs to k, and since the different powers y^i are linearly independent, it ensues that $r_i \in \mathfrak{m}$; that is, $F(T) \in \mathfrak{m}R[T]$.

10.8 *(A Noetherian ring of infinite dimension)* This examples was found by Masayoshi Nagata. In his famous book "Local ring" ends with a series of peculiar rings having unexpected properties. The first is a Noetherian ring of infinite Krull dimension. Each maximal is of course of finite height, but there are maximal ideals of arbitrary high height.

The construction has the ring $k[x_1, x_2, \ldots]$ of polynomials in countably many variables over a field k as starting point, and depends on a decomposition $\mathbb{N} = \bigcup_i I_i$ of the natural numbers as a disjoint union of finite subsets I_i so that $\#I_i$ tends to infinity when i does. It can as simples as $I_1 = \{1\}$, $I_2 = \{2, 3\}$, $I_3 = \{4, 5, 6\}$ an so forth with I_i consisting of i consecutive numbers.

Let $\mathfrak{p}_i$ be the prime ideal generated by the variables x_j for which the index j belongs to I_i, moreover S will be the set of elements in $k[x_1, \ldots, x_r \ldots]$ not belonging to any of the prime ideals $\mathfrak{p}_i$. Then S is multiplicatively closed and we let $A = k[x_1, x_2, \ldots]_S$ and $\mathfrak{q}_i = \mathfrak{p}_i A$.

The main observation is that local rings $A_{\mathfrak{p}_i}$ are equal to polynomial rings over a certain field in the variables x_j with index $j \in I_i$ localized at the prime ideal those variables generate; that is, $A_{\mathfrak{q}_i} = K_i[x_j | j \in I_i]_{(x_j | j \in I_j)}$, and where

K_i is the field of rational functions over k in the variables x_j for $j \notin I_i$. This shows that $A_{\mathfrak{q}_i}$ is Noetherian and of dimension $\#I_i$ (See problem 6.20 on page 135). It follows that A is infinite Krull dimension, and it remains to see it it Noetherian, which follows from the following lemma

LEMMA 10.30 *Assume that A is a ring such that all localisations $A_{\mathfrak{m}}$ at maximal ideals are Noetherian and that any element i A is contained in finitely many maximal ideals. Then A is Noetherian.*

PROOF: Let $\mathfrak{a}$ be an ideal. Each ideal $\mathfrak{a}A_{\mathfrak{m}}$ is generated by finitely many elements, as $A_{\mathfrak{m}}$ is Noetherian), and they may be chosen to lie in $\mathfrak{a}$. Recollecting all these generators for all the finitely many maximal ideals containing $\mathfrak{a}$, one obtains a finite set of generators for $\mathfrak{a}$. ❑

☆

PROBLEM 10.2 Let A be a Noetherian ring and let $\mathfrak{p} \subset \mathfrak{q}$ be two prime ideals. Prove that if there is a prime ideal properly contained between $\mathfrak{p}$ and $\mathfrak{q}$ then there are infinitely many. HINT: Assume that $\mathfrak{r}_1, \ldots, \mathfrak{r}_r$ are the primes lying properly between $\mathfrak{p}$ and $\mathfrak{q}$. Then $\bigcup_i \mathfrak{r}_i$ is not equal to $\mathfrak{q}$ according to the principle of Prime Avoidance. Pick an element $x \in \mathfrak{p} \setminus \bigcup_i \mathfrak{r}_i$ and apply the Principal Ideal Theorem. ★

PROBLEM 10.3 Show that among the Noetherian rings only the Artinian ones and the semi local one-dimensional ones have finitely many prime ideals. ★

Lecture 11

Principal ideal domains

Preliminary version $-\infty$ as of 2018-08-19 at 07:30:08 (typeset 3rd December 2018 at 10:03am)—
Much work remaining. Prone to misprints and errors and will change.

Principal ideal domains (*Hovedidealområder*)

A class of rings which are omnipresent in mathematics are the *principal ideal domains*. As the name indicates, they are integral domains all whose ideals are principal; that is, every ideal is generated by a single element. They are simple kind of rings with a lot of nice properties. As we shortly shall see they are automatically Noetherian and unique factorization domains.

The most prominent members of this club are the ring of integers $\mathbb{Z}$ and the ring of polynomials $k[t]$ over a field k. Modules over $\mathbb{Z}$ are just abelian groups, incontestably met everywhere in mathematics. Modules over $k[t]$ appear, if possible, even more frequently but often disguished. Such a module is just a vector space V together with a k-linear the action of t; that is, together with a linear operator.

The of club of principal ideal domains is a subclub of the even more fabshionalble club of Dedekind domains, and these are as frequently met as the PID. The ring of integers in an algebraic function field is a Dedekind domain, so they are everywhere in algebraiv number theory. An in algebraic geomtery they are the coordianet sings of non-singualr affine curves. So teh outspring of both number theory and algebaric geoemtry is found in that club.

