CHAPTER 1

REVIEW OF RINGS AND FIELDS

1.1 Rings and Ideals

Definition 1.1.1 (Rings)**.** Let R be a set and let $(+), (\cdot)\colon R \times R \to R$ be functions. We say that $(R, +, \cdot)$ is a *ring* if:

- $(R, +)$ is an abelian group;
- for all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- there exists a $1 \in R$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$;
- for all $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

The ring is *commutative* if for all $a, b \in R$, $a \cdot b = b \cdot a$.

Definition 1.1.2 (Ring Homomorphisms)**.** Let R, S be rings and let $\varphi\colon R \to S$ be a map. We say that φ is a *ring homomorphism* if:

- $\varphi(1_R) = 1_S$;
- $f(a + b) = f(a) + f(b)$ for all $a, b \in R$;
- $f(ab) = f(a)f(b)$ for all $a, b \in R$.

Further, if φ is bijective, we say that φ is a *ring isomorphism.*

Proposition 1.1.3. *Let R, S be rings and let $\varphi\colon R \to S$ be a ring isomorphism. Then, φ^{-1} is a ring isomorphism.*

Proof. Let $s_1, s_2 \in S$. We can find an $r_1, r_2 \in R$ such that $\varphi(r_1) = s_1$ and $\varphi(r_2) = s_2$. Since φ is a ring homomorphism, we have $\varphi(r_1 + r_2) = s_1 + s_2$. Hence,

$$\varphi^{-1}(s_1) + \varphi^{-1}(s_2) = r_1 + r_2 = \varphi^{-1}(s_1 + s_2).$$

Moreover, $\varphi(r_1 \cdot r_2) = s_1 \cdot s_2$. Hence,

$$\varphi^{-1}(s_1) \cdot \varphi^{-1}(s_2) = r_1 \cdot r_2 = \varphi^{-1}(s_1 \cdot s_2).$$

So, φ^{-1} is a ring homomorphism. □

Definition 1.1.4. Let R, S be rings and let $\varphi\colon R \to S$ be a ring homomorphism. We define the *kernel of* φ to be the set

$$\ker \varphi = \varphi^{-1}(0) = \{r \in R \mid \varphi(r) = 0\}.$$

Definition 1.1.5. Let R be a ring and let $I \subseteq R$. We say that I is an *ideal* of R if:

- I is a subgroup of $(R, +)$; and
- for all $r \in R$ and $i \in I$, $ri \in I$ and $ir \in I$.

Proposition 1.1.6. *Let R be a ring and let $I \subseteq R$ be an ideal. Then, R/I is an ideal with addition*

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

and multiplication

$$(a + I) \cdot (b + I) = ab + I,$$

with additive identity $0 + I$ and multiplicative identity $1 + I$.

Definition 1.1.7. Let R be a ring and $I \subseteq R$ be an ideal. We say that R/I is a *quotient ring*.

Proposition 1.1.8. *Let R, S be rings and let $\varphi \colon R \to S$ be a ring homomorphism. Then, φ is injective if and only if $\ker \varphi$ is trivial.*

Proof. First, assume that φ is injective. Since $\varphi(0) = 0$, we must have that $\ker \varphi = \{0\}$.

Next, assume that $\ker \varphi = \{0\}$. Let $r_1, r_2 \in R$ such that $\varphi(r_1) = \varphi(r_2)$. So, $\varphi(r_1 - r_2) = 0$, meaning that $r_1 - r_2 \in \ker \varphi$. Hence, $r_1 = r_2$. This implies that φ is injective. □

Lemma 1.1.9. *Let R, S be rings and let $\varphi \colon R \to S$ be a ring homomorphism. Then, $\ker \varphi$ is an ideal of R.*

Proof. Let $a \in R$ and $i \in \ker \varphi$. Then,

$$\begin{aligned} \varphi(ai) &= \varphi(a) \cdot \varphi(i) = \varphi(a) \cdot 0 = 0 \\ \varphi(ia) &= \varphi(i) \cdot \varphi(a) = 0 \cdot \varphi(a) = 0. \end{aligned}$$

Hence, $ai, ia \in \ker \varphi$. So, $\ker \varphi$ is an ideal in R. □

Theorem 1.1.10 (First Isomorphism Theorem)**.** *Let R, S be rings and let $\varphi \colon R \to S$ be a ring homomorphism. Then,*

$$R/\ker \varphi \cong \operatorname{Im} \varphi.$$

Proof. Define the map $\psi \colon R/\ker \varphi \to S$ given by $\psi(r + \ker \varphi) = \varphi(r)$. We will show that ψ is a ring isomorphism.

