LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Laurenz Wiesenberger

REPETITION WEEK 8
ALGEBRA

Winter term 25/26

Field of fractions

Let R be an integral domain. Consider the set $R \times (R \setminus \{0\})$ and define an equivalence relation $\sim$ by

$$(a, b) \sim (c, d) \quad \Longleftrightarrow \quad ad = bc.$$

It is straightforward to verify that this indeed defines an equivalence relation.

The *field of fractions* of R is then defined as

$$\mathrm{Frac}(R) := \big(R \times (R \setminus \{0\})\big)/\sim .$$

For an equivalence class we write

$$\frac{a}{b} := [(a, b)],$$

where $[(a, b)]$ denotes the class of (a, b) in $R \times (R \setminus \{0\})$.
Addition and multiplication on $\mathrm{Frac}(R)$ are defined by

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

These operations are well defined: if $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$, then

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

Theorem. The structure $(\mathrm{Frac}(R), +, \cdot)$ is a field, and the canonical map

$$\iota : R \longrightarrow \mathrm{Frac}(R), \qquad a \longmapsto \frac{a}{1},$$

is a monomorphism of rings.

The field of fractions $\mathrm{Frac}(R)$ of an integral domain R, together with the canonical map ι, satisfies the following universal property. Let

$$\varphi : R \longrightarrow R'$$

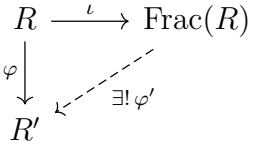
be a ring homomorphism such that $\varphi(a)$ is a unit in R' for every non-zero $a \in R$. Then there exists a unique ring homomorphism

$$\varphi' : \mathrm{Frac}(R) \longrightarrow R'$$

such that

$$\varphi' \circ \iota = \varphi,$$

that is, the diagram



commutes.
The homomorphism φ' is explicitly given by

$$\varphi'\Big(\frac{a}{b}\Big) := \varphi(a)\,\varphi(b)^{-1}.$$

If $R' \neq 0$, then φ' is injective (indeed, φ' cannot be the zero map, and hence $\ker(\varphi') = \{0\}$). If R' is a field K, we may identify $\mathrm{Frac}(R)$ with the subfield $\varphi'(\mathrm{Frac}(R)) \subseteq K$. Thus $\mathrm{Frac}(R)$ is the smallest field containing R, i.e. the field in which every non-zero element of R becomes invertible.

Example.

(1) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

(2) Let K be a field. Then

$$K(X) := \mathrm{Frac}(K[X])$$

is the field of rational functions in one variable. More generally,

$$K(X_1, \ldots, X_n) := \mathrm{Frac}(K[X_1, \ldots, X_n])$$

is the field of rational functions in n variables.

(3) In the tutorials we will show that the formal Laurent series over K, denoted by $K((X))$, coincide with

$$\mathrm{Frac}(K[[X]]).$$

Outlook : Next semester we will consider a more general construction. Let R be a commutative ring and let $S \subseteq R$ be a multiplicative set; that is,

$$1 \in S, \qquad a, b \in S \;\Rightarrow\; ab \in S.$$

We define an equivalence relation on $R \times S$ by

$$(a, s) \sim (b, s') \quad \Longleftrightarrow \quad \exists\, t \in S \text{ such that } t(as' - bs) = 0.$$

We denote the set of equivalence classes by $S^{-1}R$ and write

$$[(a, s)] := \frac{a}{s}.$$

With addition and multiplication defined in the same way as for the field of fractions, the set $S^{-1}R$ becomes a commutative ring.

There is again a canonical ring homomorphism

$$j\colon R \longrightarrow S^{-1}R, \qquad a \longmapsto \frac{a}{1}.$$

Note that this map is not injective in general: indeed,

$$\frac{a}{1} = 0 \quad \Longleftrightarrow \quad \exists\, t \in S :\ ta = 0,$$

i.e. some element of S is a zero divisor of a.

The localization $S^{-1}R$ together with the canonical map j satisfies the following universal property: If $\varphi\colon R \to R'$ is a ring homomorphism such that $\varphi(s)$ is a unit in R' for every $s \in S$, then there exists a unique ring homomorphism

$$\varphi'\colon S^{-1}R \longrightarrow R'$$

such that

$$\varphi = \varphi' \circ j.$$

Equivalently, the diagram

$$\begin{array}{ccc} R & \xrightarrow{\ j\ } & S^{-1}R \\ {\scriptstyle\varphi}\big\downarrow & \swarrow_{\exists!\,\varphi'} & \\ R' & & \end{array}$$

commutes.

Note that this construction indeed generalises the field of fractions. If R is an integral domain and we choose $S := R \setminus \{0\}$, then $S^{-1}R = \mathrm{Frac}(R)$.

Ideals and Quotient Rings

All rings in this section are commutative.

Definition. Let R be a ring. A subset $I \subseteq R$ is called an *ideal* if it satisfies:

(i) $(I, +)$ is a subgroup of $(R, +)$;

(ii) for all $x \in I$ and all $r \in R$, one has $rx \in I$.

