Contents

1	Ring	8	2
	1.1	Basic Definitions, Properties and Examples	2
	1 2	The Chinese Remainder Theorem	2

1. RINGS

1. Rings

1.1. Basic Definitions, Properties and Examples.

Definition 1.1. A commutative ring R with unity is called an **integral domain** if it has one of the following equivalent properties:

- (i) (Cancellation) zx = zy implies x = y for any $x, y, z \in R$ with $z \neq 0$.
- (ii) (No divisors of zero) xy = 0 implies either x = 0 or y = 0 for any $x, y \in R$.

Definition 1.2. A ring R with identity is called a **skew field** if $R^{\times} = R \setminus \{0\}$.

Definition 1.3. A commutative skew field is called a **field**.

Definition 1.4. A ring $R \neq \{0\}$ is called **simple** if $\{0\}$ and R are the only ideals.

Definition 1.5. Let R be a commutative ring. An ideal $P \neq R$ is called a **prime** ideal if $ab \in P$ implies either $a \in P$ or $b \in P$ for $a, b \in R$.

Proposition 1.1. An ideal $P \neq R$ of a commutative ring R with identity is a prime ideal if and only if R/P is an integral domain.

Definition 1.6. An ideal $M \neq R$ is called **maximal** if there exists no ideal I such that $M \subsetneq I \subsetneq R$.

Proposition 1.2. Let R be a commutative ring with identity. An ideal $M \neq R$ is maximal if and only if R/M is a field.

Definition 1.7. An integral domain R is called a **factorial domain** or **unique factorisation domain** when the following properties hold:

- (i) Every element $x \notin R^{\times} \cup \{0\}$ can be written as product of irreducible factors.
- (ii) If $p_1 \cdots p_n = q_1 \cdots q_m$ for irreducible $p_1, \dots, p_n, q_1, \dots, q_m \in R$, then n = m and there exists $\sigma \in S_n$ such that $p_i \sim q_{\sigma(i)}$ for $i = 1, \dots, n$.

Definition 1.8. An integral domain is called a **principal ideal domain** if every ideal of R is principal.

Theorem 1.1. Every principal ideal domain is a factorial domain.

Definition 1.9. An integral domain R is called an **euclidean domain** if there is a mapping $\varphi: R \setminus \{0\} \to \mathbb{N}_0$ with the following property: To any $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that a = qb + r and either r = 0 or $\varphi(r) < \varphi(b)$.

Example 1.1 (Euclidean Domains). Consider the *Gaussian integers* $\mathbb{Z}[i]$. The mapping $N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}_0$ defined by $N(z) := z\overline{z}$ is a euclidean norm.

Theorem 1.2. Every euclidean domain is a principal ideal domain.

Definition 1.10. A ring R is called **noetherian** if it has one of the following equivalent properties:

- (i) Every ascending chain $A_1 \subseteq A_2 \subseteq ...$ of ideals A_i of R is stationary, i.e. there exists some $k \in \mathbb{N}$ such that $A_i = A_k$ for every $i \geq k$.
- (ii) Every nonempty collection of ideals of R contains a maximal element.
- (iii) Every ideal of R is finitely generated.

Theorem 1.3 (Hilbert). If R is a commutative noetherian ring with identity then R[X] is noetherian.

Example 1.2 (Rings).

(a)
$$\mathbb{H} := \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : z, w \in \mathbb{C} \right\}$$
 is a subring of $\mathbb{C}^{2 \times 2}$ with identity.

1. RINGS

- (b) Let K be a field and $z \in K$. Then $K_z := \left\{ \begin{pmatrix} x & zy \\ y & x \end{pmatrix} : x, y \in K \right\}$ is a commutative subring of $K^{2 \times 2}$.
- (c) Let $d \in \mathbb{Z} \setminus \{1\}$ be square-free, i.e. if $x^2|d$ for $n \in \mathbb{N}$ then x = 1. Then $\mathbb{Z}[\sqrt{d}], \mathbb{Q}[\sqrt{d}] \subseteq \mathbb{C}$ are commutative rings with identity. The mapping

$$\overline{\cdot} : \begin{cases} \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}] \\ x + y\sqrt{d} \mapsto x - y\sqrt{d} \end{cases} \tag{1}$$

is an automorphism. Furthermore, the mapping $N: \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}$ defined by $N(z) := z\overline{z}$ is multiplicative. Moreover, for $z \in \mathbb{Z}[\sqrt{d}]$ we have

$$z \in \mathbb{Z}[\sqrt{d}]^{\times} \Leftrightarrow N(z) \in \{\pm 1\}. \tag{2}$$

 $\mathbb{Q}[\sqrt{d}]$ is a field, whereas $\mathbb{Z}[\sqrt{d}]$ is not.

