1 Basic definitions

Definition 1.1: A ring \( R \) is a set endowed with structure by the prescription of

(i) the structure of a commutative group, called the **additive structure** of \( R \) and described with additive notation and terminology,

(ii) the structure of a monoid, called the **multiplicative structure** of \( R \) and described with multiplicative notation and terminology and with unity \( u \),

provided that the following **distributive laws** are satisfied

\[
\begin{align*}
(a + b)c &= ac + bc \\
c(a + b) &= ca + cb
\end{align*}
\]

for all \( a, b, c \in R \). \hspace{1cm} (1.1)

**Proposition 1.1.** \( R = \{0\} \) with \( u = 0 \) is a (trivial) ring. For all other rings we have \( 0 \neq u \).

**Proposition 1.2.** The following rules hold for all \( a, b, c \in R \)

\[
\begin{align*}
(a - b)c &= ac - bc, \\
c(a - b) &= ca - cb
\end{align*}
\] \hspace{1cm} (1.2)

\[
a0 = 0a = 0. \hspace{1cm} (1.3)
\]

\[
(-a)b = a(-b) = -(ab), \hspace{1cm} (-a)(-b) = ab \hspace{1cm} (1.4)
\]

**Definition 1.2:** Let a ring \( R \) be given and put \( R^\times := R \{0\} \). We say that \( R \) is **commutative** if the multiplicative monoid \( R \) is commutative. We say that \( R \) is **integral** if \( R^\times \) is a multiplicative submonoid of \( R \). We say that \( R \) is a **division-ring** if it is integral and the multiplicative submonoid \( R^\times \) is groupable. We say that \( R \) is a **field** if it is a commutative division ring.
Proposition 1.3. If $R$ is an integral ring, then the multiplicative monoid $R^\times$ is cancellative.

Definition 1.3: A subset $a$ ring $R$ is called a subring if it is both a subgroup of the additive group $R$ and a submonoid of the multiplicative monoid $R$. We say that a subset $I$ of $R$ is an ideal if $I$ is a subgroup of the additive group $R$ and if

$$RI \subset I \text{ and } IR \subset I.$$  \hspace{1cm} (1.5)

Proposition 1.4. A subset $I$ of a ring $R$ is an ideal if it is stable under addition, contains zero, and satisfies (1.5).

If a ring is commutative or integral, so is every subring of it. A subring of a field is called a subfield if its natural ring-structure is that of a field.

Let $S$ be a subset of a given ring $R$. We denote the group-span of $S$ relative to the additive group $R$ by $\text{Asp}_R S$ and the monoid span of $S$ relative to the multiplicative monoid $R$ by $\text{Msp}_R S$.

Proposition 1.5. The collection of all subrings and the collection of all ideals of a given ring $R$ are intersection-stable.

Proposition 1.6. Let a ring $R$ and $S \in \text{Sub}_R$ be given. Then there is exactly one smallest subring of $R$ that includes $S$; it is called the ring-span of $S$ and is denoted by $Rsp S$. Also, there is exactly one smallest ideal in $R$ that includes $S$; it is called the ideal-span of $S$ and is denoted by $Isp S$.

An ideal is called a principal ideal if it is the ideal-span of a singleton. If $R$ is a commutative ring then every principal ideal in $R$ is of the form

$$\text{Isp}\{a\} = Ra \text{ for some } a \in R.$$ \hspace{1cm} (1.6)

Let a ring $R$ be given. Then $\{0\}$ and $R$ are ideals in $R$. The only ideal in $R$ that contains the unity is $R$ itself.

Proposition 1.7. A commutative ring $R$ is a field if and only if $\{0\}$ and $R$ are the only ideals in $R$. 

2
2 Homomorphisms, Quotient rings

We assume that rings $R$ and $R'$, with zeros $0$ and $0'$ and unities $u$ and $u'$, respectively, are given.

**Definition 2.1:** We say that a mapping $\varphi : R \rightarrow R'$ is a ring-homomorphism if it is both a homomorphism for the additive group structures of $R$ and $R'$ and a homomorphism for the multiplicative monoid structures of $R$ and $R'$.

