LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Laurenz Wiesenberger

REPETITION WEEK 7
ALGEBRA

Winter term 25/26

2. Rings and Fields

We now continue with the next chapter, which concerns the theory of rings and fields.

Generalities about rings

Definition. A ring is a triple $(R, +, \cdot)$ such that:

i) $(R, +)$ is an abelian group.

ii) $(R, \cdot)$ is a monoid with identity element 1.

iii) $\cdot$ is distributive with respect to $+$, i.e. for all $a, b, c \in R$:

$$(a+b)c = ac + bc, \qquad a(b+c) = ab + ac.$$

We say that a ring R is *commutative* if

$$\forall a, b \in R: \quad ab = ba.$$

Lemma. Let R be a ring. Then:

i) For all $a \in R$: $\quad a \cdot 0 = 0 = 0 \cdot a$.

ii) For all $a, b \in R$: $\quad (-a)b = a(-b) = -(ab)$.

Lemma. Let R be a ring. Then $R = 0$ if and only if $1 = 0$ in R.

Example.

1) $(\mathbb{Z}, +, \cdot)$ is the ring of integers. The structure $(\mathbb{N}, +, \cdot)$ is *not* a ring, since $(\mathbb{N}, +)$ is not a group.

2) $(\mathbb{Q}, +, \cdot) \subseteq (\mathbb{R}, +, \cdot) \subseteq (\mathbb{C}, +, \cdot)$ are all rings.

3) For $n \geq 1$, the quotient $\mathbb{Z}/n\mathbb{Z}$ is a ring. For $n = 1$, the ring $\mathbb{Z}/1\mathbb{Z} = 0$ is the trivial (zero) ring.

4) Let K be a field and $n, m \in \mathbb{N}$ with $n, m \geq 1$. Then the matrix ring $M_n(K)$ is a ring, with addition defined entrywise and multiplication given by matrix multiplication.

5) More generally, let V be a K–vector space. Then $\mathrm{End}_K(V)$ is a ring, where addition is defined pointwise and multiplication is given by composition of endomorphisms.

6) Let R, S be rings. Then $R \times S$ is a ring, called the *product ring* of R and S, with
$$(a, b) + (x, y) = (a + x,\ b + y), \qquad (a, b)(x, y) = (ax,\ by).$$
More generally, if $(R_i)_{i \in I}$ is a family of rings, then the product
$$\prod_{i \in I} R_i$$
is a ring (with componentwise addition and multiplication).

7) Let G be a group. Then the group ring $\mathbb{Z}[G]$ is a ring. Moreover, $\mathbb{Z}[G]$ is commutative if and only if G is abelian (see Tutorial Sheet 3).

Definition. Let R be a ring and $S \subseteq R$ a subset. We say that S is a *subring* of R if:

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

(ii) $1_R \in S$;

(iii) S is stable under multiplication in R, i.e. for all $a, b \in S$ we have $ab \in S$.

Example.

(1) $M_n(\mathbb{Z}) \subset M_n(\mathbb{R}) \subset M_n(\mathbb{C})$, and each inclusion is a subring.

(2) If $H \subseteq G$ is a subgroup, then $\mathbb{Z}[H] \subseteq \mathbb{Z}[G]$ is a subring of the group ring.

Definition. Let R, S be rings. A *ring homomorphism* $\varphi : R \to S$ is a map such that:

(i) For all $a, b \in R$:
$$\varphi(a + b) = \varphi(a) + \varphi(b).$$

(ii) For all $a, b \in R$:
$$\varphi(ab) = \varphi(a)\,\varphi(b).$$

(iii)
$$\varphi(1_R) = 1_S$$

Remark. In particular $\varphi : (R, +) \to (S, +)$ is a group homomorphism. Hence,

$$\varphi(0_R) = 0_S, \quad \varphi(-a) = -\varphi(a) \quad \text{for all } a \in R.$$

Definition. Let $\varphi : R \to S$ be a ring homomorphism. Then φ is called

(i) a monomorphism if φ is injective,

(ii) an epimorphism if φ is surjective,

(iii) an isomorphism if φ is bijective.

