UNIVERSITETET
I OSLO

MAT 4200 Commutative algebra

Part 1, Rings and ideals
(Chapt. 1 and 2)

August, 26 - September, 3, 2020

We study rings in general, and rings with additional properties. We also define ring homomorphisms and state basic properties of rings and ring homomorphisms before we define ideals, give some basic properties, and study how ideals behave under homomorphisms. Finally we define prime and maximal ideals.

1.1-1.3, 2.1-2.2

Definition

A **ring** *is a set A endowed with two binary operations; an addition, $a+b$, which makes A an abelian group, and a multiplication, ab. The multiplication is assumed to be* **distributive** *over the addition $a(b+c) = ab+ac$, and in this course it will always be* **associative**, $a(bc) = (ab)c$, **commutative**, $ab = ba$ *and* **unital** $1 \cdot a = a$ *(or at least almost always).*

Example

- *The ring $\mathbb{Z}$ of integers*
- *The fields of rational numbers; $\mathbb{Q}$, real numbers; $\mathbb{R}$ and complex numbers; $\mathbb{C}$.*
- *The ring $\mathbb{Z}_n$ of integers modulo a number n.*
- *The ring $M_n(\mathbb{R})$ of square $n \times n$-matrices with real entries (non-commutative).*

Example

- *The polynomial ring* $\mathbb{Q}[x_1, \ldots, x_n]$.
- *The set of continuos functions on an interval,* $C([a, b])$ *is a ring.*
- *Quadratic extensions* $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$ *of the integers are rings.*

Definition

a) A non-zero element a in a ring A is called a **zero-divisor** *if there exist a non-zero element $b \in A$ such that $ab = 0$. Non-zero-divisors are also called or a* **regular elements**.

b) A ring without zero-divisors is called an **integral domain**, *or a* **domain**.

Proposition

In an integral domain A the **cancellation law** *holds true, i.e. if $a \neq 0$ then $ab = ac$ implies $b = c$.*

Proof.

$$ab - ac = a(b - c) = 0, \quad a \neq 0 \qquad \Rightarrow \qquad b - c = 0$$

Definition

a) A non-zero element a in a ring A is **nilpotent** *if $a^n = 0$ for some $n \geq 1$.*

b) A ring without nilpotent elements is said to be **reduced**.

Notice that sums and products of nilpotent elements are nilpotent as well. In fact if $a^n = b^m = 0$, then $(a+b)^{n+m-1} = 0$.

Definition

a) A non-zero element a in a ring A is a **unit** *if there exist a non-zero element $a^{-1} \in A$ such that $aa^{-1} = 1$.*

b) A **field** *is a ring where all non-zero elements are units.*

Example

i) *The ring $\mathbb{Z}/(n)$ has zero-divisors if and only if n is a composite number.*

ii) *The ring of continuous functions on the union X of the x-axis and the y-axis has zero-divisors. The function xy vanishes identically on X, but neither x nor y does.*

iii) *The ring $\mathbb{Z}/(p^r)$ has nilpotent elements for $r > 1$.*

Definition

A subring B of A is a ring contained in A whose ring operations are induced from those of A.

Example

i) *The ring $\mathbb{Z}[\frac{1}{n}]$ is the subring of $\mathbb{Q}$ consisting of numbers where the denominator is a power of n.*

ii) *The subring $\mathbb{C}[t^2, t^3]$ of $\mathbb{C}[t]$ 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.*

iii) *The subring $\mathbb{C}[x, \frac{1}{x}]$ 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.*

Definition

a) A map $\phi : A \to B$ of rings is called a **ring homomorphism** *if it satisfies*

i) $\phi(a+b) = \phi(a) + \phi(b)$ *and* $\phi(0) = 0$

ii) $\phi(ab) = \phi(a)\phi(b)$ *and* $\phi(1) = 1$.

b) A map $\phi : A \to B$ of rings is called an **isomorphism** *if there exists a homomorphism $\psi : B \to A$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identites of A and B respectively.*

c) A ring homomorphism $\phi : A \to A$ from a ring to itself is called an **endomorphism**.

Example

i) *The* **evaluation map** $e_a : \mathbb{C}[x] \to \mathbb{C}$ *for some complex number* $a \in \mathbb{C}$, *given by mapping a polynomial* $f(x)$ *to the number* $f(a)$ *is a homomorphism.*

ii) *The map* $\mathbb{Z} \to \mathbb{Z}/(n)$ *sending* x *to its residue class* $\overline{x}$ *is a homomorphism.*

iii) *An isomorphism of a field extension* E *over a ground field* k *is a endomorphism.*

iv) *The ring homomorphism* $\mathbb{Z}/(p) \times \mathbb{Z}/(q) \to \mathbb{Z}/(pq)$ *for two primes* p *and* q *is an isomorphism.*

Definition

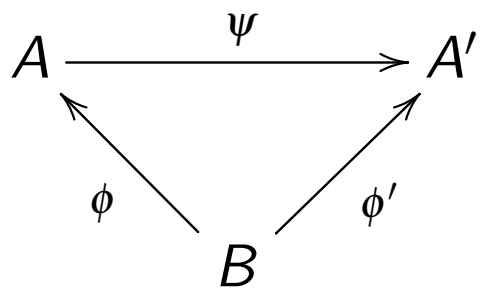
a) Let A be a ring. The element $1 \in A$ generates a subring A_0 of A, called the **prime ring** *of A.*

b) The prime ring is isomorphic to either $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}$. In the former case the integer n is called the **characteristic** *of A; $char(A) = n$, in the latter case we say that A is of* **characteristic zero**;
$char(A) = 0$.

Definition

*a) Let A and B be two rings. A B-***algebra structure** *on A is a homomorphism $\phi : B \to A$.*

b) Let $\phi : B \to A$ and $\phi' : B \to A'$ be two B-algebras. A B-algebra homomorphism $\psi : A \to A'$ is a ring homomorphism which respects the B-algebra structure, i.e. $\psi \circ \phi = \phi'$.



Notice that any ring is a $\mathbb{Z}$-algebra.

Definition

A **polynomial** *over A is an expression*

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

where $a_\alpha \in A$ and the sum is required to be finite. The polynomial ring is denoted

$$A[x_1, \ldots, x_n]$$

The **degree** *of $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ is given by $deg(x_1^{\alpha_1} \ldots x_n^{\alpha_n}) = \sum_{i=1}^n \alpha_i$.*

Definition

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.*

Proposition (The Universal Mapping Property)

Let A be a ring. Assume given a sequence $b_1, \ldots, b_r$ of elements from an A-algebra B. Then there is a uniquely determined algebra homomorphism $\phi : A[x_1, \ldots, x_r] \to B$ such that $\phi(x_i) = b_i$ for $1 \leq r$.

