

UiO : Department of Mathematics
University of Oslo

MAT2200 Spring 2023

Revision on rings

Rings

A **ring** is a set R equipped with two binary operations, on this slide written $+$ and $*$, which satisfy

1. $(R, +)$ is an abelian group
2. $*$ is an associative operation: For $a, b, c \in R$

$$a * (b * c) = (a * b) * c.$$

3. The left and right distributive laws hold: For $a, b, c \in R$

$$a * (b + c) = a * b + a * c$$
$$(b + c) * a = b * a + c * a$$

After this slide we always write ab instead of $a * b$.

Basic properties/notation of rings

Let R be a ring, so in particular $(R, +)$ is an abelian group.

Notation

- Write $0 \in R$ for additive identity.
- Given $a \in R$, write $-a$ for additive inverse
- Given integer $n > 0$ and $a \in R$, let

$$n \cdot a = \overbrace{a + \cdots + a}^{n}, \quad (-n) \cdot a = \overbrace{(-a) + \cdots + (-a)}^{n}, \quad 0 \cdot a = 0$$

Basic properties

- If $a \in R$, we have $0a = a0 = 0$.
- If $a, b \in R$, we have $(-a)b = a(-b) = -(ab)$
- If $a, b \in R$, we have $(-a)(-b) = ab$.

Examples

- With the usual operations of addition and multiplication, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are rings.
- With the usual operation of matrix addition and multiplication

$$M_n(\mathbb{R}) = \{(n \times n)\text{-matrices}\}$$

  forms a ring.
- With the usual operation of addition and multiplication of functions,

$$C(\mathbb{R}) = \{\text{functions } f : \mathbb{R} \to \mathbb{R}\}$$

  forms a ring.

Example: Integers modulo n

Let $n > 0$ be an integer. Given integers i, j, we say i and j are **congruent modulo** n and write

$$i \equiv j \pmod{n}$$

if i and j have the same remainder upon division by n.
The set of **integers modulo** n,

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

forms a ring, with addition $+_n$ and multiplication $*_n$ defined by

$$a +_n b = c \text{ if } a + b \equiv c \pmod{n}$$

and

$$a *_n b = c \text{ if } ab \equiv c \pmod{n}$$

Special properties of rings, I: Unity

Let R be a ring.

- A multiplicative identity, that is an element $a \in R$ such that

$$ab = ba = b \qquad \forall b \in R$$

  is called **unity**.
- A unity of a ring is unique if it exists, and denoted $1 \in R$.
- If such an element exists, we say that R is a **ring with unity**.[1]

Examples

The ring $\mathbb{Z}$ has unity $1 \in \mathbb{Z}$, the ring

$$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$$

does not have a unity element.

[1] Many sources use the word ring exclusively for rings with unity.

Special properties of rings II: Commutativity

Let R be a ring.
We say R is **commutative** if for all $a, b \in R$, we have

$$ab = ba.$$

Examples

- The rings $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative
- If $n \geq 2$, the ring $M_n(\mathbb{R})$ of $(n \times n)$ real matrices is not commutative, e.g.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Zero-divisors and units

Let R be a ring.

- If $0 \neq a \in R$ is such that there exists a $b \in R$ with either $ab = 0$ or $ba = 0$, we say that a is a **0-divisor**.
- If R has unity, we say that $a \in R$ is a **unit** if there exists a $b \in R$ such that
$$ba = ab = 1.$$
- If a is a 0-divisor, then a is not a unit.
- It a is a unit, then a is not a 0-divisor.

Integral domains and fields

- If R is commutative, has unity, and has no 0-divisors, we say that R is an **integral domain**.
- If R is commutative, has unity, and every non-zero element is a unit, we say that R is a **field**.
- If R is a field, then R is an integral domain.

Examples

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields (and so also integral domains).
- $\mathbb{Z}$ is an integral domain, but not a field.

Notation

If F is a field and $a, b \in F$, with $b \neq 0$, we write $1/b$ for multiplicative inverse of b, and $\frac{1}{b}a = \frac{a}{b} = a\frac{1}{b}$.

Properties of $\mathbb{Z}_n$

Let $n > 0$ be an integer.

0-divisors in $\mathbb{Z}_n$

The 0-divisors in $\mathbb{Z}_n$ are the d with $1 \leq d \leq n-1$ such that

$$\gcd(d, n) \neq 1.$$

Units in $\mathbb{Z}_n$

The units of $\mathbb{Z}_n$ are the d with $1 \leq d \leq n-1$ such that

$$\gcd(d, n) = 1$$

If n is prime, then $\mathbb{Z}_n$ is a field. If n is not prime, then $\mathbb{Z}_n$ is not (even) an integral domain.

Fermat's and Euler's theorems

Let p be a prime.

Fermat's theorem

Three versions:

1. If $0 \neq a \in \mathbb{Z}_p$, then $a^{p-1} = 1$ in $\mathbb{Z}_p$.
2. If $a \in \mathbb{Z}_p$, then $a^p = a$ in $\mathbb{Z}_p$.
3. If $k \in \mathbb{Z}$, then $k^p \equiv k \pmod{p}$.