They are integrally closed domains of Krull dimesion one: So the ring of regular affine curves!

The principal ideal domains live in a family of four. The closest relativ being the big brothers, rthe Bezout domains. They are not necessarly Noetehrein, but have proerty that any fintely generated ideal is principal.

The two other family members are the so called Dede kind rings and the Prufer rings. They There is a genaralization of PID's called Bezout domains. These rings are not requiered to be Noetherian, but they have the property that any finitely generated ideal is principal. A theorem in the theory of functions states that the ring of holomorphic functions i a domain Ω of $\mathbb{C}$ are Bezout domians which makes the Bezout rings important. The Bezout rings share several nice properties with the PID's and we shall prove some whose proof does not have addirional difficulties.

The finitely generated modules over a PID are one of the very few classes of modules which are completely classified. The well-known "Main theorem for finitely generated abelian groups" states that such a group M decomposes as a direct sum of cyclic groups; that is, one has

$$M \simeq \mathbb{Z}^\nu \oplus \bigoplus_i \mathbb{Z}/p_i^{\nu_i}\mathbb{Z},$$

where ν is non-negative integer, the ν_i's are positive integers and the p_i are prime numbers; of course the sum is finite. Over any PID finitely generated modules decomposes in total analogy to this; it holds true that

$$M \simeq A^\nu \oplus \bigoplus_i A/p_i^{\nu_i}A \tag{11.1}$$

where now the p_i's are irreducible members of A, or what amounts to the same, prime elements. As to uniqueness, the integers ν and the *sequence* $(\nu_i)_i$ of the ν_i's appearing is unique. Moreover the sequence $(p_i)_i$ of the irreducible elements p_i's is unique up units; in other words, the sequence of the ideals $(p_i)A$ of unique.

The isomorphism classes of the modules $A/p_i^{v_i}A$, as is the number of times each occur in (11.1), are thus invariants of M, but the direct summands, regarded as submodules of M, are no more unique than bases are for vector spaces.

These classification results hinge on two facts, that any submodule of a free module is free, and that any matrix a with entries from A can be diagonalized; to be precise it can be expresses as a matrix product $a = bdc$ where d is diagonal and b and c invertible.

The decomposition theorem persists being true over quotint rings $R = A/(q)A$ of a PID A. A finite generated module over R is just an A-module that is killed by q. Remarkably the decomposition theorem prevails for any module over R; finitely generated or not. Frequrntly the teroem is atted for so called A-module being of *of bounded exponent* which is synomymus with being killed by an lement q.

q as $q = p_1^{n_1} \dots p_r^{n_r}$ with the p_i'different this amounts to M.

11.1 *Elementary properties.*

Bezout domains (*Bezout-områder*)

As indicated in the introduction a domain A is said to be a *Bezout domain* if every finitely generated ideal is principal. Clearly a PID is a Bezout domain, and the converse holds when the Bezout domain is Noetherian.

Associate elements (*Assosierte elementer*)

11.1 A notion often met in algebraic number theory is that of associated elements. Two elements a and b are *associate* when they are related by an invertible factor; in other words, when $a = \eta b$ for a unit η in A. Of course, being associate is equivalent to generating the same principal ideal. For integers this

is just the good old $\pm$-thing, and polynomials over a field are associate when they differ by a constant factor; but of course, units in most rings are not that simple to describe.

Being associate is evidently an equivalence relation, and the set of principal ideals in A incarnates the set of equivalence classes. Two elements $a|b$ if and only if $(b) \subseteq (a)$; so the divisibility lattice mod association equals the opposit of the lattice of principal ideals.

11.2 Recall that a *greates common divisor* of a finite collection $a_1, \ldots, a_r$ of elements from a ring A is an element d so that $d|a_i$ for all i, and if b is another ring element dividing all the a_i's, then $b|d$. If a greatest common divisor exists, it is unique up to multiplication by a unit.

Greates common divisor (*Største felles divisor*)

Greatest common divisors do not necessarily exist in general, but in a Bezout domain any finite set of elements has one. The ideal $(a_1, \ldots, a_r)$ is in that case principal, and any generator serves as a greatest common divisor of the a_i's. Indeed, if d is generator, it holds that $d|a_i$ since $a_i \in (d)$, and to see that b divides d when $b|a_i$ for all i, just write $d = \sum_i c_i a_i$. Then $d = (\sum_i c_i d_i)b$ where the d_i's are elements with $a_i = d_i b$.