(d) Let R be a commutative ring with identity. Then

$$R[[X]] := \{ f : f : \mathbb{N}_0 \to R \} \tag{3}$$

is a commutative extension ring with identity of R[X]. We have

$$R[[X]]^{\times} = \left\{ \sum_{i \in \mathbb{N}_0} a_i X^i : a_0 \in R^{\times} \right\}. \tag{4}$$

(e) Let R be a commutative ring with ideal A. Then

$$\sqrt{A} := \{ x \in R : \exists n \in \mathbb{N} \text{ s.t. } x^n \in A \}$$
 (5)

is an ideal in R. It holds that

$$A = \sqrt{A} \Leftrightarrow R/A$$
 does not contain any nilpotent elements $\neq 0$. (6)

Furthermore, for any prime ideal P we have $P = \sqrt{P}$ and

$$\sqrt{(0)} = \bigcap_{P \text{ prime ideal}} P. \tag{7}$$

Example 1.3 (Automorphism of Rings).

- (a) Let R be an integral domain and $a \in R^{\times}$, $b \in R$. Then there exists a unique $\varphi \in \operatorname{Aut}(R[X])$, such that $\varphi|_R = \operatorname{id}_R$ and $\varphi(X) = aX + b$. Furthermore, if $\varphi \in \operatorname{Aut}(R[X])$ with $\varphi|_R = \operatorname{id}_R$, there are $a \in R^{\times}$, $b \in R$ such that $\varphi(X) = aX + b$.
- (b) Let R be an integral domain and $B \in R[X]$. The mapping

$$\varepsilon_B : \begin{cases} R[X] \to R[X] \\ A \to A(B) \end{cases}$$
(8)

is an automorphism if and only if deg(B) = 1 and the leading coefficient of B is a unit in R.

(c) Consider \mathbb{Q} and \mathbb{R} as rings. Then

$$|\operatorname{Aut}(\mathbb{Q})| = 1 = |\operatorname{Aut}(\mathbb{R})| \tag{9}$$

1.2. The Chinese Remainder Theorem.

Theorem 1.4 (Chinese Remainder Theorem). Let R be a ring with identity and A_1, \ldots, A_n ideals of R with $A_i + A_j = R$ whenever $i \neq j$. Then the mapping

$$\Phi: \begin{cases} R/(A_1 \cap \dots \cap A_n) \to R/A_1 \times \dots \times R/A_n \\ a + A_1 \cap \dots A_n \mapsto (a + A_1, \dots, a + A_n) \end{cases}$$
 (10)

is an isomorphism of rings.

1. RINGS 4

Proof. Well-definedness and injectivity are easy. For surjectivity proove

$$R = A_j + \bigcap_{i \neq j} A_i \tag{11}$$

for
$$j = 1, \ldots, n$$
.

Example 1.4 (Application of the Chinese Remainder Theorem 1.4). Consider the system of congruence equations

$$X \equiv a_1 \bmod r_1, \dots, X \equiv a_n \bmod r_n \tag{12}$$

where $r_1, \ldots, r_n \in \mathbb{Z}$ are pairwise coprime and $a_1, \ldots, a_n \in \mathbb{Z}$. Now set

$$r := r_1 \cdots r_n$$
 and $s_i := \frac{r}{r_i}$ (13)

for each i = 1, ..., n and determine $k_i \in \mathbb{Z}$ such that

$$k_i s_i \equiv 1 \bmod r_i \tag{14}$$

for each $i=1,\ldots,n$. This can be done using the extended euclidean algorithm, i.e. since s_i and r_i are coprime, we find $t_i \in \mathbb{Z}$ such that

$$k_i s_i + t_i r_i = 1. (15)$$

Then

$$k := k_1 s_1 a_1 + \dots + k_n s_n a_n \tag{16}$$

is a solution of (12) and the set of solutions of (12) is $k + r\mathbb{Z}$.