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 $\phi(p) = \sum_\alpha a_\alpha b_1^{\alpha_1} \cdot \ldots \cdot b_r^{\alpha_r}$ gives a well-defined map which easily is seen to be additive and multiplicative. □

Definition (free object)

An object $F(S)$ (ring, group, module, etc.) in a category $\mathscr{C}$ is **free** *on a set S if for any other object C in the same category;*

$$Mor_{\mathscr{C}}(F(S), C) = Mor_{\underline{sets}}(S, g(C))$$

where $g : \mathscr{C} \to \underline{sets}$ is the forgetfull functor.

Example

* *The polynomial ring $A[x_1, \ldots, x_r]$ is a free ring (k-algebra) since we have*

$$Hom_{\underline{rings}}(A[x_1, \ldots, x_r], R) = Mor_{\underline{sets}}(\{x_1, \ldots, x_r\}, f(R))$$

* *Free abelian groups (finitely generated): $\mathbb{Z}^N$.*
* *Any vector space is free. (Notice that for an infinite vector space this depends on Zorn's lemma, see September, 2).*

Definition

A **formal power series** *over A is an expression*

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

where $a_\alpha \in A$ *and the sum is not required to be finite. The ring of formal power series is denoted*

$$A[[x_1, \ldots, x_n]]$$

Definition

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 idempotents** *when $fg = 0$. The unit element and zero are called the* **trivial idempotents**.

Some facts:

- The element $1 - e$ is idempotent and orthogonal to e;
- The subset $Ae = \{ae \mid a \in A\}$ is a subring with e as a unit element.
- In the direct product $A_1 \times A_2$ there are two natural defined orthogonal idempotents, $(1,0)$ and $(0,1)$.

Proposition

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 Ae_i is a subring in the restricted sense, and the association $x \mapsto (xe_1, \ldots, xe_r) = (xe_i)_i$ gives an isomorphism of rings

$$\phi : A \xrightarrow{\simeq} \prod_i Ae_i.$$

The projection onto Ae_i is realized as multiplication by e_i.

Proof.

1) Clearly ϕ is additive. Let x and y be two elements from A. The e_i's being idempotents, we find

$$\phi(x)\phi(y) = (xe_i)_i \cdot (ye_i)_i = (xye_ie_i)_i = (xye_i)_i = \phi(xy),$$

and thus ϕ also respects the multiplication.

2) The unit element 1 maps to the string $(e_i)_i$ which is the unit element in the product

3) If $\phi(x) = (xe_i)_i = 0$, it follows that each $xe_i = 0$, hence $x = x \cdot 1 = x\sum e_i = \sum xe_i = 0$. Thus ϕ is injective.

4) Given an element $(x_ie_i)_i$ in the product, we set $x = \sum_i x_ie_i$. Using that the e_i's are mutually orthogonal, we find $xe_j = \sum_i x_ie_ie_j = x_je_j$, and x maps to the given element $(x_ie_i)_i$. It follows that ϕ is surjective.

□

Definition

An additive subgroup $\mathfrak{a}$ of A is called an **ideal** *if $A\mathfrak{a} = \mathfrak{a}$. The ideal is* **proper** *if $\mathfrak{a} \neq A$, and it is* **non-trivial** *if $\mathfrak{a} \neq 0$,*

In other words, $\mathfrak{a}$ is proper if $1 \neq \mathfrak{a}$, and non-trivial if there exists a non-zero element $0 \neq a \in \mathfrak{a}$.

Example

The non-trivial proper ideals of the integers $\mathbb{Z}$ are in one-to-one correspondence with the natural numbers $\mathbb{Z}_+$.

$$(n) \subset \mathbb{Z}$$

Proposition

A ring A is a field if and only if it has no proper non-trivial ideals.

Proof. $\Rightarrow$. Let A be a field, and suppose $\mathfrak{a}$ is a non-trivial proper ideal with $a \in \mathfrak{a}$ a non-zero element. Then $a^{-1} \cdot a = 1 \in \mathfrak{a}$, which contradicts the properness.
$\Leftarrow$. Let $a \in A$ be a non-zero element. By assumption $(a) = A$ and consequently $1 \in (a)$, i.e. there exist an invers $a^{-1} \in A$. $\square$

Definition

a) A **partial order** *on a set* Γ *is a relasjon* $\leq$ *defined on a subset of* $\Gamma \times \Gamma$ *containing the diagonal and satisfying the axioms:*

Reflexivity: $x \leq x$ *for all* $x \in \Gamma$.

Anti-symmetry: *If* $x \leq y$ *and* $y \leq x$, *then* $x = y$.

Transitivity: *If* $x \leq y$ *and* $y \leq z$, *then* $x \leq z$.

b) A set with a partial order is called a **partial order set**, *or* **poset**.

The set of ideals in the ring A is denoted $\mathscr{I}(A)$. It is a **partial ordered set** under the inclusion relation, i.e. $\mathbf{a} \leq \mathbf{b}$ if $\mathbf{a} \subseteq \mathbf{b}$.

Some facts about ideals:

i) $\cap_{i\in I}\mathfrak{a}_i$ of an arbitrary set of ideals is the largest ideal contained in all $\mathfrak{a}_i$.

ii) $\sum_{i\in I}\mathfrak{a}_i$ consisting of all finite sums of elements of the $\mathfrak{a}_i$'s. It is the smallest ideal containing all $\mathfrak{a}_i$.

iii) An ideal generated by a single element $a \in A$ is called a **principal ideal**, denoted (a).

iv) The product of two ideals **a** and **b** is given by

$$\mathbf{a}\cdot\mathbf{b} = \{a_1b_1 + \cdots + a_rb_r \,|\, a_i \in \mathbf{a},\, b_i \in \mathbf{b}\}$$

v) A domain where all ideals are principal is called a **principal ideal domain** (PID).

vi) The **transporter**

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \,|\, x\mathfrak{b} \subset \mathfrak{a}\}$$

vii) The **annihilator** of an ideal $\mathfrak{a}$; $\mathrm{Ann}(\mathfrak{a}) = (0 : \mathfrak{a})$ and of element $a \in A$; $\mathrm{Ann}(a) = (0 : (a))$.

Warning: Notice that $\cup_{i \in I} \mathfrak{a}_i$ in general is not an ideal. But if the ideals are nested, i.e.

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \subseteq \ldots$$

then the union is an ideal.