- First, we show that ψ is well-defined. So, let $r + \ker \varphi = s + \ker \varphi$. Then, $r - s \in \ker \varphi$, meaning that $\varphi(r - s) = 0$. Hence,

  $$\psi(r + \ker \varphi) = \varphi(r) = \varphi(s) = \psi(s + \ker \varphi).$$

  So, the map is well-defined.

- Next, we show that ψ is a ring homomorphism. So, let $r, s \in R$. Then,

$$\begin{aligned}\psi((r+\ker\varphi)+(s+\ker\varphi)) &= \psi((r+s)+\ker\varphi)\\ &= \varphi(r+s)\\ &= \varphi(r)+\varphi(s)\\ &= \psi(r+\ker\varphi)+\psi(s+\ker\varphi).\end{aligned}$$

  Moreover,

$$\begin{aligned}\psi((r+\ker\varphi)\cdot(s+\ker\varphi)) &= \psi(rs+\ker\varphi)\\ &= \varphi(rs)\\ &= \varphi(r)\varphi(s)\\ &= \psi(r+\ker\varphi)\psi(s+\ker\varphi).\end{aligned}$$

  So, ψ is a ring homomorphism.

- Now, we find that

$$\begin{aligned}\ker\psi &= \{r+\ker\varphi \in R/\ker\varphi \mid \psi(r+\ker\varphi)=0\}\\ &= \{r+\ker\varphi \in R/\ker\varphi \mid \varphi(r)=0\}\\ &= \{r+\ker\varphi \in R/\ker\varphi \mid r \in \ker\varphi\} = \{\ker\varphi\}.\end{aligned}$$

  So, ψ is injective.

Hence, we have a ring isomorphism

$$R/\ker\varphi \cong \operatorname{Im}\varphi.$$

□

Theorem 1.1.11 (Correspondence Theorem)**.** *Let R be a ring, I be an ideal of R. Then,*

- *for an ideal $I \subseteq J \subseteq R$,*

$$J/I := \{j+I \mid j \in J\}$$

  is an ideal of R/I;

- *for an ideal K of R/I, the set*

$$J = \bigcup_{a+I\in K}\{a+i \mid i \in I\}$$

  is an ideal of R containing I;

- *there is a bijection between ideals of R/I and ideals of R containing I, given by $J \mapsto J/I$.*

Proof.

- Let $I \subseteq J \subseteq R$ be an ideal. By the correspondence theorem for groups, we know that J/I is a subgroup of R/I. Now, let $j + I \in J/I$ and $r + I \in R/I$. Then,

  $$(j+I)(r+I) = jr + I \in J/I, \qquad (r+I)(j+I) = rj + I \in J/I$$

  since $jr, rj \in J$. Hence, J/I is an ideal of R/I.

- Let $K \subseteq R/I$ be an ideal. By the correspondence theorem for groups, we know that J is a subgroup of R. Now, let $j \in J$ and $r \in R$. Since K is an ideal, we find that

  $$(j+I)(r+I) = jr + I \in K, \qquad (r+I)(j+I) = rj + I \in K.$$

  So, $jr, rj \in J$. Hence, J is an ideal of R.

- This follows from the results above.

$\square$

Definition 1.1.12. Let R be a ring and let $X \subseteq R$. We define the *ideal generated by* X, denoted (X), by the intersection of all ideals of R containing X.

Proposition 1.1.13. *Let R be a ring and let $X \subseteq R$. Then, the ideal (X) is composed of finite sums of the form*

$$\sum_{i=1}^{n} a_i x_i b_i,$$

where $a_i, b_i \in R$ and $x_i \in X$ for all $1 \leq i \leq n$.