Example.

(1) For every $n \in \mathbb{Z}$, the set $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal.

(2) Let K be a field. If $I \subseteq K$ is an ideal, then either $I = \{0\}$ or $I = K$.

(3) Let $I \subsetneq R$ be an ideal. If $I \neq R$, we call I a *proper ideal*.

(4) Let $a \in R$. The set

$$(a) := \{\, ra \mid r \in R \,\}$$

is an ideal, called the *principal ideal* generated by a.

Let I, J be ideals of R. Then

$$I + J = \{\, a + b \mid a \in I,\ b \in J \,\},$$
$$I \cap J = \{\, a \in R \mid a \in I \text{ and } a \in J \,\},$$
$$IJ := \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; n \in \mathbb{N},\ a_i \in I,\ b_i \in J \right\}$$

are ideals of R. Note that $IJ \subseteq I \cap J$. Moreover, the set of all ideals of R, equipped with ideal multiplication, forms a commutative monoid with identity element R.

(5) More generally, for a family of ideals $(I_i)_{i \in A}$ in R one defines:

$$\sum_{i \in A} I_i := \left\{ \sum_{i \in A} a_i \;\middle|\; a_i \in I_i, \text{ and only finitely many } a_i \neq 0 \right\},$$
$$\bigcap_{i \in A} I_i := \{\, a \in R \mid a \in I_i \text{ for all } i \in A \,\}.$$

Both $\sum_{i \in A} I_i$ and $\bigcap_{i \in A} I_i$ are ideals of R.

(6) Let X be a subset of R. The ideal generated by X is the smallest ideal of R that contains X. This can be described explicitly as

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} r_i a_i \;\middle|\; n \in \mathbb{N},\ r_i \in R,\ a_i \in X \right\}.$$

Note that this generalises (4).

Lemma. Let $\varphi : R \to S$ be a ring homomorphism. Then the kernel

$$\ker(\varphi) := \{\, x \in R \mid \varphi(x) = 0_S \,\}$$

is an ideal of R.

Definition.

(i) An ideal $I \subseteq R$ is said to be *of finite type* or *finitely generated* if there exist elements $a_1, \ldots, a_r \in R$ such that

$$I = (a_1, \ldots, a_r).$$

(ii) A ring R is called *noetherian* if every ideal of R is of finite type.

(iii) A commutative ring R is called a *PID* (Principal Ideal Domain) if R is an integral domain and every ideal of R is principal, i.e. generated by a single element.

Remark. In particular, every PID is noetherian.

Let R be a ring and let I be an ideal of R. Recall from group theory that the quotient R/I is an abelian group, where addition is defined by

$$(a+I)+(b+I) := (a+b)+I.$$

Analogously, we define a multiplication on R/I by

$$(a+I)\cdot(b+I) := (ab)+I.$$

One checks that this multiplication is well defined. Thus R/I becomes a commutative ring, and we have the canonical epimorphism

$$\pi\colon R \longrightarrow R/I, \qquad a \longmapsto a+I,$$

with kernel $\ker(\pi) = I$.
The quotient ring R/I together with the map π satisfies the following universal property:

Theorem (Fundamental theorem on homomorphisms)**.**
Let $\varphi\colon R \to S$ be a ring homomorphism and let $I \subseteq R$ be an ideal with $I \subseteq \ker(\varphi)$. Then there exists a unique ring homomorphism $\overline{\varphi}\colon R/I \longrightarrow S$ such that $\varphi = \overline{\varphi}\circ\pi$, that is, the diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\,\overline{\varphi}} & \\ R/I & & \end{array}$$

commutes.
Moreover, φ is surjective if and only if $\overline{\varphi}$ is surjective, and $\overline{\varphi}$ is injective if and only if $I = \ker(\varphi)$. In particular, $R/\ker(\varphi) \cong \operatorname{im}(\varphi)$.

As an immediate consequence, we obtain the following corollary.

Corollary.

(a) Let R be a ring, let $U \subseteq R$ be a subring, and let $I \subseteq R$ be an ideal. There exists a canonical ring isomorphism

$$U/(U\cap I) \;\cong\; (U+I)/I.$$

(b) Let R be a ring and let $I \subseteq J \subseteq R$ be ideals. There exists a canonical ring isomorphism

$$(R/I)\big/(J/I) \;\cong\; R/J.$$

Definition. Let R be a ring. A proper ideal $\mathfrak{p} \subseteq R$ is called a *prime ideal* if for all $a, b \in R$ we have

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

In the following we present two characterizations of prime ideals. They will be proved in the tutorials.

Lemma. Let R be a ring. Then the following statements hold:

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

(ii) $\mathfrak{p}$ is a prime ideal if and only if for all ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$ satisfying

$$\mathfrak{ab} \subseteq \mathfrak{p},$$

we have $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.