Example

i) *Let* $p, q \in \mathbb{Z}$ *be two primes. Then*

$$(p) \cap (q) = (pq) \quad (p) + (q) = \mathbb{Z}$$

ii) *In* $\mathbb{Z}/(40)$ *one has* $Ann(2) = (20)$ *and* $Ann(8) = (5)$.

iii) *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, let* $f \in \big((xy, y^2) : (x, y)\big)$ *i.e.* $fx = gxy + hy^2$ *with* $g, h \in \mathbb{C}[x, y]$ *Since* x *divides* fx *and* gxy, *it divides* hy^2 *as well, i,e.* $h = h'x$, *and by cancelling* x, *we get* $f = gy + h'y \in (y)$.

A map of rings $\phi : A \to B$ induces:

i) Contravariant map $\phi^{-1} : \mathscr{I}(B) \to \mathscr{I}(A)$ given by $\mathfrak{b} \mapsto \phi^{-1}(\mathfrak{b})$ (**Contraction**).

ii) Covariant map $\phi^e : \mathscr{I}(A) \to \mathscr{I}(B)$ given by $\phi^e(\mathfrak{a}) = \phi(\mathfrak{a})B$ (**Extension**).

Lemma

i) $\phi^{-1}(\mathfrak{a}) \cap \phi^{-1}(\mathfrak{b}) = \phi^{-1}(\mathfrak{a} \cap \mathfrak{b})$

ii) $\phi^{-1}(\mathfrak{a}) + \phi^{-1}(\mathfrak{b}) \subseteq \phi^{-1}(\mathfrak{a} + \mathfrak{b})$

iii) $\phi^{-1}(\mathfrak{a}) \cdot \phi^{-1}(\mathfrak{b}) \subseteq \phi^{-1}(\mathfrak{a} \cdot \mathfrak{b})$

Lemma

i) $\phi^e(\mathfrak{a} \cdot \mathfrak{b}) = \phi^e(\mathfrak{a}) \cdot \phi^e(\mathfrak{b})$

ii) $\phi^e(\mathfrak{a} + \mathfrak{b}) = \phi^e(\mathfrak{a}) + \phi^e(\mathfrak{b})$

iii) $\phi^e(\mathfrak{a} \cap \mathfrak{b}) \subseteq \phi^e(\mathfrak{a}) \cap \phi^e(\mathfrak{b})$

Proof. [Pullback i)] Let $x \in \phi^{-1}(\mathfrak{a}) \cap \phi^{-1}(\mathfrak{b})$. Then $\phi(x) \in \mathfrak{a}$ and $\phi(x) \in \mathfrak{b}$, and $\phi(x) \in \mathfrak{a} \cap \mathfrak{b}$. Thus $x \in \phi^{-1}(\mathfrak{a} \cap \mathfrak{b})$. The reversed argument gives the other inclusion. □

Proof. [Pushout ii)] The inclusion $\phi^e(\mathfrak{a}+\mathfrak{b}) \subseteq \phi^e(\mathfrak{a}) + \phi^e(\mathfrak{b})$ is obvious. Let

$$y_1 + y_2 = \sum \phi(x_{1i}) b_i + \sum \phi(x_{2j}) b_j \in \phi(\mathfrak{a})B + \phi(\mathfrak{b})B$$

with $x_{1i} \in \mathfrak{a}$ and $x_{2j} \in \mathfrak{b}$. It follows that $x_{1i} + 0, 0 + x_{2i} \in \mathfrak{a} + \mathfrak{b}$ and

$$y_1 + y_2 = \sum \phi(x_{1i} + 0) b_i + \sum \phi(0 + x_{2i}) b_j \in \phi^e(\mathfrak{a} + \mathfrak{b})$$

□

Example

A simple example of strict inclusion in the previous lemma ii) is the diagonal map $\delta : A \to A \times A$ *sending* $a \mapsto (a, a)$. *The two ideals* $\mathfrak{b} = (0) \times A$ *and* $\mathfrak{b}' = A \times (0)$ *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. *Thus* $\phi^{-1}(\mathfrak{b}) + \phi^{-1}(\mathfrak{b}') \neq phi^{-1}(\mathfrak{b} + \mathfrak{b}')$.

Lemma

Let $\phi : A \to B$ be a ring homomorphism. The kernel of ϕ;

$$\ker(\phi) = \{a \in A \,|\, \phi(a) = 0\}$$

is an ideal of A.

Proof. Let $x \in \ker(\phi)$ and $a \in A$. Then

$$\phi(ax) = \phi(a)\phi(x) = \phi(a) \cdot 0 = 0$$

□

Lemma

For an ideal $\mathfrak{a}$ of A, the residue class group $A/\mathfrak{a}$ has a natural structure as a ring.

The projection of an element $a \in A$ into the quotient will often be denoted $\overline{a}$.

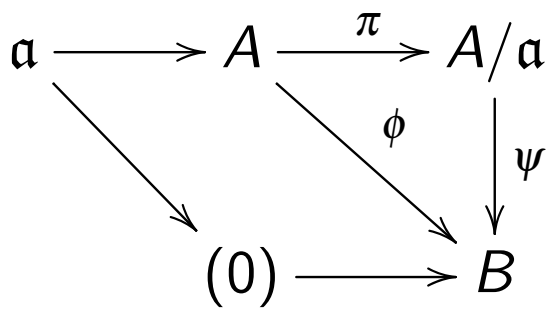
August, 27, 2020

We continue to study ideals in general, moving on to prime and maximal ideals. Many of the results are rather technical, but later on they will turn out to be very useful to understand the more geometrical properties of the so-called prime spectrum of a ring.

2.2-2.3

Theorem (The Factorization Theorem)

Given an ideal $\mathfrak{a}$ in the ring A. A map of rings $\phi : A \to B$ vanishes on $\mathfrak{a}$ if and only if it factors through the quotient map $\pi : A \to A/\mathfrak{a}$. The factorization is unique.



Proposition (Ideals in quotients)

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

i) *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 $\mathfrak{c} \subset A/\mathfrak{a}$ is of this form for a unique ideal $\mathfrak{b}$, indeed one has $\mathfrak{c} = \pi^{-1}(\mathfrak{c})/\mathfrak{a}$, i.e. $\mathfrak{b} = \pi^{-1}(\mathfrak{c})$.*

ii) *For every ideal $\mathfrak{b}$ in A it holds true that $\pi^{-1}(\pi(\mathfrak{b})) = \mathfrak{b} + \mathfrak{a}$;*

iii) *An ideal is mapped to the zero ideal in $A/\mathfrak{a}$ if and only if it is contained in $\mathfrak{a}$.*

.