Proof. Let $[X]$ denote all finite sums of the form

$$\sum_{i=1}^{n} a_i x_i b_i,$$

where $a_i, b_i \in R$ and $x_i \in X$ for all $1 \leq i \leq n$. For all $x \in X$, we have $x = 1x1 \in [X]$, so $X \subseteq [X]$. By construction, the set $[X]$ is closed under addition. Moreover, we have

$$-\left(\sum_{i=1}^{n} a_i x_i b_i\right) = \sum_{i=1}^{n} (-a_i) x_i b_i \in [X]$$

with $a_i, b_i \in R$ and $x_i \in X$ for all $1 \leq i \leq n$, so $[X]$ is an additive subgroup. Also,

$$a\left(\sum_{i=1}^{n} a_i x_i b_i\right) = \sum_{i=1}^{n} (a a_i) x_i b_i \in [X], \qquad \left(\sum_{i=1}^{n} a_i x_i b_i\right) b = \sum_{i=1}^{n} a_i x_i (b_i b) \in [X],$$

meaning that $[X]$ is an ideal of R containing X.

Now, let $I \subseteq R$ be an ideal of R containing X. We show that $[X] \subseteq I$. Since $X \subseteq I$, we find that for all $a, b \in R$ and $x \in X$, $abx \in I$. Moreover, since I is closed under addition, we have

$$\sum_{i=1}^{n} a_i x_i b_i \in I.$$

Hence, $[X] \subseteq I$. Since $[X]$ is an ideal of R containing X, we find that

$$(X) = \bigcap_{\substack{I \subseteq R \text{ ideal} \\ X \subseteq I}} I = [X].$$

□

Using this result, we find that in a commutative ring R, the ideal generated by $\{x\}$, for some $x \in R$ is given by

$$(x) = \{rx \mid r \in R\}.$$

1.2 Integral Domains and Fields

Definition 1.2.1. Let R be a ring and let $u \in R$. We say that u is a *ring* there exists a $v \in R$ such that $uv = 1 = vu$. We say that v is a *multiplicative inverse* of u.

Proposition 1.2.2. *Let R be a ring and let $u \in R$ with multiplicative inverses v_1 and v_2. Then, $v_1 = v_2$.*

Proof. We know that $uv_1 = 1 = v_1 u$ and $uv_2 = 1 = v_2 u$. So,

$$v_1 = v_1 \cdot 1 = v_1(uv_2) = (v_1 u)v_2 = 1 \cdot v_2 = v_2.$$

□

Definition 1.2.3. Let K be a non-zero ring (i.e. $K \neq \{0\}$). We say that K is a *field* if for all $x \in K$ with $x \neq 0$, x is a unit.

Proposition 1.2.4. *Let R be a commutative ring. Then, R is a field if and only if it has no non-trivial proper ideals.*

Proof. Assume first that R is a field, and let $I \subseteq R$ be a non-trivial ideal. In that case, there exists a $u \in I$ such that $u \neq 0$. Since R is a field, we find that u is a unit. Hence, for all $a \in R$,

$$a = au^{-1} \cdot u \in I.$$

So, $I = R$. That is, R has no non-trivial proper ideals.

Now, assume that R has no non-trivial proper ideals, and let $u \in R$ be non-zero. We know that (u) is a non-trivial ideal of R. Hence, $(u) = R$. In particular, there exists a $v \in R$ such that $uv = 1$. So, u is a unit. □

Corollary 1.2.5. *Let K be a field, R a non-zero ring and let $\varphi\colon K \to R$ be a ring homomorphism. Then, φ is injective.*

Proof. We know that $\ker \varphi$ is an ideal of K. Moreover, since $\varphi(1) = 1$, we know that $\ker \varphi \neq R$. Hence, $\ker \varphi$ is trivial, meaning that φ is injective. □

Definition 1.2.6. Let R be a commutative ring and let $r \in R$ be non-zero. We say that r is a *zero divisor* if there exists a non-zero $s \in R$ such that $rs = 0$. We say that R is an *integral domain* if it is non-zero and has it has no zero divisors.