In a similar vein, a generator d of the intersection $\bigcap_i (a_i)$ is a *least common multiple* of the a_i's. It is clear that $a_i|d$. Moreover, if $a_i|b$ for all indices i, the element b lies in the intersection $\bigcap_i (a_i)$, and is therefore divisible by d. In a Bezout domain the intersection of finitely many principal ideals is principal. When the ring is a PID, this is automatic, but for general Bezout domains an argument is needed. In the next lemma we prove it for the intersection of two ideals; the general case follows by an easy induction.

Least common multiple (*Minste felles multiplum*)

LEMMA 11.3 *Let a and b be elements from a domain A. If (a, b) is principal, then the intersection $(a) \cap (b)$ is principal.*

PROOF: Assume that $(a, b) = (d)$ and let x and y be ring elements such that $a = xd$ and $b = yd$. Moreover there are ring elements u and v such that $ux + vy = 1$. An element s from the intersection $(a) \cap (b)$ is shaped like $s = za = wb$, and then $zx = wy$. Multiplying the relation $ux + vy = 1$ by z, one obtains $z = zux + zvy = y(wu + zy)$, or $z = \gamma y$ with $\gamma = wu + zy$. Hence $za = \gamma ya$ and ya (which equals xb) generates the intersection. ❑

The end of this story is that we have established the following:

PROPOSITION 11.4 *In a Bezout domain every finite set of elements has as greatest common divisor and a least common multiple.*

11.5 As signalled in the introduction, the principal ideal domains are the Noetherian members of the Bezout club.

PROPOSITION 11.6 *A PID is Noetherian. Consequently, a Bezout ring is a PID if and only if it is Noetherian.*

PROOF: Assume that A is a PID. Let $\{(a_i)\}$ be an ascending chain of ideals in A and let a be a generator of their union. Then a lies in one of the (a_i)'s, and at that point the chain stabilizes; indeed, $(a) \subseteq (a_i) \subseteq \bigcup_j (a_j) = (a)$ so that $(a_i) = \bigcup_j (a_j)$ and consequently $(a_i) = (a_j)$ for $j \geqslant i$.

As to second statement, if a Bezout domain is Noetherian, every ideal is finitely generated and hence principal. ❑

PID *s and* UFD *s.*

11.7 The notion of prime numbers can be generalized to elements in any ring. A *prime element* in a ring A is an element a such if a divides a product, it divides one of the factors; in other words, a relation like $bc = ya$ for some y implies $c = xa$ or $b = xb$ for some x. This is obviously equivalent to the principal ideal (a) being a prime ideal.

Prime elements (*Primelementer*)

In a polynomial ring one has the notion of irreducible polynomials which generalizes in the following way. An *irreducible element* a in a ring A is essentially an element without other factors than itself. One can of course modify a by multiplying it with a unit, so the natural requirement for a to be irreducible, is that a relation $a = bc$ implies that either b or c is a unit. In terms of ideals, this is equivalent to the principal ideal (a) being maximal among the proper principal ideals.

irreducible elements (*irreducible elementer*)

11.8 In general being prime implies being irreducible; indeed, if a is prime and $a = bc$, it holds true that $b = xa$ or $c = xa$, hence $a = xca$ and $1 = xc$ or $a = xba$ and $1 = xb$. The converse does not hold in general; but in Bezout domains it holds:

PROPOSITION 11.9 *In Bezout ring being prime is equivalent to being irreducible.*

PROOF: Asumme that a is irreducible and that $xa = bc$, we have to see that $a|b$ or $a|c$. The ring A being Bezout, it the ideal (a, b) is principal and obviously $(a) \subseteq (a, b)$. By assumption a is irreducible so that (a) is maximal among the principal ideals. It follows that either $(a) = (a, b)$ or $(a, b) = 1$. In the former case $a|b$ and in the latter there is a relation $ya + zb = 1$, which upon multiplication by c transfomez into $(yc + x)a = c$; that is, $a|c$. ❑

COROLLARY 11.10 *In a* PID *every prime ideal is maximal.*

PROOF: Assume that (p) is a prime ideal. Let $\mathfrak{m}$ be a maximal ideal containing (p); it is principal since the ring is PID. By Proposition 11.9 above p is irreducible and hence (p) is maximal among the principal ideals; thus $(p) = \mathfrak{m}$. ❑

EXAMPLE 11.1 A kind of generic example of irreducibles elements not being prime is manifest in the ring $k[x, y, z, w]/(xy - zw)$. Clearly, the class of x is not a prime element, but for degree reasons, it must be irreducible. Of course, the same holds for any of the other variables. See Problem 11.2 below. ☆