Alternative formulation:

$$\{\mathfrak{b} \in \mathscr{I}(A) \,|\, \mathfrak{a} \subseteq \mathfrak{b}\} \overset{1-1}{\longleftrightarrow} \mathscr{I}(A/\mathfrak{a})$$

Theorem (The Isomorphism Theorem)

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in A. Then the following two isomorphism relations hold, where in the second it is assumed that $\mathfrak{a} \subseteq \mathfrak{b}$:

i) $\mathfrak{b}/\mathfrak{b} \cap \mathfrak{a} \simeq (\mathfrak{a} + \mathfrak{b})/\mathfrak{a}$;

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

Proof. i) The composition map

$$\mathfrak{b} \to \mathfrak{a} + \mathfrak{b} \to (\mathfrak{a} + \mathfrak{b})/\mathfrak{a}$$

is surjective since $a + b \equiv b$ (modulo $\mathfrak{a}$). The kernel is $\mathfrak{b} \cap \mathfrak{a}$.
ii) When $\mathfrak{a} \subseteq \mathfrak{b}$ the map $A/\mathfrak{a} \to A/\mathfrak{b}$ is surjective, and the kernel is $\mathfrak{b}/\mathfrak{a}$. □

Example (Strict inclusion in Pullback iii), version 1)

Let

$$\phi : k[z] \to k[x,y,z]/(z-xy) = B$$

be the inclusion and let $\mathfrak{c} \subseteq B$ *be an ideal. Then* $\phi^{-1}(\mathfrak{c}) = \mathfrak{c} \cap k[z]$.
Let

$$\mathfrak{a} = (x)B \quad \textit{and} \quad \mathfrak{b} = (y)B$$

Since $z = xy$ *it holds that* $z \in (x)B = \mathfrak{a}$ *and* $z \in (y)B = \mathfrak{b}$ *and* $\mathfrak{a} \cap (z) = \mathfrak{a} \cap k[z] = \mathfrak{b} \cap k[z] = (z)$ *and therefore* $(\mathfrak{a} \cap k[z]) \cdot (\mathfrak{b} \cap k[z]) = (z^2)$. *On the other hand* $\mathfrak{ab} = (xy)B = (z)B$, *so* $(\mathfrak{ab}) \cap k[z] = (z)$. *Hence* $\phi^{-1}(\mathfrak{a}) \cdot \phi^{-1}(\mathfrak{b}) \subsetneq \phi^{-1}(\mathfrak{ab})$.

Example (Strict inclusion in Pullback iii), version 2)

Let

$$\phi : k[z] \to k[x,y]$$

be the inclusion $z \mapsto xy$ *and let* $\mathfrak{c} \subseteq k[x,y]$ *be an ideal. Then* $\phi^{-1}(\mathfrak{c}) = \mathfrak{c} \cap k[z = xy]$. *Let*

$$\mathfrak{a} = (x)k[x,y] \quad \textit{and} \quad \mathfrak{b} = (y)k[x,y]$$

Since $z \mapsto xy$ *it holds that* $\phi(z) \in (x)k[x,y] = \mathfrak{a}$ *and* $\phi(z) \in (y)k[x,y] = \mathfrak{b}$ *and* $\mathfrak{a} \cap (z) = \mathfrak{a} \cap k[z] = \mathfrak{b} \cap k[z] = (z)$ *and therefore* $(\mathfrak{a} \cap k[z]) \cdot (\mathfrak{b} \cap k[z]) = (z^2)$. *On the other hand* $\mathfrak{a}\mathfrak{b} = (xy)k[x,y] = (z)k[x,y]$, *so* $(\mathfrak{a}\mathfrak{b}) \cap k[z] = (z)$. *Hence* $\phi^{-1}(\mathfrak{a}) \cdot \phi^{-1}(\mathfrak{b}) \subsetneq \phi^{-1}(\mathfrak{a}\mathfrak{b})$.

Definition (Prime ideal)

A **prime ideal** $\mathfrak{p} \subset A$ *is a proper ideal such that if* $ab \in \mathfrak{p}$*, then either* $a \in \mathfrak{p}$ *or* $b \in \mathfrak{p}$*.*

If a prime number p divides a composite number $ab \in \mathbb{Z}$, then p divides a or p divides b.

Definition (Maximal ideal)

A **maximal ideal** $\mathfrak{m}$ *is an ideal which is maximal amongst proper ideals of* A*, that is if* $\mathfrak{m} \subseteq \mathfrak{a} \neq A$ *for an ideal* $\mathfrak{a}$*, then* $\mathfrak{m} = \mathfrak{a}$*.*

Proposition

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. The quotient $A/\mathfrak{a}$ is a domain iff $\overline{ab} = 0$ implies $\overline{a} = 0$ or $\overline{b} = 0$, i.e. $ab \in \mathfrak{a}$ iff $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$. The second statement follows from the ideal structure of a quotient ring. □

Example

i) *The kernel of the evaluation map* $k[x_1, \ldots, x_n] \to k$ *is a maximal ideal.*

ii) *In the ring* $k[x, y]$ *the ideal* (x) *is prime, but not maximal. In fact,* $k[x, y]/(x) \simeq k[y]$ *which is a domain, but not a field.*

iii) *If* k *is algebraically closed (e.g.* $k = \mathbb{C}$*), the maximal ideals in the ring* $k[x, y]$ *are given by* $\mathfrak{m} = (x - a, y - b)$*, where* $a, b \in k$*.*

Proposition

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

Proof. Using the fact that a field is a domain and the ideal structure of quotient rings, the result follows immediately. □

Proposition (Prime inclusion property)

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 for contradiction that $\mathfrak{a}, \mathfrak{b} \not\subset \mathfrak{p}$. Pick $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ outside $\mathfrak{p}$. By assumption $ab \in \mathfrak{p}$. By the prime ideal property either a or b is in $\mathfrak{p}$. Contradiction. □

If a prime number p divides a composite number $ab \in \mathbb{Z}$, then p divides a or p divides b.

Lemma

Let $\phi : A \to B$ be a ring homomorphism and $\mathfrak{q} \subset B$ a prime ideal. Then $\phi^{-1}(\mathfrak{q})$ is a prime ideal of A.

Proof. Let $ab \in \phi^{-1}(\mathfrak{q})$. Then $\phi(ab) = \phi(a)\phi(b) \in \mathfrak{q}$, and it follows that $\phi(a) \in \mathfrak{q}$ or $\phi(b) \in \mathfrak{q}$, i.e. $a \in \phi^{-1}(\mathfrak{q})$ or $b \in \phi^{-1}(\mathfrak{q})$, □

Proposition (Prime ideals in quotients)

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 $\mathfrak{m}/\mathfrak{a}$ with $\mathfrak{m}$ a maximal ideal in A likewise containing $\mathfrak{a}$.

