Algebra I&II – Summary
Source Code at
`https://github.com/kimhanm/kimhanm.github.io`

Han-Miru Kim

June 14, 2021

1 Rings

Definition

An element $a \in R \setminus \{0\}$ is called a **zero divisor** (Nullteiler), if there exists a $b \in R \setminus \{0\}$ with $ab = 0$. A ring $R \neq \{0\}$ is called an **integral domain** (Integritätsbereich), if it has no zero divisors. This is equivalent to asking that the following holds

$$ab = ac \wedge a \neq 0 \implies b = c$$

Proposition

- Every subring of an integral domain is again an integral domain.
- Every field is an integral domain.
- $Z/n\mathbb{Z}$ is an integral domain $\iff$ n is prime.

Definition

In a commuative ring R, $a, b \in R$ we say that a **divides** b, (write $a|b$) if there exists a $c \in R$ with $b = ac$. Define the **group of units** (Einheitengruppe)

$$R^\times := \{a \big| a \text{ divides } 1\}$$

If $b = ac$ for some unit $c \in R^\times$, write $b \sim a$.

Proposition

- $a \sim b \implies a|b$ and $b|a$
- If R is an integral domain, then $a \sim b \Leftarrow a|b$ and $b|a$.

Definition

Let R be an integral domain. It's **quotient field** (Quotientenkörper) is the field

$$\operatorname{Quot}(R) := {R \times (R \setminus \{0\})}\big/{\sim}, \quad (a, b) \sim (p, q) \iff aq = bp$$

and write $\frac{a}{b} = [(a, b)]_\sim$. There is a canonical inclusion

$$\iota : R \hookrightarrow \operatorname{Quot}(R), \quad x \mapsto \frac{x}{1}$$

- $\operatorname{Quot}(\mathbb{Z}) = \mathbb{Q}$
- Because $i^2, \sqrt{2}^2 \in \mathbb{Z}$ we have $\operatorname{Quot}(\mathbb{Z}[i]) = \operatorname{Quot}(Z)[i]$, $\operatorname{Quot}(\mathbb{Z}[\sqrt{2}]) = \operatorname{Quot}(\mathbb{Z})[\sqrt{2}]$

Definition

For a commutative ring R, the **polynomial ring** (with variable X) is the collection of finite power series

$$R[X] := \left\{ \sum_{k=0}^{n} a_k X^k \Big| a_k \in R n \in \mathbb{N} \right\}$$

with coefficient-wise addition and Cauchy-multiplication

$$\left(\sum_{k=0}^{n} a_k X^k \right) \left(\sum_{k=0}^{m} b_k X^k \right) = \sum_{k=0}^{n+m} c_k X^k, \quad c_k = \sum_{i+j=k} a_i b_j$$

To construct this ring, we start with the set of all sequences $(a_n)_{n \in \mathbb{N}} \in R^{\mathbb{N}}$ and identify $(0, 1, 0, \ldots) =: X$. Every polynomial $f \in R[X]$ induces a function $f : R \to R, x \mapsto f(x)$, but the mapping

$$R[X] \to \operatorname{End}_{\mathsf{Set}}(R), f \mapsto (x \mapsto f(x))$$

is not injective. (i.e $X^2 + X \in \mathbb{F}_2[X]$)
The ring of formal power series is denoted by $R[\![X]\!]$

Definition

For $f \in R[X]$ define its **degree**

$$\deg(f) = \sup\{n \in \mathbb{N} \big| a_n = 0\}$$

in particular $\deg(0) = -\infty$.

Proposition

If R is an integral domain, then so is $R[X]$ and

- $\deg(fg) = \deg(f) + \deg(g)$
- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
- $(R[X])^\times = R^\times$. (In general, only $R^\times \subseteq R[X]^\times$, For example $2X + 1 \in \mathbb{Z}/4\mathbb{Z}[X]$ is invertible.)

Definition

For $n \in \mathbb{N}$, define the polynomial ring in n-variables inductively as

$$R[X_1, \ldots, X_n] = \begin{cases} R & n = 0 \\ R[X_1, \ldots, X_{n-1}][X_n] & n > 0 \end{cases}$$

This ring has multiple degree functions, $\deg_{X_1}, \ldots, \deg_{X_n}$ or $\deg_{\text{tot}}$.
For a field K, define the field of **rational functions** in n-variables as

$$\begin{aligned} K(X1, \ldots, X_n) &:= \operatorname{Quot}(K[X_1, \ldots, X_n]) \\ &= \{\frac{f}{g} \big| f, g \in K[X_1, \ldots, X_n], g \neq 0\} \end{aligned}$$

Theorem

For the canonical inclusion $\iota : R \to R[X_1, \ldots, X_n]$, n-elements $x_1, \ldots, x_n \in S$, any ringhomormophism $\varphi : R \to S$ induces a unique ringhomomorphism $\overline{\varphi} : R[X_1, \ldots, X_n] \to S$ such that the following diagram commutes

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & S \\ & R[X_1, \ldots, X_n] \arrow[ur, dotted, "\exists! \overline{\varphi}"'] & \end{tikzcd}$$

and $\overline{\varphi}(X_i) = x_i$.