EXAMPLE 11.2 The simplest example of irreducibles not being prime is found in the ring $\mathbb{Z}[\sqrt{-5}]$. There the relation

$$2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$$

holds, so for instance, 2 is not a prime element. It is however irreducible, for if $2 = zw$, one has $4 = \|2\|^2 = \|z\|^2\|w\|^2$. But being shaped like $a^2 + 5b^2$ with $a, b \in \mathbb{Z}$, both $\|z\|^2$ and $\|w\|^2$ are integers, and we infer that either $\|w\| = 1$ or $\|z\| = 1$. Finally, a relation like $a^2 + 5b^2 = 1$ between integers entails that $a = 1$ and $b = 0$, and we may conclude that either z or w equals ± 1. ⋆

PROPOSITION 11.11 *In a Noetherian ring any element is a product of finitely many irreducible elements.*

PROOF: We consider the set Σ of "bad guys": The set of principal ideals (x) so that x is a counterexample to the assertion; or in other words, so that x is not a product of finitely many irreducibles. If non-empty, the set Σ has a maximal member, say (a). Then a is not irreducible, and we may write $a = bc$ with neither factor being a unit. This means that $(a) \subsetneq (b)$ and $(a) \subsetneq (c)$, and by consequence, neither (b) nor (c) belongs to Σ as (a) was maximal there. Hence both b and c can be expressed as finite products of irreducibles, and the same is true for a. Contradiction. ❑

PROPOSITION 11.12 *In a Bezout domain the factors in a finite product of irreducibles are unique up to order and multiplication by a unit.*

PROOF: The proof proceeds by induction on the number irreducible factors. Assume that $\prod_i p_i = \prod_j q_j$ both products being finite and all the factors being irreducible. By Proposition 11.9 above the factors are all prime elements, and it follows that one of the p_i's divide one of the q_j's, and after reordering the factors we may assume that $p_1 = aq_1$. Now p_1 is irreducible, so a is a unit, and we may as well assume that $p_1 = q_1$. Cancelling p_1 we have reduced the number of factors, and we are done by induction. ❑

11.13 Combining the two previous propositions, we see that in principal ideal domain one has unique factorization:

THEOREM 11.14 *Every* PID *is a* UFD.

PROOF: A PID is Noetherian so every element factors as a product of finitely many irreducibles (Proposition 11.11). A PID being a Bezout domain, the factors are unique up yo order and units (Proposition 11.12). ❑

EXAMPLE 11.3 The theorem is not true for Bezout domains that are not Noetherian; For example, the irreducible elements in the ring of holomorphic functions in a domain are (up to units) the simple linear functions $z - a$; and finite products of such of course merely have finitely many zeros. In

any domain $\Omega \subseteq \mathbb{C}$ there are functions with infinitely many zeros which can not be products of finitely many irreducibles. In fact, a famous theorem of Weierstrass' asserts that for any sequence $\{a_n\}$ of distinct points in Ω not accumulating in Ω, there is a function vanishing at the a_n's and nowhere else; one may even prescribe the order of vanishing at each a_n. ☆

Problems

11.1 Referring to Example 11.2 show that the three other involved numbers 3, $1 + i\sqrt{5}$ and $1 - i\sqrt{5}$ are irreducible.

11.2 This exercise gives a general version of Example 11.1. Assume that $A = \bigoplus_{i \geqslant 0} A_i$ is a graded integral domain with A_0 being a field. Assume there are four homogeneous elements of degree one x, y, z and w that satisfy $xy = zw$. Show that x is irreducible but not prime. HINT: Assume that there is a factorization $x = pq$. Work with the non-vanishing homogeneous components of p and q of highest degree.

11.3 Let $A = \mathbb{Z}[x, y, z, w]/(xy - wz)$ show that the class of x is irreducible but not prime.

11.4 *(Euclidean domains.)* A domain A is said to be *Euclidean* if there is function δ on A assuming values in the set $\mathbb{N}_0$ of non-negative integers that has the following property:

Euclidean domains (Euklidske områder)

- For any pair x and y with $y \neq 0$ there are elements q and r in A so that $x = yq + r$ and either $\delta(r) < \delta(y)$.

Show that a Euclidean domain is a PID. HINT: An ideal $\mathfrak{a}$ will be generated by an x minimizing δ over the non-zero members of $\mathfrak{a}$.

11.5 Show that the conclusion that A is a PID in the previous exercise persist when in the definiton of δ the set $\mathbb{N}_0$ is replaced with any *well-ordered* set W .

11.6 Let $n \in \mathbb{Z}$ and put $\delta(n)$ to be the number binary digit of $\|n\|$. Show that δ is the smallest Eucliden function on $\mathbb{Z}$. The article[1] is a nice paper about Eucliden algorithms.

[1]

11.7 Show that $\mathbb{Z}[i]$ is Euclidean.

11.8 Show that $\mathbb{Z}[\sqrt{-d}]$ is Euclidean for $d = 1, 3, 7, 11$.

11.9 Let $r > 0$ be a real number. Show that set of power series that converge for $\|z\| > r$ is an Euclidean ring. HINT: The number of zeros in the disk $\{ z \mid \|z\| \leqslant r \}$ is a Euclidean function.