Proof. Follows from the Ideals in quotient Proposition. □

Lemma (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 $\bigcup_j \mathfrak{p}_j$, then $\mathfrak{a}$ is contained in at least one of the $\mathfrak{p}_j$'s.

The reason for the name of the lemma is the opposite formulation; If $\mathfrak{a} \not\subset \mathfrak{p}_i$ for all i, then there is an $x \in \mathfrak{a}$ such that $x \notin \mathfrak{p}_i$ for all i.

Proof.

1) We can assume that the family of prime ideals is irredundant; none of the prime ideals are contained in the union of the others.
2) For each j pick $y_j \in \mathfrak{p}_j$, but $y_j \notin \mathfrak{p}_i$, $i \neq j$.
3) Suppose for a contradiction that $\mathfrak{a}$ is not contained in any of the prime ideals. Let $x_j \in \mathfrak{a} \setminus \mathfrak{p}_j$.
4) The element $z_j = x_j \prod_{i \neq j} y_i \in \mathfrak{a} \cap \mathfrak{p}_i$ for $i \neq j$, but not in $\mathfrak{p}_j$.
5) Then $z = z_1 + \cdots + z_r \in \mathfrak{a}$, but $z \notin \mathfrak{p}_i$ for any i, contradicting the fact that $\mathfrak{a}$ is contained in the union of the primes.

□

Lemma

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. We have $\mathfrak{p}_i \subseteq \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_s$ and by the Prime avoidance lemma $\mathfrak{p}_i \subseteq \mathfrak{q}_j$ for some j. By symmetry $\mathfrak{q}_j \subseteq \mathfrak{p}_k$, thus

$$\mathfrak{p}_i \subseteq \mathfrak{q}_j \subseteq \mathfrak{p}_k$$

and by assumption of non-trivial inclusion relations $i = k$ and $\mathfrak{p}_i = \mathfrak{q}_j$. □

Lemma

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. We have $\mathfrak{p}_i \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ and by Prime inclusion property $\mathfrak{p}_i \subseteq \mathfrak{q}_j$ for some j. By symmetry $\mathfrak{q}_j \subseteq \mathfrak{p}_k$, thus

$$\mathfrak{p}_i \subseteq \mathfrak{q}_j \subseteq \mathfrak{p}_k$$

and by assumption of non-trivial inclusion relations $i = k$ and $\mathfrak{p}_i = \mathfrak{q}_j$. □

September, 2, 2020

We move to the existence of maximal ideals. This fact is based on an axiom called Zorn's lemma. Next we define the radical of an ideal and the concept of a local ring. Finally we prove a general algebraic version of the Chinese remainder theorem.

2.4-2.7

Theorem (Zorn's lemma)

Let Σ be a partially ordered set in which every chain is bounded above. Then Σ possesses a maximal element.

Zorn's lemma is known to be equivalent to the **Axiom of Choice**:

Axiom (Axiom of choice)

For any family X of nonempty sets, it is possible to chose an element from each member A of X.

and also to the **well-ordering principle**:

Axiom (Well-ordering principle)

Every set can be well-ordered.

(See https://www.mn.uio.no/math/tjenester/kunnskap/kompendier/acwozl.pdf for a proof)

Theorem (Existence of maximal ideals)

Let A be a ring different from the null-ring. Every proper ideal $\mathfrak{a}$ in A is contained in a maximal ideal. In particular, there is at least one maximal ideal in every ring.

Proof. The set of proper ideals in A forms a non-empty partially ordered set. Let

$$\mathfrak{a} \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_r \subseteq \ldots$$

be a chain of ideals in A containing $\mathfrak{a}$. The union $\bigcup_i \mathfrak{a}_i$ is a proper ideal containing $\mathfrak{a}$ and an upper bound for the chain. By Zorn's lemma the set of ideals containing $\mathfrak{a}$ has a maximal element, i.e. a maximal ideal. For the last statement, let $\mathfrak{a} = (0)$. □

There is a slightly more general version of the Existence of maximal ideals Theorem. We consider proper ideals to be ideals not meeting the set $S = \{1\}$. In the more general version the set S is an arbitrary subset of A.

Theorem (The Fundamental Existence Theorem for Ideals)

Assume given a ring A, an ideal $\mathfrak{a}$ in A and a subset S not meeting $\mathfrak{a}$. Then $\mathfrak{a}$ is contained in an ideal $\mathfrak{b}$ maximal subject to the condition $S \cap \mathfrak{b} = \emptyset$. If S is multiplicatively closed, the ideal $\mathfrak{b}$ will be a prime ideal.

Proof. [that $\mathfrak{b}$ is prime] Suppose $xy \in \mathfrak{b}$, but $x, y \notin \mathfrak{b}$. By maximality of $\mathfrak{b}$ $(\mathfrak{b}, x) \cap S \neq \emptyset$ and $(\mathfrak{b}, y) \cap S \neq \emptyset$. Thus there are $a, b \in \mathfrak{b}$ and $\alpha, \beta \in A$ such that $a + \alpha x, b + \beta y \in S$. It follows by multiplicativity of S that

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

But $ab + a\beta y + b\alpha x + \alpha\beta xy \in \mathfrak{b}$, contradicting the fact that $S \cap \mathfrak{b} = \emptyset$. □

Definition

Let $\mathfrak{a}$ be an ideal in the ring A. The radical $\sqrt{\mathfrak{a}}$ is the set

$$\sqrt{\mathfrak{a}} = \{a \in A \,|\, \exists m \in \mathbb{Z}_+ \text{ such that } a^m \in \mathfrak{a}\}$$

Lemma

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

Proof. If $a^u \in \mathfrak{a}$ and $b^v \in \mathfrak{a}$, then $(a+b)^{u+v} \in \mathfrak{a}$ and $(ra)^u \in \mathfrak{a}$ □

Definition

An ideal $\mathfrak{a}$ which satisfies $\sqrt{\mathfrak{a}} = \mathfrak{a}$ is called a **radical** *ideal.*

Corollary

The set of nilpotent elements in A form an ideal, called the **nilradical** *of A.*

Proposition

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

Example

i) *The radical of the ideal $(p^n) \subset \mathbb{Z}$ is (p).*

ii) *The radical of the ideal $(x^2, y^3) \subset k[x, y]$ is the ideal (x, y).*

Proposition (The radical as intersection of primes)

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,

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subset \mathfrak{p}} \mathfrak{p}$$

Proof. Let $\mathfrak{a} \subseteq \mathfrak{p}$. If $a \in \sqrt{\mathfrak{a}}$, then $a^m \in \mathfrak{a}$ for some m, i.e. $a^m \in \mathfrak{p}$, and by the prime ideal property it follows that $a \in \mathfrak{p}$. Thus $\sqrt{\mathfrak{a}} \subseteq \bigcap_{\mathfrak{a} \subset \mathfrak{p}} \mathfrak{p}$.