Proposition 1.2.7. *Let R be an integral domain and let $r, a, b \in R$ such that $ra = rb$. Then, either $r = 0$ or $a = b$.*

Proof. We know that $r(a - b) = 0$. Now, if $r \neq 0$, then since r cannot be a zero divisor, we must have that $a - b = 0$. So, either $r = 0$ or $a = b$. □

Lemma 1.2.8. *Let K be a field. Then, K is an integral domain.*

Proof. Let $a \in K$ be non-zero and let $b \in K$ such that $ab = 0$. Since K is a field, we know that a is a unit. Hence,

$$b = a^{-1} \cdot (ab) = 0.$$

So, a is not a zero divisor. Hence, K is an integral domain. □

Definition 1.2.9. Let R be a commutative ring and let $I \subseteq R$ be an ideal. We say that I is *principal* if there exists a $p \in R$ such that

$$I = (p) = \{rp \mid r \in R\}.$$

We say that R is a *principal ring* if all its ideals are principal. If R is an integral domain, we further say that R is a *principal ideal domain*.

Proposition 1.2.10. *The set $\mathbb{Z}$ is a principal ideal domain.*

Proof. Let $I \subseteq \mathbb{Z}$ be an ideal. If $I = \{0\}$, then $I = (0)$. Otherwise, let $n \in I$ be the smallest positive integer. Now, let $m \in I$. By the division algorithm, there exist $q, r \in \mathbb{Z}$ such that

$$m = qn + r,$$

with $0 \leq r < n$. We have

$$r = m - qn \in I$$

since I is an ideal. By the minimality of n, we must have that $r = 0$. That is, $m = qn \in (n)$. By the definition of ideal, we have $(n) \subseteq I$, meaning that $I = (n)$. $\square$

1.3 Maximal and prime ideals

Definition 1.3.1. Let R be a ring and let $I \subseteq R$ be an ideal.

- We say that I is *prime* if for all $a, b \in R$ with $ab \in I$, either $a \in I$ or $b \in I$;
- We say that I is *maximal* if for all ideals $I \subseteq J \subseteq R$, either $J = I$ or $J = R$.

Proposition 1.3.2. *Let R be a commutative ring and let M be a maximal ideal of R. Then, M is a prime ideal.*

Proof. Let $a, b \in R$ with $a \notin M$ such that $ab \in M$. We know that

$$J = M + (a) = \{m + ar \mid m \in M, r \in R\}$$

is an ideal in R containing a. Since $a \notin M$ and $M \subseteq J$, we find that $J = R$. In particular, $1 = m + ar$, for some $m \in M$ and $r \in R$. Hence,

$$b = b \cdot 1 = b \cdot (m + ar) = mb + abr \in M$$

since $m, ab \in M$. So, M is a prime ideal. □

Theorem 1.3.3. *Let R be a commutative ring and let $I \subseteq R$ be an ideal. Then, I is prime if and only if R/I is an integral domain.*

Proof. Assume first that I is a prime ideal. Let $a + I, b + I \in R/I$ such that $(a + I)(b + I) = 0 + I$. In that case, $ab + I = 0 + I$, meaning that $ab \in I$. Since I is a prime ideal, we know that either $a \in I$ or $b \in I$. That is, either $a + I = 0 + I$ and $b + I = 0 + I$. So, R/I is an integral domain.

Assume now that R/I is an integral domain. Let $a, b \in R$ such that $ab \in I$. In that case,

$$(a + I)(b + I) = ab + I = 0 + I.$$

Since R/I is an integral domain, we find that $a + I = 0 + I$ or $b + I = 0 + I$. Hence, either $a \in I$ or $b \in I$. So, I is a prime ideal. □

Theorem 1.3.4. *Let R be a commutative ring and let $I \subseteq R$ be an ideal. Then, I is maximal if and only if R/I is a field.*

Proof. Assume first that I is a maximal ideal. Let $a + I \in R/I$ be non-zero. In that case, $a \notin I$. Now, let

$$J = I + (a) = \{i + ar \mid i \in I, r \in R\}.$$

We know that J is an ideal of R. Moreover, since $a \notin I$ and I maximal, we find that $J = R$. In particular, there exists an $i \in I$ and a $r \in R$ such that $1 = i + ar$. Hence,

$$(a + I)(r + I) = ar + I = (ar + i) + I = 1 + I.$$

So, $a + I$ is a unit. This implies that R/I is a field.