Remark. If we introduce the notation

$$\mathfrak{a} \mid \mathfrak{b} \quad :\Longleftrightarrow \quad \mathfrak{b} \subseteq \mathfrak{a},$$

then characterization (ii) above takes the familiar form of the usual definition of a prime element. Indeed, an ideal $\mathfrak{p} \neq R$ is prime if and only if

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

Example.

(1) In $\mathbb{Z}$ the zero ideal $\{0\} = (0)$ is a prime ideal. (Indeed, in any integral domain the zero ideal is a prime ideal.)

(2) If p is a prime number, then the ideal $(p) \subset \mathbb{Z}$ is prime, since

$$\mathbb{Z}/(p) \cong \mathbb{F}_p$$

is a field.

(3) In $\mathbb{Z}[X]$ the ideal (X) is prime, since

$$\mathbb{Z}[X]/(X) \cong \mathbb{Z}.$$

(4) If p is a prime number, then $(p) \subset \mathbb{Z}[X]$ is a prime ideal. Indeed,

$$\mathbb{Z}[X]/(p) \cong (\mathbb{Z}/p\mathbb{Z})[X] = \mathbb{F}_p[X],$$

which is an integral domain.

We now turn to the definition of maximal ideals. Let $I(R)$ denote the set of all proper ideals of R (note that $I(R) \neq \emptyset$ if and only if $R \neq 0$). Then $I(R)$ is partially ordered by inclusion.

Definition. A proper ideal $\mathfrak{m} \subseteq R$ is called a *maximal ideal* if it is a maximal element of $I(R)$ with respect to inclusion. Equivalently, $\mathfrak{m}$ is maximal if for every ideal $\mathfrak{a}$ with $\mathfrak{m} \subseteq \mathfrak{a}$, we have either $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = R$.

In the tutorials we will prove, using Zorn's Lemma, that if $R \neq 0$, then for every proper ideal $\mathfrak{a} \subsetneq R$ there exists a maximal ideal $\mathfrak{m}$ with $\mathfrak{a} \subseteq \mathfrak{m}$.

Next we observe that maximal ideals are prime ideals. This can be shown directly, but it also follows immediately from the following lemma.

Lemma. Let R be a ring. Then for an ideal $\mathfrak{m} \subseteq R$ we have:

$$\mathfrak{m} \text{ is a maximal ideal} \iff R/\mathfrak{m} \text{ is a field.}$$

Example.

(1) For every prime p, the ideal $(p) \subseteq \mathbb{Z}$ is maximal (see above example).

(2) The ideal $(X) \subseteq \mathbb{Z}[X]$ is a prime ideal but not maximal. The same holds for the ideal $(p) \subseteq \mathbb{Z}[X]$.

(3) Let p be a prime number. Then the ideal $(p, X) \subseteq \mathbb{Z}[X]$ is a maximal ideal. Indeed, we have the following isomorphisms

$$\mathbb{Z}[X]/(p, X) \cong \big(\mathbb{Z}[X]/(p)\big)\big/\big((p, X)/(p)\big) \cong \mathbb{F}_p[X]/(X) \cong \mathbb{F}_p.$$

(4) We will show later that if R is a PID, then the following equivalence holds:

$$\mathfrak{p} \neq 0 \text{ is a prime ideal} \iff \mathfrak{p} \text{ is a maximal ideal.}$$

Euclidean division in $R[X]$

Theorem. Let R be a commutative ring. Let $P \in R[X]$ be non-zero with

$$n := \deg(P) \in \mathbb{N}_0, \quad P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0.$$

Assume that $a_n \in R^\times$. Then for every $B \in R[X]$ there exist polynomials $Q, R \in R[X]$ such that

$$B = QA + R, \qquad \deg(R) < d.$$

Recall. In $\mathbb{Z}$, for all $a > 0$ and $b \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ such that

$$b = qa + r, \qquad 0 \leq r \leq a - 1.$$

We will need the following corollary later in field theory, when we study field extensions.

Corollary. Let K be a field and let $P \in K[X]$ be non-zero. Then the quotient ring $K[X]/(P)$ is a K-vector space with basis

$$\{\,\overline{1},\, X,\, X^2,\, \ldots,\, X^{n-1}\,\},$$

where $n := \deg(P) \geq 1$.

In the following we prove that over a field K, the polynomial ring $K[X]$ is a principal ideal domain. The same argument shows that every *euclidean ring* is a PID.

Corollary. Let K be a field. Then the polynomial ring $K[X]$ is a principal ideal domain.

One can even show that there is an equivalence, i.e. $K[X]$ is a PID if and only if K is a field. Indeed, for the converse direction assume that $K[X]$ is a PID; in particular K is an integral domain. Using

$$K[X]/(X) \cong K,$$

we obtain that (X) is a prime ideal, and since $K[X]$ is a PID, it is therefore maximal. Hence $K[X]/(X)$ is a field, and therefore K is a field.

Corollary. Let R be a commutative ring, let $P \in R[X]$ and $x \in R$. Then

$$P(x) = 0 \quad \Longleftrightarrow \quad (X - x) \mid P(X).$$