For the other inclusion, suppose $a \notin \sqrt{\mathfrak{a}}$. Apply the Fundamental Extension Theorem with $S = \{a^n \mid n \in \mathbb{N}\}$, and observe that $S \cap \mathfrak{a} = \emptyset$. The conclusion of the theorem gives a prime ideal $\mathfrak{p}$, not meeting S, i.e. $a \notin \mathfrak{p}$. □

Corollary

The set of nilpotent elements in A equals the intersection of all prime ideals in A; that is $\sqrt{(0)} = \bigcap_{\mathfrak{p}\ prime} \mathfrak{p}$

Lemma

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

Proof. Since the collection is finite it is enough to prove that

$$\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}}$$

The inclusion $\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} \supseteq \sqrt{\mathfrak{a} \cap \mathfrak{b}}$ is obvious. For the other inclusion, observe that if $x \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$, then $x^r \in \mathfrak{a}$ and $x^s \in \mathfrak{b}$ for some numbers r and s. Let m be maximum of r and s. Then $x^m \in \mathfrak{a} \cap \mathfrak{b}$ and $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$.

Example

The radical respects finite intersections, but for infinite intersections it is no more true. Consider the sequence

$$\mathbb{Z} \supset (p) \supset (p^2) \supset \cdots \supset (p^n) \supset \ldots$$

The intersection $\bigcap_n (p^n) = (0)$, *and consequently* $\sqrt{\bigcap_n (p^n)} = (0)$. *But* $\sqrt{(p^n)} = (p)$ *and* $\bigcap_n \sqrt{(p^n)} = (p) \neq \sqrt{\bigcap_n (p^n)}$,

Definition

A **local ring** *is a ring with only one maximal ideal.*

Proposition

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

i) *A is a local ring with maximal ideal $\mathfrak{m}$;*

ii) *The group of units and the complement of $\mathfrak{m}$ coincide; that is, $A^* = A \setminus \mathfrak{a}$;*

iii) *The ideal $\mathfrak{m}$ is maximal and consists of elements a such that $1 + a$ is invertible.*

Proof.

i) $\Rightarrow$ ii) Suppose $a \notin \mathfrak{m}$ is a non-unit. Then a is contained in a maximal ideal, i.e. $a \in \mathfrak{m}$, which is a contradiction.

ii) $\Rightarrow$ iii) Since any element outside of $\mathfrak{m}$ is a unit, the ideal has to be maximal. Furthermore, if $a \in \mathfrak{m}$, then $a+1 \notin \mathfrak{m}$, hence a unit.

iii) $\Rightarrow$ i) Suppose A is not local and let a be a non-unit outside $\mathfrak{m}$. Maximality of $\mathfrak{m}$ gives $\mathfrak{m}+(a) = A$, i.e. $a = 1+m$ for some $m \in \mathfrak{m}$, thus invertible, contradicting the fact that a is a non-unit. $\square$

Definition

The **Jacobson radical** *in a ring A is the intersection of all maximal ideals, that is*

$$J(A) = \bigcap_{\mathfrak{m}\ max} \mathfrak{m}$$

Proposition

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. Let $a \in J(A)$. If $1+xa$ is a non-unit for some $x \in A$, it will be an element of some maksimal ideal, which also contains xa. But then 1 is in the same maximal ideal. Contradiction.

Let $a \in A$ have the property that $1+xa$ is invertible for all $x \in A$, and suppose a is outside some maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}+(a) = A$, i.e. $1 = m+ax$ for some $m \in \mathfrak{m}$ and $x \in A$ and it follows that m is invertible, a contradiction. □

Example

Let p be a prime number and let $\mathbb{Z}_{(p)}$ be the ring of rational numbers expressible as $\frac{n}{m}$ where the denominator m is relatively prime to p. Then $\mathbb{Z}_{(p)}$ is a local ring whose maximal ideal is generated by (p). Even more is true, the only ideals in $\mathbb{Z}_{(p)}$ are the principal ideals (p^ν); indeed, every rational number lying in $\mathbb{Z}_{(p)}$ may be written as $\frac{p^\nu}{m}$ with $\nu \geq 0$ and neither n nor m having p as factor. And among these ideals (p) contains all the others.

Example

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;*

$$\mathfrak{m}_a = (x_1 - a_1, \ldots, x_r - a_r)$$

It follows that the Jacobson radical of $\mathbb{C}[x_1, \ldots, x_r]$ *equals* (0).

Example

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* $A = \{\frac{n}{m} \mid n, m \in \mathbb{Z}, (m, pq) = 1\}$. *The principal ideals* (p) *and* (q) *are the only two maximal ideals in* A, *and* $J(A) = (p) \cap (q) = (pq)$.

Proposition

The ideals of $A = \prod_{1 \le i \le r} A_i$ *are all of the form* $\prod_{1 \le i \le r} \mathfrak{a}_i$ *where each* $\mathfrak{a}_i$ *is an ideal in* A_i*. An ideal* $\mathfrak{p} \subset A$ *is prime if and only if* $\mathfrak{p}_i = A_i$ *for all but one index* i_0 *and* $\mathfrak{p}_{i_0}$ *is a prime ideal.*

Proof. Let $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ be the i'th **standard idempotent**.
Then $A_i = e_i A$, and $\mathfrak{a}_i = e_i \mathfrak{a}$ is an ideal in A_i, and since $\sum e_i = 1$ we have $\mathfrak{a} = \sum e_i \mathfrak{a}_i$.
The map $\rho : A \to \prod_{1 \le i \le r} A_i \mathfrak{a}_i$ is obviously surjective. If $x = \sum e_i x_i$ is in the kernel of ρ, then $e_j x = \sum e_j e_i x_i = x_j \in \mathfrak{a}_j$ and $x \in \sum e_i \mathfrak{a}_i = \mathfrak{a}$.
The statement about the primes follows from the fact that if at least two standard idempotens e_i and e_j are non-zero in the quotient $A/\mathfrak{a}$, and of course $e_i e_j = 0$, the ideal $\mathfrak{a}$ is not prime. □