Euler's theorem (= Fermat's if n is prime)

Let $n > 0$ be an integer. If $k \in \mathbb{Z}$ is such that $\gcd(k, n) = 1$, then $k^{\varphi(n)} \equiv k \pmod{n}$, where

$$\varphi(n) = |\{d \in \{1, \ldots, n\} \mid \gcd(d, n) = 1\}| = \text{ no. of units in } \mathbb{Z}_n.$$

The field of quotients[2]

Let D be an integral domain.

- There exists a field F containing a subring isomorphic to D. The field F is called the **field of fractions** of D.
- Objects of F are equivalence classes of pairs $(a, b) \in D \times D$ satisfying $b \neq 0$, and with the equivalence relation

$$(a, b) \sim (c, d) \text{ if } ad = bc.$$

- The subring

$$\{[(a, 1)] \mid a \in D\} \subset F$$

  is isomorphic to D.
- Motivating example: $D = \mathbb{Z}$, $F = \mathbb{Q}$.

[2] Feel free to ignore in your exam preparation

Rings of polynomials

Let R be a ring. The **ring of polynomials with coefficients** in R is denoted $R[x]$. Its elements are formal expressions

$$\sum_{i=0}^{\infty} r_i x^i \qquad r_i \in R.$$

where there are only finitely many i such that $r_i \neq 0$. Addition is given by

$$\sum_{i=0}^{\infty} r_i x^i + \sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{\infty} (r_i + s_i) x^i,$$

and multiplication by

$$\left(\sum_{i=0}^{\infty} r_i x^i\right)\left(\sum_{i=0}^{\infty} s_i x^i\right) = \sum_{i=0}^{\infty} t_i x^i, \text{ with } t_i = \sum_{j=0}^{i} r_j s_{i-j}.$$

Rings of polynomials II

If $\sum_{i=0}^{\infty} r_i x^i$ is a polynomial, we normally drop terms of the form $0x^i$, e.g. we can write

$$1 + 2x + 14x^2 + 0x^3 + 0x^4 + \cdots = 1 + 2x + 14x^2.$$

The **degree** of a polynomial $f(x) = \sum_{i=0}^{\infty} r_i x^i$ is the maximal i such that $r_i \neq 0$ (and is undefined if $f(x) = 0$).

Properties of $R[x]$

- If R has unity, then $R[x]$ has unity.
- If R is commutative, then $R[x]$ is commutative.
- If R is an integral domain, then $R[x]$ is an integral domain.

Polynomial division

Let F be a field, and let $f(x), g(x) \in F[x]$.

Polynomial division of $f(x)$ by $g(x)$

There exist unique polynomials $q(x)$ ("the quotient") and $r(x)$ ("the remainder") in $F[x]$ satisfying

$$f(x) = g(x)q(x) + r(x)$$

and either $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

If $r(x) = 0$, so that $f(x) = g(x)q(x)$, we say that $g(x)$ **divides** $f(x)$.

Zeros of polynomials

Let F be a subfield of a field E and let $\alpha \in E$. The **evaluation homomorphism** $\varphi_\alpha \colon F[x] \to E$ is given by, for any

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 \in F[x],$$

$$\varphi_\alpha(f(x)) = f(\alpha) = c_n \alpha^n + c_{n-1} \alpha^{n-1} + \cdots + c_0 \in E$$

If $f(\alpha) = 0$, then we say that α is a **zero** of $f(x)$.

Theorem

The element $\alpha \in F$ is a zero of $f(x)$ if and only if $(x - \alpha)$ divides $f(x)$.

Theorem

A polynomial $f(x) \in F[x]$ of degree n has at most n zeros in F.

Irreducible polynomials

Let F be a field, and let $f(x) \in F[x]$ be a nonconstant polynomial. We say that $f(x)$ is **irreducible** (over F) if there is no way to write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$ of lower degree than $f(x)$.

Criteria for irreducibility

- If $f(x)$ has a zero in F and deg $f(x) > 1$, then $f(x)$ is reducible.
- If $f(x)$ has degree 2 or 3 and no zeros in F, then $f(x)$ is irreducible.
- Gauss' lemma: If $f(x) = c_n x^n + \cdots + c_0$ with $c_i \in \mathbb{Z}$, then $f(x)$ is irreducible over $\mathbb{Q}$ if and only if $f(x)$ is irreducible over $\mathbb{Z}$.
- The Eisenstein criterion: Let p be a prime and $f(x) = c_n x^n + \cdots + c_0$ with c_i integers. If p divides c_i for $i < n$, p does not divide c_n, and p^2 does not divide c_0, then $f(x)$ is irreducible over $\mathbb{Q}$.