Assume now that R/I is a field, and let $I \subsetneq J \subseteq R$ be an ideal. By the correspondence theorem, we know that J/I is an ideal of R/I. Moreover, it is non-trivial. Since R/I is a field, we find that $J/I = R/I$. That is, $J = R$. So, I is a maximal ideal. □

Definition 1.3.5. Let R be an integral domain and $a \in R$. We say that a is *reducible* if it is not a unit and $a = bc$, for $b, c \in R$ not units. If a is not reducible, then a is *irreducible.*

Proposition 1.3.6. *Let R be a principal ideal domain and let $r \in R$ not a unit and non-zero. Denote $I = (r)$. Then, I is a non-trivial proper ideal, and the following are equivalent:*

1. *The element r is irreducible;*
2. *The ideal I is a prime ideal;*
3. *The ideal I is a maximal ideal;*
4. *The quotient R/I is an integral domain;*
5. *The quotient ring R/I is a field.*

Proof. We have already shown that $(3) \implies (2), (2) \iff (4), (3) \iff (5)$. So, we show that $(2) \implies (1)$ and $(1) \implies (3)$:

$(2) \implies (1)$ Assume that r is reducible. So, $r = ab$, for $a, b \in R$ not units. We claim that $a \notin (r)$. Assume, for a contradiction, that $a \in (r)$. In that case, $a = rx$, for some $x \in R$. Hence,

$$r = ab = rbx \iff r(1 - bx) = 0.$$

We know that $r \neq 0$, so we must have $bx = 1$. So, b is a unit- this is a contradiction. So, $a \notin (r)$. Similarly, $b \notin (r)$. We have $ab = r \in (r)$, so I cannot be a prime ideal.

$(1) \implies (3)$ Assume that r is irreducible, and let $I \subseteq J \subsetneq R$ be ideals. Since R is a principal ideal domain, we know that $J = (k)$, for some $k \in R$. Moreover, since $J \neq R$, we know that k is not a unit. Since $r \in J$, we find that $r = kx$, for some $x \in R$. Since k is not a unit and r is irreducible, we must have that x is a unit. So, $k = x^{-1}r \in (r)$. Hence, $J = I$. So, I is a maximal ideal.

□

Definition 1.3.7. Let K be a field and let $L \subseteq K$ be a subring. If L is a field, we say that L is a *subfield* of K.

Definition 1.3.8. Let K be a field. Then, the intersection of all subfields of K is called the *prime subfield* of K.

Proposition 1.3.9. *Let K be a field. Then, the prime subfield of K is either isomorphic to $\mathbb{Q}$ or $\mathbb{F}_p$, for a unique prime p.*

Proof. Let $P \subseteq K$ be the prime subfield. Define the map $f\colon \mathbb{Z} \to K$ by $f(n) = n \cdot 1$. Since $P = (1)$, we find that $\mathrm{Im}(f) \subseteq P$. Moreover, by the First Isomorphism Theorem, we know that

$$\mathbb{Z}/\ker f \cong \mathrm{Im}(f).$$

Since $\mathrm{Im}(f)$ is an integral domain, we must have that $\ker f$ is a prime ideal. If $\ker f$ is zero, then $\mathbb{Z} \cong \mathrm{Im}(f)$. Since every non-zero element in $\mathrm{Im}(f)$ has an inverse, we can extend the map to $g\colon \mathbb{Q} \to P$ by $g(0) = 0$ and

$$g(p/q) = f(p)f(q)^{-1}$$

otherwise. Then, $\ker g$ is zero, meaning that the map is injective. So, $\mathbb{Q} \cong \mathrm{Im}(f)$. In particular, it is a field. Since P is the prime subfield, we must therefore have $P = \mathrm{Im}(g) \cong \mathbb{Q}$.