Theorem (The Chinese Remainder Theorem)

Let A be a ring and let $\{a_i\}_{1\leq i\leq r}$ be a finite collection of pairwise comaximal ideals. Then

$$A/\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r \simeq \prod_{1\leq i\leq r} A/\mathfrak{a}_i$$

Proof. Composing the diagonal map with taking residues gives a map $A \to \prod A/\mathfrak{a}_i$ with the intersection of all the ideals as the kernel. Thus the map $A/\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r \to \prod A/\mathfrak{a}_i$ is injective.
To show that the map is surjective we shall construct an element $a_i \in A$, congruent to 1 modulo $\mathfrak{a}_i$ and congruent to 0 modulo $\mathfrak{a}_j$, $j \neq i$. Since the ideals are pairwise comaximal, we can find $c_{ij} \in \mathfrak{a}_j$ and $c_{ji} \in \mathfrak{a}_i$ such that $1 = c_{ij} + c_{ji}$. Thus c_{ij} is congruent to 1 modulo $\mathfrak{a}_i$. Let

$$a_i = \prod_{j\neq i} c_{ij}$$

By construction $a_i \in \mathfrak{a}_j$ for all $j \neq i$, and a_i is congruent to 1 modulo $\mathfrak{a}_i$.

Definition

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

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

of additive subgroups R_ν *subject to the rule* $R_\nu \cdot R_\mu \subseteq R_{\nu+\mu}$.

b) *Elements from the subgroup* R_ν *are said to be* **homogenous of degree** ν.

c) *An ideal* $\mathfrak{a}$ *is a* **homogenous ideal** *if* $\mathfrak{a} = \bigoplus(\mathfrak{a} \cap R_\nu)$

Proposition

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

i) *The ideal a is homogenous;*

ii) *All homogenous components of elements in $\mathfrak{a}$ belong to $\mathfrak{a}$;*

iii) *The ideal $\mathfrak{a}$ may be generated by homogenous elements.*

Proposition

Let R be a graded ring and $\mathfrak{a}$ a homogeneous ideal. Then the quotient $R/\mathfrak{a}$ is a graded ring whose homogeneous components are given as $(R/\mathfrak{a})_v = R_v/\mathfrak{a}_v$

September, 3, 2020

We define the prime spectrum of a ring. The prime spectrum is the basis of algebraic geometry, and it is equipped with a topology, the Zariski topology. We give some basic definitions and propositions.

2.8-

Definition

a) *The set of prime ideals of a ring A is called the* **prime spectrum** *of the ring, denoted $Spec(A)$.*

b) *$Spec(A)$ is endowed with a topology, called the* **Zariski topology**, *defined by the closed subsets;*

$$V(\mathfrak{a}) = \{\mathfrak{p} \subset A \,|\, \mathfrak{p} \; prime \; , \mathfrak{p} \supseteq \mathfrak{a}\}$$

for an ideal $\mathfrak{a}$.

Notice that we can define $V(S)$ for an arbitrary set S, by putting $V(S) = V(I(S))$, where $I(S)$ is the smallest ideal which contains S.

Let X be any set and let τ be a collection of subsets of X. Then τ is a topology on X if and only if:

i) Any intersection of arbitrary many closed sets of X under τ is a closed set of X under τ.

ii) The union of any finite number of closed sets of X under τ is a closed set of X under τ.

iii) The whole space X and the empty set $\emptyset$ are closed sets of X under τ.

Proposition

Let A be a ring.

i) $V(0) = Spec(A)$ *and* $V(1) = \emptyset$;

ii) *For any ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *in* A *it holds true that* $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$;

iii) *For any family* $\{\mathfrak{a}_i\}_{i \in I}$ *of ideals one has* $V(\Sigma_{i \in I} \mathfrak{a}_i) = \cap_{i \in I} V(\mathfrak{a}_i)$;

iv) *If* $\mathfrak{a} \subset \mathfrak{b}$, *then* $V(\mathfrak{b}) \subset V(\mathfrak{a})$

v) $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$

Proof.

i) Every prime ideal contains 0, and no proper ideal contains 1.

ii) The Prime inclusion property says that if $\mathfrak{a}$ and $\mathfrak{b}$ are 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 $\mathfrak{p}$. Thus $V(\mathfrak{a}) \cup V(\mathfrak{b}) \supseteq V(\mathfrak{ab})$. The other inclusion is obvious.

iii) The inclusion $V(\Sigma_{i \in I} \mathfrak{a}_i) \supseteq \cap_{i \in I} V(\mathfrak{a}_i)$ is obvious. The other inclusion follows from the fact that $\mathfrak{a}_i \subseteq \Sigma_{i \in I} \mathfrak{a}_i$

iv) Obvious.

v) The inclusion $\sqrt{\mathfrak{a}} \subseteq \mathfrak{a}$ gives one inclusion (a consequence of iv) above. The other inclusion follows from the defining property of a prime ideal.

□

Lemma

The closed points in $Spec(A)$ are the maximal ideals.

Proof. 1) The points of the prime spectrum are the prime ideals, and the closed sets are all primes that contain a given ideal. So a prime ideal $\mathfrak{q}$ is a closed set if

$$\{\mathfrak{q}\} = V(\mathfrak{a})$$

for some ideal $\mathfrak{a}$. Thus $\mathfrak{q} \supseteq \mathfrak{a}$ 2) We must show that $\mathfrak{q}$ is maximal. We know that $\mathfrak{q}$ is contained in a maximal ideal (or equal to), say $\mathfrak{m}$. Consequently

$$\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{m}$$

and it follows that $\mathfrak{m} \in V(\mathfrak{a}) = \{\mathfrak{q}\}$. Thus $\mathfrak{q} = \mathfrak{m}$ and $\mathfrak{q}$ is maximal ideal. □

Lemma

Let $\phi : A \to B$ be a ring homomorphism and $\mathfrak{q} \subset B$ a prime ideal. Then $\phi^{-1}(\mathfrak{q})$ is a prime ideal of A.

Definition

Let $\phi : A \to B$ be a ring homomorphism. Define $\tilde{\phi} : Spec(B) \to Spec(A)$ by

$$\tilde{\phi}(\mathfrak{p}) = \phi^{-1}(\mathfrak{p})$$

Proposition

The map $\tilde{\phi}$ is continuous.