★

11.2 *Some general facts*

Torsion modules

Let A be a domain and let M by any module over A. Recall that a *torsion element* in A is an element killed by some non-zero member of the ring.

Torsion elements (*Torsjonselementer*)

Cleary the sum of two torsion elements is a torsion element (if a kills x and b kills y, the product ab kills $x+y$) as is cx for any $c \in A$. In other words, the torsion elements form a submodule $T(M)$ of M:

$$T(M) = \{\, x \in M \mid am = 0 \text{ for a non-zero } a \in A \,\}.$$

The torsion module depends functorially on M, and it sits in the short exact sequence

$$0 \longrightarrow T(M) \longrightarrow M \longrightarrow M/T(M) \longrightarrow 0.$$

The quotient $M/T(M)$ is clearly torsion free; if ax is torsion, x will be. A module M is called a *torsion module* if $T = T(M)$, and M is said to be primary if $x \in M$ ar killed by powers of a single prime p; that is, for some integer $p^\nu x = 0$ for every $x \in M$. The actual power need for the killing depends on x, and need not be bounded. For intstance when p is a prime number, the group $\mathbb{Z}_{p^\infty}$ has elements of every odre a power of p. The annihilator of such modules is zero eventhough the annihilator over single element has $(p)A$ as radical.

Torsion modules (*Torsjonsmoduler*)

LEMMA 11.15 *Assume that A is a* PID. *A torsion module T over A decomposes as the direct sum $T = \bigoplus_p T_p$ of the primary modules T_p, where the sum extends over all prime ideals (p) in A.*

PROOF: Obviously $T_p \cap T_q = 0$ when p and q are realtively prime; Writing $1 = \alpha p + \beta q$ gives $x = \alpha p x + \beta q x = 0$ whenever x belongs to the intersection.

Let x be any element in T and assume that $ax = 0$ with $a \neq 0$. As A is a UFD, there is a factorization $a = \prod_i p_i^{\nu_i}$ of a into a product of powers of distinct irreducible elements. The crucial fact is that the products $q_j = \prod_{i \neq j} p_i^{\nu_i}$ do not have common factors for different j's; hence there is relation

$$1 = c_1 q_1 + \ldots + c_r q_r.$$

And from ensues upon multiplication by x the relation

$$x = c_1 q_1 x + \ldots + c_r q_r x.$$

Now $a = q_j p_j^{v_j}$, so that each summand $c_j q_j x$ is annihilated by $p_j^{\nu_j}$ and therefore belongs to T_{p_j}. ❑

EXAMPLE 11.4 The abelian group $\mathbb{Q}/\mathbb{Z}$ is a typical infinite torsion group, and the p-torsion part equals the group $\mathbb{Z}_{p^\infty} = \mathbb{Z}[p^{-1}]/\mathbb{Z}$. Indeed, that a rational number x satisfies $p^\nu x \in \mathbb{Z}$, means that $x = a/p^v$ for some $a \in \mathbb{Z}$. It follows

that there is a decomposition $\mathbb{Q}/\mathbb{Z} = \bigoplus_p \mathbb{Z}_{p^\infty}$ where the sum extends over all primes.

Verbatim, this reasoning works for any principal ideal domain A, and one has a decomposition

$$K/A = \bigoplus_p A_{p^\infty}$$

where K is the fraction field of A and $A_{p^\infty} = A[p^{-1}]$, and where the sum is taken over all prime ideals (p). ☆

11.3 *Finitely generated modules*

Principal ideal domains enjoy the property that all projective modules are free. It holds unconditionally, but we shall prove it merely for projective modules of finite rank to avoid diving into the deep waters of transfinite induction arguments. Moreover, any submodule of a free module is free which is a rather rare property for a ring to have. Consequently any module has a free resolution of length two; that is, it sits in an exact sequence of shape

$$0 \longrightarrow A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0,$$

where in general n and m designate possibly infinite cardinal numbers. When M is finitely generated however, both are finite, and M can be described as the cokernel of a matrix Φ with entries in A. Subsequently we shall establish that Φ may even be taken to be diagonal, and the decomposition theorem ensues directly from this.

Again we shall work with Bezout rings. All the above results follow, but for modules of finite presentation. An A-module M is of finite presentation if it sits in an exact sequence

$$A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0.$$

In other words it is finitely generated and one may chose the generators in way that the relations between them are finitely generated as well. Over a Noetherian ring every submodule of A^n is finitely generated, hence being finitely generated is equivalent to being finitely presented.

Free and projective modules

Recall that the *rank* of a module M over a domain A is the dimension $\dim_K M\otimes_A K$ of $M\otimes_A K$ as a vector space over the function field K of A. Since localization is an exact operation, the rank is additive over exact sequences, and a free module is of rank n precisely when having a basis with n elements.