**Proposition 2.1.** $\varphi : R \rightarrow R'$ is a ring-homomorphism if and only if it preserves addition, multiplication, and unities, i.e., if and only if

$$
\begin{align*}
\varphi(a + b) &= \varphi(a) + \varphi(b) \\
\varphi(ab) &= \varphi(a)\varphi(b)
\end{align*}
$$

for all $a, b \in R$ (2.1)

and

$$
\varphi(u) = u'.
$$

(2.2)

**Note:** If $u' \in \text{Rng}\varphi$, then (2.2) is automatically valid. If the context makes it clear what is meant, a ring-homomorphism is often just called a homomorphism.

**Proposition 2.2.** Images and pre-images under homomorphism of subrings are again subrings.

**Proposition 2.3.** Let $\varphi : R \rightarrow R'$ be a homomorphism. Pre-images of ideals in $R'$ are ideals in $R$; in particular $\ker\varphi := \varphi^{-1}(\{0'\})$ is an ideal in $R$. If $\varphi$ is surjective, then images of ideals in $R$ are ideals in $R'$.

**Theorem 2.1.** Let a ring $R$ and an ideal $K$ in $R$ be given and consider the additive quotient group

$$
R/K := \{a + K \mid a \in R\}.
$$

(2.3)

(a) For every $P, Q \in R/K$ there is exactly one piece of the partition $R/K$ of $R$ that includes the memberwise product $PQ$: we denote this piece by $P \cdot Q$, so that $PQ \subset P \cdot Q$ and $P \cdot Q = PQ + K$. 

3
(b) If we prescribe, in \( R/K \), a multiplication by
\[
((P,Q) \mapsto P \cdot Q) : R/K \times R/K \to R/K
\]
and a unity \( U \) by
\[
U := u + K,
\]
then \( R/K \) acquires the structure of a ring. We call the ring obtained in this way the quotient-ring of \( R \) over \( K \).

**Proposition 2.4.** Let \( K \) be an ideal in a given ring \( R \). Then the mapping
\[
\omega_K : R \to R/K
\]
defined by
\[
\omega_K(x) = x + K \quad \text{for all} \quad x \notin R
\]
is a ring-homomorphism and we have \( \text{Ker}\omega_K = K \).

**Proposition 2.5.** Let \( \varphi : R \to R' \) be a ring-homomorphism and put \( K := \text{Ker}\varphi \). Then there is exactly one injective ring-homomorphism
\[
\sigma : R/K \to R'
\]
such that
\[
\varphi = \sigma \circ \omega_K,
\]
where \( \omega_K \) is the homomorphism described in Prop. 4. Moreover, if \( I' \) is a given ideal in \( R' \), then \( I := \varphi^{-1}(I') \) is an ideal in \( R \) such that
\[
K \subset I \quad \text{and} \quad I/K = \sigma^{-1}(I').
\]

**Remark:** Props. 2.4 and 2.5 above are analogous of Props. 2.8 and 2.9 in “Groups”.

**Example:** For the ring \( \mathbb{Z} \) of integers, the ideals in \( \mathbb{Z} \) are the sets of the form \( m\mathbb{Z} \) with \( m \in \mathbb{Z} \). By the Theorem, \( \mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} \) has the natural structure of a ring; \( \mathbb{Z}_m \) is often called the “ring of integers modulo \( m \)”. \( \mathbb{Z}_m \) is actually a field if and only if \( m \) is a prime number.
3 Polynomial rings

We assume that a commutative ring $R$ with unity $u$ is given.

**Definition 3.1:** We say a ring $P$ is a polynomial ring over $R$ if

(i) $P$ is commutative and includes $R$ as a subring.

(ii) $P$ is endowed with additional structure by the prescription of an element $x \in P$, called the indeterminate of $P$, such that the mapping

$$\rho : R^{(\mathbb{N})} \rightarrow P$$

defined by

$$\rho(c) := \sum_{n \in \mathbb{N}} c_n x^n \text{ for all } c \in R^{(\mathbb{N})}$$

is invertible.

We now assume that a polynomial ring $P$ over $R$, with indeterminate $x$, is given. We denote the inverse of the mapping (3.1) defined by (3.2) by

$$\gamma : P \rightarrow R^{(\mathbb{N})},$$

so that

$$p = \sum_{n \in \mathbb{N}} \gamma(p)_n x^n \text{ for all } p \in P.$$

Given $p \in P$, the sequence $\gamma(p)$ is called the sequence of coefficients of $p$.