Example. The canonical map

$$\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$$

is an epimorphism of rings.

Formal Power Series and Polynomials

Let R be a ring. We consider

$$R^{\mathbb{N}_0} = \mathrm{Map}(\mathbb{N}_0, R), \quad (a_n)_{n\in\mathbb{N}_0} : \mathbb{N}_0 \to R,\ n \mapsto a_n.$$

We define addition and multiplication on $R^{\mathbb{N}_0}$:

$$\begin{aligned} + : R^{\mathbb{N}_0} \times R^{\mathbb{N}_0} &\longrightarrow R^{\mathbb{N}_0}, \quad \big((a_n), (b_n)\big) \longmapsto (a_n + b_n)_{n\in\mathbb{N}_0}, \\ \cdot : R^{\mathbb{N}_0} \times R^{\mathbb{N}_0} &\longrightarrow R^{\mathbb{N}_0}, \quad \big((a_n), (b_n)\big) \longmapsto (c_n)_{n\in\mathbb{N}_0}, \end{aligned}$$

where $c_n := \sum_{i=0}^{n} a_i b_{n-i} \in R$.

Theorem. The structure $(R^{\mathbb{N}_0}, +, \cdot)$ is a ring, with $1_{R^{\mathbb{N}}} = (1, 0, 0, \dots)$ and $0_{R^{\mathbb{N}}} = (0, 0, 0, \dots)$. It is commutative if and only if R is commutative.
We denote this ring by $R[[X]]$

We can interpret R as a subring of $R[[X]]$ as follows: Consider the embedding, that is, the injective ring homomorphism

$$R \overset{\iota}{\hookrightarrow} R[[X]], \qquad a \longmapsto (a, 0, 0, \dots).$$

This allows us to regard R as a subset of $R[[X]]$ and to identify the element a with $(a, 0, 0, \dots)$. Therefore, from now on we simply write a instead of $(a, 0, 0, \dots)$.
The next step is to express an element $(a_n)_{n\in\mathbb{N}_0}$ as a “usual” power series, that is,

$$\sum_{n\in\mathbb{N}_0} a_n X^n = \sum_{n=0}^{\infty} a_n X^n.$$

For this purpose, set $X := (0, 1, 0, 0, \dots)$. One then shows by induction that $X^m = (0, \dots, 0, 1, 0, \dots)$, where the entry 1 appears in the m-th coordinate. Consequently, for any $(a_n)_{n\in\mathbb{N}_0} \in R[[X]]$ we obtain

$$(a_n)_{n\in\mathbb{N}_0} = \sum_{n=0}^{\infty} a_n X^n.$$

Definition. Let $R[X] \subseteq R[[X]]$ be the subset of all formal power series

$$P = \sum_{n=0}^{\infty} a_n X^n \in R[[X]]$$

such that there exists an $N \in \mathbb{N}_0$ with $a_n = 0$ for all $n > N$. Then $R[X]$ is a subring of $R[[X]]$. We call $R[X]$ the *ring of polynomials* with coefficients in R in the variable X.

For a polynomial $P \in R[X]$, we define its degree by

$$\deg(P) := \max\{n \in \mathbb{N}_0 \mid a_n \neq 0\}.$$

Note that $\max(\emptyset) = -\infty$. Therefore the zero polynomial $P = 0$ has degree $-\infty$. If $\deg(P) = n$, then a_n is called the leading coefficient of P. If the leading coefficient of P is 1, we call P *monic*.

Remark. Observe that we may iterate this construction. Starting from the inclusion

$$R[X, Y] \subseteq R[[X, Y]] = R^{\mathbb{N}^2},$$

we obtain

$$(R[X])[Y] \cong R[X, Y] \cong (R[Y])[X].$$

In this way one defines the polynomial ring $R[X_1, \dots, X_n]$ in n variables.

Example.