This ringhomomorphism is given by

$$\begin{aligned} &\overline{\varphi}\left(\sum_{k_1, \ldots, k_n = 0}^{m} a_{k_1, \ldots, k_n} X_1^{k_1} \ldots X_n^{k_n}\right) \\ &= \sum_{k_1, \ldots, k_n = 0}^{m} \varphi(a_{k_1, \ldots, k_n}) x_1^{k_1} \ldots x_n^{k_n} \in S \end{aligned}$$

2 Ideals

Definition

Let R be a commutative ring. A subset $\mathfrak{a} \subseteq R$ is called an **ideal** if

(a) $\mathfrak{a} \neq 0$

(b) $\forall a, b \in \mathfrak{a} : a + b \in \mathfrak{a}$

(c) $\forall a \in \mathfrak{a}, r \in R : ra \in \mathfrak{a}$

Trivially, R itself and $\{0\}$ are ideals. The kernel of a ring homomorphism is an ideal.

Definition

For a commutative ring R and elements $a_1, \ldots, a_n$, define the **ideal generated by** $a_1, \ldots, a_n$ as

$$(a_1, \ldots, a_n) = \{\sum_{k=1}^{n} a_i x_i \big| x_i \in R\}$$

An ideal $\mathfrak{a}$ is called a **principal ideal** (Hauptideal), if it can be generated by a single element $\mathfrak{a} = (a)$. If every ideal in R is a principal ideal, then R is called a **principal ideal domain** (PID).

A non-principal ideal is $(X, Y) \subseteq Z[X, Y]$

Definition

For ideals $\mathfrak{a}, \mathfrak{b}$ and an element $r \in R$ define

(a) $r \cdot \mathfrak{a} := \{ra \big| a \in \mathfrak{a}\} \subseteq \mathfrak{a}$

(b) $\mathfrak{a} + \mathfrak{b} := \{a + b \big| a \in \mathfrak{a}, b \in \mathfrak{b}\} \subseteq \mathfrak{a}, \mathfrak{b}$

(c) $\mathfrak{a}\mathfrak{b} := \{\sum_{k=1}^{n} a_k b_k \big| a_k \in \mathfrak{a}, b_k \in \mathfrak{b}\} \subseteq \mathfrak{a}, \mathfrak{b}$.

Theorem

The relation $a \sim b \iff a - b \in \mathfrak{a}$ defines an equivalence relation on R and we write $a \equiv b \mod \mathfrak{a}$.
The quotient $R/\mathfrak{a}$ is called the **factor ring** (Faktorring) "R modulo $\mathfrak{a}$" with induced addition and multiplication. It allows a surjective ring homomor-

phism called the canonical projection

$$\rho : R \to R/\mathfrak{a}, \quad x \mapsto x + \mathfrak{a}$$

Lemma

Let $\mathfrak{a}, \mathfrak{b} \subseteq R$ be ideals in a commutative ring. Then

(a) $I = R \iff 1 \in I \iff I \cap R^\times \neq \emptyset$

(b) $(a) \subseteq (b) \iff b | a$

Proposition

Let $\varphi : R \to S$ be a ring homomorphism and $\mathfrak{a} \subseteq \operatorname{Ker} \varphi$ an ideal.
This induces a ring homomorphism $\overline{\varphi} : {}^{R}\!/\!_{\mathfrak{a}} \to S$ such that the following diagram commutes.

$$\begin{tikzcd}
R \arrow[rr, "\varphi"] \arrow[dr, "\rho"'] & & S \\
& {}^{R}\!/\!_{\mathfrak{a}} \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}$$

and if $\mathfrak{a} = \operatorname{Ker} \varphi$, $\overline{\varphi}$ is an isomorphism.

For example, the map

$$\varphi : \mathbb{R}[X] \to \mathbb{C}, X \mapsto i$$

has kernel $(X^2 + 1)$ and gives us the isomorphism ${}^{\mathbb{R}}\!/\!_{(X^2+1)} \cong \mathbb{C}$.

Definition

An ideal $\mathfrak{p} \subseteq R$ is called a **prime ideal**, if $\mathfrak{p} \neq R$ and for all $a, b \in R$ we have

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}$$

. An ideal $\mathfrak{m} \subseteq R$ is a **maximal ideal**, if $\mathfrak{m} \neq R$ and any other ideal containing $\mathfrak{m}$ is either $\mathfrak{m}$ or R.
Equivalently, we have

(a) $\mathfrak{p}$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain.

(b) $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.

(a) $\mathbb{Z}/(0)$ is a prime ideal, but not a maximal ideal.

(b) For $R = \mathbb{Z}[X]/(X^2)$ we have

$$R/(X) \cong {}^{\mathbb{Z}[X]}\!/\!_{(X^2, X)} \cong \mathbb{Z}$$

so $(X) \subseteq R$ is a prime ideal.

Proposition

Let $\mathfrak{a}_0 \subseteq R$ be an ideal. There exists a correspondence between ideals that contain $\mathfrak{a}_0$ and ideals in $R/\mathfrak{a}_0$ given by

$$\mathfrak{a}_0 \subseteq \mathfrak{a} \subseteq R \leftrightsquigarrow \mathfrak{a} + \mathfrak{a}_0 \subseteq R/\mathfrak{a}_0$$

Cliv-hanger: Does every ring have a maximal ideal?