**Proposition 3.1.** The mappings $\rho$ and $\gamma$ defined by (3.1) – (3.4) are additive group-isomorphisms.

**Proposition 3.2.** For all $p, q \in P$, we have

$$pq = \sum_{n \in \mathbb{N}} \left( \sum_{k \in (n+1)^{\dagger}} \gamma(p)_k \gamma(q)_{n-k} \right) x^n,$$

so that

$$\gamma(pq)_n = \sum_{k \in (n+1)^{\dagger}} \gamma(p)_n \gamma(q)_{n-k} \text{ for all } n \in \mathbb{N}.$$
Theorem 3.1. Let $\eta : R \rightarrow R'$ be a homomorphism from $R$ to a commutative ring $R'$. For every $a \in R'$ there is exactly one homomorphism $\eta_a : P \rightarrow R'$ such that

$$\eta_a|_R = \eta \quad \text{and} \quad \eta_a(x) = a.$$  \hspace{1cm} (3.7)

Corollary 3.1. For every $a \in R$, there is exactly one homomorphism $\varepsilon_a : P \rightarrow R$ such that $\varepsilon_a|_R = \eta$ and $\varepsilon_a(x) = a$. We have

$$\varepsilon_a(p) = \sum_{k \in \mathbb{N}} \gamma(p)_{k} a^{k} \quad \text{for all} \quad p \in P.$$  \hspace{1cm} (3.8)

We will use the notation

$$p'(a) := \varepsilon_a(p) \quad \text{for all} \quad p \in P, \ a \in R$$  \hspace{1cm} (3.9)

and call $p'(a)$ the value of $p$ at $a$. Given $p \in P$, the mapping $p' \in \text{Map}(R, R)$ defined by (3.9) is called the polynomial function associated with $p$. The set of all polynomial functions is denoted by

$$\text{Pol} \ R := \{ p' \in \text{Map}(R, R) \mid p \in P \}.$$  \hspace{1cm} (3.10)

We note that if $S$ is any set, then $\text{Map}(S, R)$ acquires the structure of a commutative ring if we define the zero and unity in $\text{Map}(S, R)$ to be the constants with value 0 and $u$ and if we define addition, opposition, and multiplication in $\text{Map}(S, R)$ by value-wise application of these operations.

Proposition 3.3. $\text{Pol} \ R$ is a subring of $\text{Map}(R, R)$ and

$$p \mapsto p' : P \rightarrow \text{Pol} \ R$$

is a surjective ring-homomorphism. It is invertible if and only if $p' = 0 \implies p = 0$ for all $p \in P$.

Definition 2: For every $p \in P^\times$ the degree of $p$ is defined by

$$\deg p := \max Supt \gamma(p)$$  \hspace{1cm} (3.11)

and the leading coefficient of $p$ is defined by

$$\text{lc}(p) := \gamma(p)_{\deg p}.$$  \hspace{1cm} (3.12)

We say that $p \in P^\times$ is a monic polynomial if $\text{lc}(p) = u$. 

6
Proposition 3.4. Let $p,q \in P^\times$ be given such that $p+q \in P^\times$. Then

$$\deg(p+q) \leq \max\{\deg(p), \deg(q)\}, \quad (3.13)$$

in which the inequality is strict if and only if $\deg(p) = \deg(q)$ and $\lc(p) = -\lc(q)$. If $\deg(p) \neq \deg(q)$ or $\lc(p) \neq -\lc(q)$, then,

$$\lc(p+q) = \gamma(p)_{\deg(p+q)} + \gamma(q)_{\deg(p+q)}. \quad (3.14)$$

Proposition 3.5. Let $p,q \in P^\times$ be given such that $pq \in P^\times$. Then

$$\deg(pq) \leq \deg(p) + \deg(q), \quad (3.15)$$

in which the inequality is strict if and only if $\lc(p) \lc(q) = 0$. If $\lc(p) \lc(q) \neq 0$, we have

$$\lc(pq) = \lc(p) \lc(q). \quad (3.16)$$

Corollary 3.2. If $p,q \in P^\times$ are monic polynomials, so is $pq$ and we have

$$\deg(pq) = \deg(p) + \deg(q). \quad (3.17)$$

Corollary 3.3. If $R$ is an integral ring, so is $P$ and (3.17) holds for all $p,q \in P^\times$. 