Factorisation of polynomials

Theorem

For any nonconstant $f(x) \in F[x]$, we can write

$$f(x) = p_1(x)p_2(x)\cdots p_n(x)$$

with the $p_i(x) \in F[x]$ irreducible. The $p_i(x)$ are unique up to reordering and multiplying by constants, e.g.

$$x^2 + 3x + 2 = (x+1)(x+2) = (x+2)(x+1) = (2x+4)(\frac{x}{2} + \frac{1}{2}).$$

Ring homomorphisms

Let R and S be rings. A map $\varphi\colon R \to S$ is a **ring homomorphism** if for any $a, b \in R$, we have

$$\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$$

and

$$\varphi(ab) = \varphi(a)\varphi(b).$$

If φ is moreover a bijection, we call φ an isomorphism and write $R \simeq S$. The **kernel** of φ is

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0\}.$$

A homomorphism φ is injective if and only if $\ker \varphi = \{0\}$.

Ideals

Let R be a ring and $I \subseteq R$. The set I is an **ideal** of R if

1. I is a subgroup of $(R, +)$, and
2. for every $a \in R$ and $b \in I$ we have

$$ab \in I \text{ and } ba \in I.$$

Examples

- For any ring R, the sets $\{0\}, R \subset R$ are ideals.
- For any homomorphism $\varphi\colon R \to S$, $\ker \varphi \subset R$ is an ideal.
- The ideals of $\mathbb{Z}$ are all of the form

$$n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$$

for some $n \geq 0$.

Quotient rings

Let R be a ring and let I be an ideal. Thinking of I as a subgroup of the abelian group $(R, +)$, for each $a \in R$ we have the left (=right) coset

$$a + I = \{a + r \mid r \in I\}.$$

The set

$$R/I = \{\text{cosets of } I\} = \{a + I \mid a \in R\},$$

has structure of a ring by setting for $a, b \in R$

$$(a + I) + (b + I) = (a + b) + I,$$
$$(a + I)(b + I) = ab + I.$$

We call R/I the **quotient ring** of R by I.

Examples of quotient rings

- Take $I = R$. Then

$$R/R = \{a + R \mid a \in R\} = \{R\}$$

  has one element, so $R/R \simeq \{0\}$.
- Take $I = \{0\}$. Then

$$R/\{0\} = \{a + \{0\} \mid a \in R\} = \{\{a\} \mid a \in R\} \simeq R.$$

- For $n > 0$, we have

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}\} \simeq \mathbb{Z}_n.$$

The fundamental homomorphism theorem

Let $\varphi\colon R \to S$ be a homomorphism of rings. Then

- $\varphi[R]$ is a subring of S
- we have an isomorphism

$$\psi\colon R/\ker\varphi \to \varphi[R]$$

given by

$$\psi(a+\ker\varphi) = \varphi(a).$$

Example

- Let $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$ be $\varphi(k) =$ the remainder of k divided by n. Then $\ker\varphi = n\mathbb{Z}$, and $\varphi[\mathbb{Z}] = \mathbb{Z}_n$, so we find

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker\varphi \simeq \varphi[\mathbb{Z}] = \mathbb{Z}_n.$$

- If $\ker\varphi = \{0\}$, then $R/\ker\varphi \simeq R$, so that $R \simeq \varphi[R] \leq S$.

Prime and maximal ideals

Let R be a commutative ring with unity, and let $I \leq R$ be an ideal. Then

- I is a **prime ideal** if for all $a, b \in R$ such that $a \notin I$ and $b \notin I$, then $ab \notin I$.
- I is a **maximal ideal** if there is no ideal J such that $I < J < R$.

Main theorem

Let R and I be as above.

- The ideal I is prime if and only if R/I is an integral domain.
- The ideal I is maximal if and only if R/I is a field.
- If I is maximal, then I is prime.

Example

If n is prime, then $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ is a field, so $n\mathbb{Z} < \mathbb{Z}$ is a maximal ideal. If n is not prime, $\mathbb{Z}_n$ is not an integral domain, so $n\mathbb{Z}$ is not a prime ideal.

Principal ideals

If $a \in R$ and R is commutative, the **principal ideal** generated by a is

$$\langle a \rangle = \{ra \mid r \in R\} \subseteq R.$$

Examples

- For any ring R, $\langle 0 \rangle = \{0\}$.
- If R has unity and $a \in R$ is a unit, then $\langle a \rangle = R$
- For $n \in \mathbb{Z}$, we have $\langle n \rangle = n\mathbb{Z}$.
- If F is a field and $0 \neq f(x) \in F[x]$, then

$$\langle f(x) \rangle = \{g(x) \in F[x] \mid f(x) \text{ divides } g(x)\}.$$

Theorem

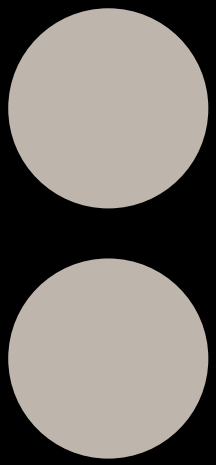
Let F be a field, and let $0 \neq f(x) \in F[x]$. The following are equivalent

1. $f(x)$ is irreducible.
2. $\langle f(x) \rangle$ is a prime ideal.
3. $\langle f(x) \rangle$ is a maximal ideal.

Corollary

The ring $F[x]/\langle f(x) \rangle$ is a field if and only if $f(x)$ is irreducible.

UiO : Department of Mathematics
University of Oslo



MAT2200 Spring 2023

Revision on rings