Recall also that if A is a domain and M is a torsion free A-module, the canonical map $M \to M\otimes_A K$ is injective; indeed, the kernel consists of those

elements m in M that are killed by a non-zero divisor in A, and as M is torsion free, there are no such a part from zero. This leads to the following

LEMMA 11.16 *Assume that M is a finitely generated torsion free module over the domain A. Then there is non-zero A-linear map $\phi\colon M \to A$.*

PROOF: Start by choosing a non-zero K-linear map $\tilde{\phi}\colon M \otimes_A K \to K$. The module M is contained in and spans the K-vector space $M \otimes_A K$. Therefore $\tilde{\phi}$ does not vanish on M, but of course it does not necessarily assume values in A. To achieve this let $m_1, \dots, m_r$ be generators for M and let a be a common denominator for the images $\tilde{\phi}(m_i)$. Then $\phi = a \cdot \tilde{\phi}$ does the job. ❑

THEOREM 11.17 *Assume that A is a Bezout domain. Then every finitely generated submodule of a finitely generated torsion free A-module E is free. In particular, every finitely generated torsion free A-module is free.*

Torsion free modules over a PID which are not finitely generated is a devilish class, and even for abelian groups there are large white areas on the map. For instance, torsion free subgroup contained in $\mathbb{Q}^2$ seem to be impossible to classify. However those contained in $\mathbb{Q}$ are rather easy to lay hands on (see exercise xxx).

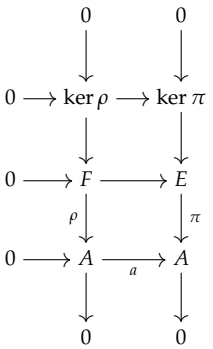
The case of principal ideal domains merits is own announcement. The finitely general case i cover by the theorem above, but it holds without hypotheses on the projective modules—in fact almost Noetherian domains projective modules that are not finitely generated are free.

COROLLARY 11.18 *Assume that A is a PID. Then every projective module is free and every submodule of a free module is free.*

PROOF OF THEOREM 11.17: Since E is a submodule of itself, the second assertion ensues from the first. The proof of the first proceeds by induction on the rank of the projective module E. Let $F \subseteq E$ be a submodule.

Choose any non-zero A-linear map $\pi\colon E \to A$ that does not vanish on F. Its image is a finitely generated ideal which is principal because A is Bezout. But principal ideals are isomorphic to A as A-modules, and consequently we have a *surjective* A-linear map $\pi\colon E \to A$. This settles the rank one case, as π will be an isomorphism in that case.

In a similar vein, the image of F under π is an ideal which is finitely generated and thus principal, say generated by a. Then we may write $\pi|_F = a \cdot \rho$ where ρ is a surjective map $F \to A$. Lemma xxx ensures that both π and $\pi|_F$ are split surjections, and there are decompositions $E \simeq A \oplus \ker \pi$ and $F \simeq A \oplus \ker \rho$.



Now, $\ker \pi$ being a direct summand in a finitely generated projective module, is finitely generated and projective; moreover, its rank is obviously one less than that of E. By induction we infer that $\ker \rho$ is free, and consequently F is free in view of the isomorphism $F \simeq A \oplus \ker \rho$. ❑

11.19 Just being slightly more careful in the proof the lemma can be generalized to

LEMMA 11.20 *Let A be Prufer domain, then every finitely generated torsion free A-module is isomorphic to a direct sum of projective modules of rank one.*

Recall that a Prufer domain is an integral domain with all finitely generated ideals being projective. Dedekind domains are of this sort, and of course principal ideal domains as well, their ideals are even free modules. In the dictionary between algebra and geometry, projective modules correspond to vector bundles. Hence on the affine curve $X = \operatorname{Spec} A$, any vector bundle decomposes as the sum of line bundles. This is far from being the case on projective curves, the projective line being the sole exception.
PROOF: Induction on the rank will do. The rank one case being the hypothesis that A be Prufer. Once we have non-zero map

$$E \to A$$

the kernel decomposes as a direct sum of rank one projectives, and since E is finitely generated the image is a projective ideal. Hence $E \simeq I \oplus \ker \pi$, and $\ker \pi$ is finitely generated projective. The ranks has dropped by one, and the induction hypothesis applies to $\ker \pi$.