(1) If R is commutative, then every polynomial

$$P = \sum_{i=0}^{n} a_i X^i \in R[X]$$

defines a map

$$f_P : R \longrightarrow R, \qquad x \longmapsto P(x) = \sum_{i=0}^{n} a_i x^i.$$

Thus we obtain a canonical ring homomorphism, called the *evaluation map*,

$$\mathrm{ev} : R[X] \longrightarrow \mathrm{Map}(R, R), \qquad P \longmapsto f_P.$$

(2) If R is an infinite field, then the evaluation map

$$\mathrm{ev} : R[X] \longrightarrow \mathrm{Map}(R, R), \qquad P \longmapsto f_P$$

is a ring monomorphism. We will prove this in the tutorials.

More generalities about rings

We now return to generalities about rings.
Let R be a (not necessarily commutative) ring.

Lemma. Let

$$R^\times := \{\, x \in R \mid \exists y \in R : xy = 1 = yx \,\}$$

be the subset of invertible elements of R. Then $(R^\times, \cdot)$ is a group with the neutral element 1_R. It is called the multiplicative group of R or the group of units of R.

Example.

(1) $\mathbb{Z}^\times = \{\pm 1\}$.

(2) $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

(3) $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(x, n) = 1\}$

(4) If K is a field, then the ring of invertible $n \times n$ matrices $M_n(K)$, denoted by

$$\mathrm{GL}_n(K) := M_n(K)^\times,$$

is called the the general linear group over K.

Lemma. Let R and S be rings let $\varphi : R \to S$ be a ring homomorphism. Then

$$\varphi(R^\times) \subseteq S^\times.$$

In particular, φ induces a group homomorphism

$$\varphi^\times : R^\times \longrightarrow S^\times, \qquad x \longmapsto \varphi(x),$$

called the homomorphism induced on the group of units.

This construction defines a functor

$$(-)^\times : \mathbf{Ring} \longrightarrow \mathbf{Grp}, \qquad R \longmapsto R^\times, \quad \varphi \longmapsto \varphi^\times.$$

Definition. A ring R is called a *division algebra* (or *division ring* or *skew field*) if

$$R^\times = R \setminus \{0\}.$$

If R is in addition commutative, we say that R is a *field*.

Example.

(1) Typical examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and, for a prime p, the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(2) If $\varphi : K \to L$ is a ring homomorphism between fields, then φ is injective.

(3) Let $\mathbb{H}$ be the 4-dimensional $\mathbb{R}$-vector space with basis

$$(1,\ i,\ j,\ k).$$

Define a multiplication on $\mathbb{H}$, which is obtained by $\mathbb{R}$-bilinear extension, i.e. $\cdot : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ is bilinear, of the following relations:

$$1 \cdot x = x \cdot 1 = x \qquad \text{for all } x \in \mathbb{H},$$

and

$$\begin{aligned} i^2 &= -1, & ij &= k, & ji &= -k, \\ j^2 &= -1, & jk &= i, & kj &= -i, \\ k^2 &= -1, & ki &= j, & ik &= -j. \end{aligned}$$

Theorem. $(\mathbb{H}, +, \cdot)$ is a division algebra over $\mathbb{R}$, called the *Hamiltonian quaternions*.

Remark. Since $\mathbb{R} \cong \mathbb{R} \cdot 1$ and $\mathbb{C} \cong \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot i$, we may view $\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$.

Definition. A commutative ring R with $1 \neq 0$ is called an *integral domain* if it satisfies for all $x, y \in R$:

$$x \cdot y = 0 \implies x = 0 \text{ or } y = 0.$$

In other words, the product of two non-zero elements is always non-zero.

Example.

(1) $\mathbb{Z}$ is an integral domain.

(2) Every field is an integral domain. Moreover, every subring of a field is an integral domain.

(3) Let K be a field. Then the polynomial ring $K[X]$ is an integral domain. More generally: if R is an integral domain, then so is $R[X]$ (see the following lemma).

Lemma. Let R be an integral domain and let $P, Q \in R[X]$. Then

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Example. In the exercises it will be shown that for an integral domain R one has

$$R[X_1, \dots, X_n]^\times = R^\times.$$