Proof. We have

$$\tilde{\phi}^{-1}(V(\mathfrak{a})) = V(\phi(\mathfrak{a}))$$

□

Proposition (Prime ideals in quotients)

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 $\mathfrak{a}$, i.e.

$$Spec(A/\mathfrak{a}) = V(\mathfrak{a})$$

Proposition

Let $\tilde{\phi} : Spec(B) \to Spec(A)$ be induced by $\phi : A \to B$. Then the invers 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 $\mathfrak{p}$ is naturally homeomorphic to $Spec(B/\mathfrak{p}B)$.

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \end{array}$$

$$\begin{array}{ccccc} \mathrm{Spec}(A) & \xleftarrow{\tilde{\phi}} & \mathrm{Spec}(B) & & \\ \uparrow & & \uparrow & & \\ V(\mathfrak{a}) & \longleftarrow & \tilde{\phi}^{-1}(V(\mathfrak{a})) & \xrightarrow{\simeq} & \mathrm{Spec}(B/\mathfrak{a}B) \end{array}$$

Example

The direct product of two fields $A = k \times k'$ has two prime ideals $(0) \times k'$ and $k \times (0)$, i.e. $Spec(A)$ has two closed points with the discret topology.

Example

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), where $(0) \subset (p)$.

We consider the $\mathbb{C}$-algebra $A = \mathbb{C}[y]$.

- A is a PID, every non-zero prime is generated by an irreducible polynomial.
- By the fundamental theorem of algebra the irreducible polynomials are linear.
- It follows that $\mathrm{Spec}(A) = (0) \cup \left(\bigcup_{b \in \mathbb{C}} (y - b) \right)$.
- All primes except the zero ideal are maximal, i.e. the closed points of $\mathrm{Spec}(A)$ are in 1-1 correspondence with points of $\mathbb{C}$.

Next we consider the $\mathbb{C}$-algebra $B = \mathbb{C}[x,y]/(y-x^2) \simeq \mathbb{C}[x]$.

* We have $\mathrm{Spec}(B) = (0) \cup \left(\bigcup_{a \in \mathbb{C}} (x-a) \right)$.
* All primes except the zero ideal are maximal, i.e. the closed points of $\mathrm{Spec}(B)$ are in 1-1 correspondence with points of $\mathbb{C}$.
* By the isomorphism above the maximal ideals are given by (a, a^2) for $a \in \mathbb{C}$, i.e. the real part is precisely the parabola $y = x^2$, and the isomorphism corresponds to the projection onto the x-axis.

There is a natural ring homomorphism

$$\phi : A = \mathbb{C}[y] \to \mathbb{C}[x,y]/(y-x^2) = B$$

* The induced map $\tilde{\phi} : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is given by $(a, a^2) \mapsto a^2$
* For a prime ideal $\mathfrak{b} = (y-b) \subset A$ the fiber $\tilde{\phi}^{-1}(\mathfrak{b})$ is naturally homeomorphic to $\mathrm{Spec}(B/\mathfrak{b}B)$.
* We have

$$B/\mathfrak{b}B = \mathbb{C}[x]/(x^2-b^2) = \mathbb{C}[x]/((x-b)(x+b))$$

* Notive that

$$((x-b)(x+b)) = (x-b)\cdot(x+b) = (x-b)\cap(x+b)$$

The Chinese remainder Theorem for two maximal ideals:

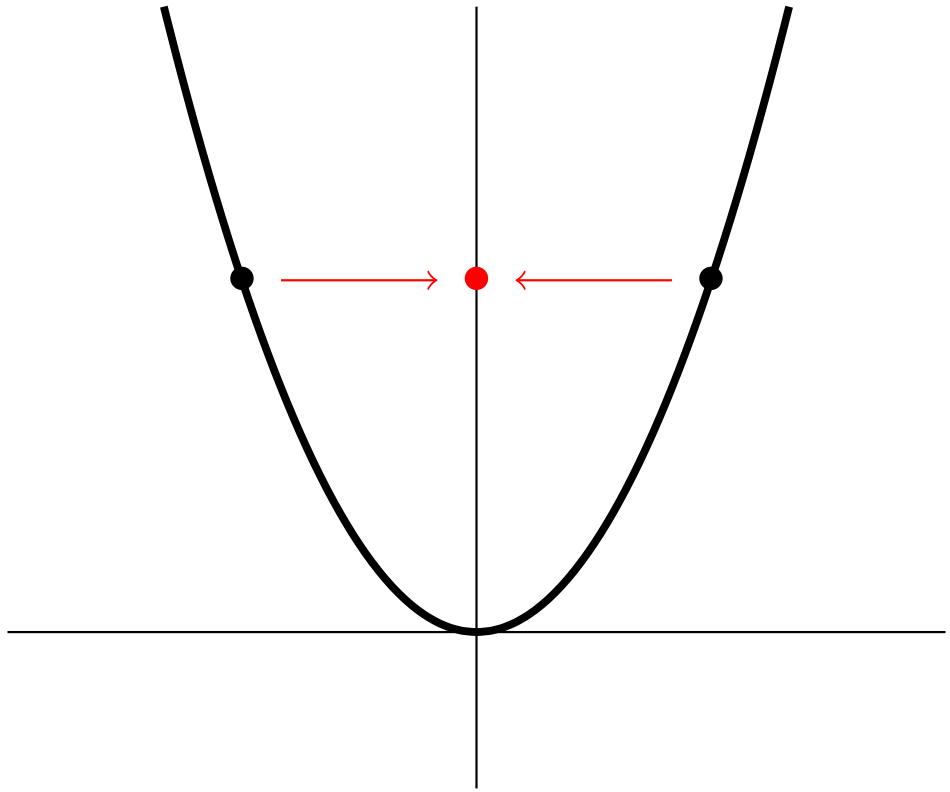
Let $\mathfrak{a}, \mathfrak{b} \subset A$ be two maximal ideals, i.e. a consequence is that $\mathfrak{a} + \mathfrak{b} = A$. The Chinese remainder Theorem says that

$$A/\mathfrak{a} \cap \mathfrak{b} \simeq A/\mathfrak{a} \times A/\mathfrak{b}$$

Thus we get

$$B/\mathfrak{b}B = \mathbb{C}[x]/((x-b)(x+b)) \simeq \mathbb{C}[x]/(x-b) \times \mathbb{C}[x]/(x+b) \simeq \mathbb{C} \times \mathbb{C}$$

The prime ideals of the direct product ring $A_1 \times A_2$ are the union of the prime ideals of the the two rings A_1 and A_2. It follows that the fiber described above consists of two distinct closed points (except for $b = 0$).



The figur illustrates the map

$$\phi^* : \mathrm{Spec}(\mathbb{C}[x,y]/(y-x^2)) \to \mathrm{Spec}(\mathbb{C}[y])$$