So have to infer that E^* has a non zero element, but this is just xxxx, any element E that maps to $E \otimes_A K$ is torsion. ❑

PROBLEM 11.10 Assume that M is a finitely generated graded A-module that is torsion free. Show that M is free; *i.e.* M is isomorphic to a finite sum $M \simeq \bigoplus_i A(n_i)$ HINT: Copy the proof of lemma xxx and notice that homogeneous ideals in $k[x, y]$ are principal. ★

The fundamental theorem

With basis in the lemma we esatbilished in the previous paragraph, we shall establish that any A-lineaer map between two free A-modules can with appropiate choices of bases in two module be represented by a diagonal matrix. any matrix with enries in F can be diagonalise. The proof we present is totally elemnetary and goes back to Wedderburn who showed the teorem for matrices of holomorphicx function.

The assumpition that A is Bezout does no at complications,

But in the wek sens

he classification ensues from the *a priori* stronger result that matrices with entries in a PID can be diagonalized. Indeed, as mentioned in the beginning of the section every finitely presented module is the cokernel of an A-linear map between free modules.

11.21 Our first lemma is a criterion for when an element in a free module is part of a basis:

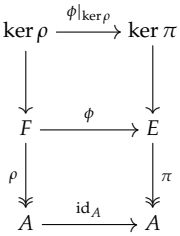
LEMMA 11.22 *Assume that A is a Bezout domain. Let E be a free A-module of finite rank and let $e \in E$ be an element. Assume there is an A-linear map $\pi\colon E \to A$ with $\pi(e) = 1$. Then e is part of a basis for E.*

PROOF: The kernel of π is free by Proposition 11.17, so pick a basis $\{e_i\}_{1 \leqslant in-1}$ for it. We contend that joining e to that basis we obtain a basis for E. Applying π to a linear dependence relation $\sum_i a_i e_i + ae = 0$ immediately gives $a = 0$, so e together with the e_i's constitute a linearly independent set. They also generate E since for any $x \in E$ the element $x - \pi(x)e$ lies in $\ker \pi$, and hence is a linear combination of the e_i's. ❑

PROPOSITION 11.23 *Let E and F be free A-modules of the same rank. Let $\phi\colon F \to E$ be an injective linear map. Then there are bases $\{f_i\}$ for F and $\{e_i\}$ for E and ring elements λ_i so that $\phi(f_i) = \lambda_i e_i$.*

In the case A is a field and E and F are vector spaces of the same dimension, the proposition just says that the image of basis under an injection is a basis; in fact, in that case, the matrix may be taken to be the identity matrix. The result is far less subtle than any existence theporem for eigenvalues.
PROOF: Pick an element $f \in F$ that is part of a basis $\{\hat{f}_i\}$ for F, and chose a basis $\{\hat{e}_i\}$ for E. These two bases are auxiliary and not the ones we shall end up with—hence the hat. Anyhow, $\phi(f)$ may be expressed in terms of the $\hat{e}_i$'s; that is, it can be written as a linear combination $\phi(f) = \sum_j a_i \hat{e}_i$ with the a_i's from A. The ideal $(a_1, \ldots, a_n)$ generated by the a_i's is principal since A is a Bezout domain, and let us say it is generated by the element d.

❑ The case $d = 1$.



This means that there are ring elements c_i so that $\sum_i c_i a_i = 1$. Define an A-linear map $\pi\colon E \to A$ by sending an element $\sum_i x_i \hat{e}_i$ to $\sum_i c_i x_i$. Put $\rho = \pi \circ \phi$; then by the choice of the c_i's, it holds true that $\rho(f) = 1$, and the maps ρ and π are both split surjections. Their kernels are therefore free (Proposition 11.17) and ranks have dropped by one. By induction the two kernels have bases $\{f_i\}_{1 \leqslant i \leqslant n-1}$ and $\{e_i\}_{1 \leqslant i \leqslant n-1}$ respectively so that

$$\phi(f_i) = \lambda_i e_i \tag{11.2}$$

for $1 \leqslant i \leqslant n-1$ and for approriate ring elements λ_i. By Lemma 11.22 above adjoining $e = \phi(f)$ and f respectively to the bases $\{e_i\}$ and $\{f_i\}$ we obtain bases for E and F. Evidently the relations in (11.2) persist, and by construction $\phi(f) = e$.

❑ The genral case.

The idea is to factor ϕ as a map falling under the first case and one which apriori has diagonal martxi. Assume then that $d \neq 1$ then there are ring

elements g_i so that $a_i = g_i d$ and $(g_1, \dots, g_n) = A$. Define a new map $\psi\colon F \to E$ by $\psi(f) = \sum_i g_i \hat{e}_i$ and $\psi(\hat{f}_i) = \phi(\hat{f}_i)$. Then ψ satisfy the hypothesis of the first case, and there are bases $\{e_i\}$ and $\{f_i\}$ like in the first case. Now define a map $\sigma\colon F \to F$ by putting $\sigma(f) = df$ and $\sigma(f_i) = f_i$ for the rest of the basis f_i. Then it holds true that $\phi = \psi \cdot \sigma$ and we are trhough. ❑

THEOREM 11.24 *Let E and F be two free A-module of finite rank, and $\phi\colon F \to F$ an A-linear map. The there are bases for F and E so that the matrix is semi-diagonal.*

Semi-diagonal means that the only non-zero elements of the matrix are situated on the diagonal that emanates from the upper left corner. Of course when matrix is squar, this is just being diagonal.
PROOF: The image of ϕ is a free module after Ppropostion **??** as is the kernel, and hence $F \simeq \in \phi \oplus \ker \phi$. The map ϕ factors trhroug an injective $\tilde{\phi}\colon \operatorname{im}\phi \to E$, and by Proposition xxx there are bases for $\in \phi$ and E relative to which $\tilde{\phi}$ has a diagonal matrix. Lift these basis elements to F and complement them with a basis for $\ker\phi$ to obtain a basis for F of the right sort. ❑

COROLLARY 11.25 *Let A be a Bezout domian. Then everyr finitely presented A-module has a decompositiob in cyclicv modules*

$$M \simeq A^{\nu} \oplus \bigoplus_i A/p_i^{\nu_i} A$$

where ν is a non-negative integer and where the p_i's are irreducidble elements in A and the ν_i's natural numbers.

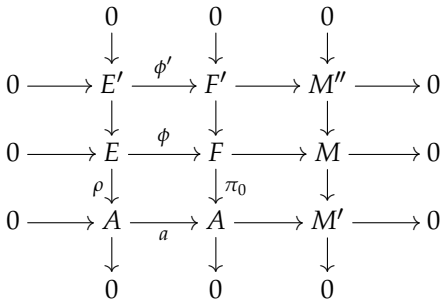
PROOF OF PROPOSITION **??**: For simplicity we assume that F is of finite rank; say n, and proceed by induction on n. The assumption that A is a PID immediatly solves the case that $n = 1$; indeed, the image of ϕ is an ideal in A which is principal as A is a PID, hence it is isomorphic to A as an A-module.

As to the induction step, the trick is choose an A-linear map $\pi\colon F \to A$ in the following optimal way. The images $\operatorname{im}\pi \circ \phi$ where π runs through the surjective maps $\pi\colon F \to A$, form a non-empty set of ideals which, since A is noetherian, contains a maximal[2] element. We let π_0 be a map realizing a maximal image and let a be a generator for $\operatorname{im}\phi \circ \pi_0$, or in other words, $\phi \circ \pi_0$ factors as $a\rho$ for some surjective A-linear map $\rho\colon E \to A$.

These maps enter into a selfexplanatory commutative diagamme[3]with exact

[2] It is not necessarily a maximal ideal, but merely maximal among the ideals under consideration.
[3] If you don't find it self explanatory: E' and F' are the kernels of ρ and π_0; the column to the right is made up of cokernels and is exact by the snake lemma

rows and column



By lemma xxx on page xxx we infer that the middle column is split so that $E \simeq F' \oplus A$, and it follows that F' is projective. By lemma xxx from this ensues that F' is free, and obviously, its rank is one less than F. Hence the induction hypothesis applies, and we can conclude that E' is free. Now, the leftmost column is also split and $E = F' \oplus A$. Thus E is free and the first assertion is established.

Then we attack the assertion about the bases, and we denote the rank of E by M and that of F by n. By induction, there are bases $e_1, \ldots, e_{m-1}$ for E' and $f_1, \ldots, f_{n-1}$ for F' such that $\phi|_{E'}$ sends e_i to $a_i f_i$ with $a_i \in A$ We extend these bases to bases for E and F by respectively adding an element e_m of E such that $\rho(e_m) = 1$ and and element f_n of F with $\pi_0(f_n) = 1$.

The crucial observation is that for any projection $\pi\colon F \to A$, it holds true that $\pi(\rho(e_m)) \in (a)$. Indeed, assume not, and let $b = \pi(\rho(e_m))$. Then $(a, b) = 1$, and one may write $\alpha a + \beta b = 1$ for appropriate elements α and β in A. Then $\alpha\pi_0 + \beta\pi$ sends e_m to 1, contradicting the maximality of (a).

Applying this observation to the projections onto the different basis elements f_i, leads us to an expression $\phi(e_m) = af_m + \sum_i c_i a f_i$ for c_i's in A, and simply replacing f_m by $f_m + \sum_i c_i f_i$, we have the requested basis element. ❑

In fact observing that if $E = A \oplus M'$ and M is finitely generated, if follows that M' is finitely generated. This follows for instance, by decomposing $\mathrm{id}_M = \eta_1 + \eta_2$ into a sum of two oprthogonal idempotents, such that $\eta_2(M) = M'$.

Å lese: Lam, T. Y. (2006), Serre's Problem on Projective Modules, Springer Monographs in Mathematics, Berlin, Heidelber

Ât′