Now, assume that $\ker f$ is non-zero. In that case, $\ker f = (p)$, for prime p. Hence,

$$\mathrm{Im}(f) \cong \mathbb{F}_p$$

is a field. Since P is the prime subfield, we must therefore have $P = \mathrm{Im}(f) \cong \mathbb{F}_p$. Since $\mathbb{F}_p \cong \mathbb{F}_q$ if and only if $p = q$, the prime p is unique. □

Lemma 1.3.10. *Let R be an integral domain, and let $\sim$ be the relation on $R \times R \setminus \{0\}$ be given by*

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

Then, $\sim$ is an equivalence relation.

Proof. Let $(a, b) \in R \times R \setminus \{0\}$. We trivially have $(a, b) \sim (a, b)$ since $ab = ab$. Now, let $(a, b), (c, d) \in R \times R \setminus \{0\}$ such that $(a, b) \sim (c, d)$. Hence, $ad = bc$, meaning that $cb = da$ as well. Therefore, $(c, d) \sim (a, b)$. Finally, let $(a, b), (c, d), (e, f) \in R \times R \setminus \{0\}$ such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. In that case, we know that $ad - bc = 0$ and $cf - de$. Moreover,

$$d \cdot (af - be) = ad \cdot f - b \cdot de = bc \cdot f - b \cdot de = b \cdot (cf - de) = b \cdot 0 = 0.$$

Since $d \neq 0$, we find that $af = be$. So, $(a, b) \sim (e, f)$. This implies that $\sim$ is an equivalence relation. □

Lemma 1.3.11. *Let R be an integral domain, and let $\sim$ be the equivalence relation on $R \times R \setminus \{0\}$ given by*

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

We denote the equivalence class of (a, b) by $\frac{a}{b}$. Then, the quotient $R \times R \setminus \{0\}/\sim$ forms a field under the following operations:

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

Proof. We first show that the operations are well-defined. So, let $(a_1, b_1), (a_2, b_2), (c_1, d_1), (c_2, d_2) \in R \times R \setminus \{0\}$ such that $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_1, d_2)$. In that case, $a_1 b_2 = b_1 a_2$ and $c_1 d_2 = d_1 c_2$. Hence,

$$\begin{aligned} (a_1 d_1 + b_1 c_1) \cdot b_2 d_2 &= a_1 b_2 \cdot d_1 d_2 + c_1 d_2 \cdot b_1 b_2 \\ &= b_1 a_2 \cdot d_1 d_2 + d_1 c_2 \cdot b_1 b_2 \\ &= (a_2 b_2 + c_2 d_2) b_1 d_1. \end{aligned}$$

So, $(a_1d_1 + b_1c_1, b_1d_1) \sim (a_2d_2 + b_2c_2, b_2d_2)$. Similarly,

$$a_1c_1 \cdot b_2d_2 = a_1b_2 \cdot c_1d_2 = b_1a_2 \cdot d_1c_2 = a_2c_2 \cdot b_1d_1.$$

This implies that $(a_1c_1, b_1d_1) \sim (a_2c_2, b_2d_2)$. So, the operations are well-defined.

Now, we show that the operations are associative. So, let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in R \times R \setminus \{0\}$. Then,

$$\begin{aligned} \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) &= \frac{a}{b} + \frac{cf+de}{df} & \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} &= \frac{ad+bc}{bd} + \frac{e}{f} \\ &= \frac{adf + b(cf+de)}{bdf} & &= \frac{(ad+bc)f + bde}{bdf} \\ &= \frac{adf + bcf + bde}{bdf} & &= \frac{adf+bcf+bde}{bdf}. \end{aligned}$$

So, the addition operation is associative. Moreover,

$$\frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{ce}{df} = \frac{ace}{bdf} = \frac{ac}{bd} \cdot \frac{e}{f} = \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f}.$$

So, the multiplication operation is associative.

Next, let $\frac{a}{b} \in R \times R \setminus \{0\}/\sim$. Then,

$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}, \qquad \frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}.$$

So, both operations have an identity. Moreover,

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab - ab}{b^2} = \frac{0}{b^2} = \frac{0}{1},$$

and if $a \neq 0$, then

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{a \cdot b} = \frac{1}{1}.$$

So, both operations have an inverse.

Finally, let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in R \times R \setminus \{0\}/\sim$. We know that

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{b} \cdot \frac{a}{b},$$

so the multiplication operation is commutative. Moreover,

$$\begin{aligned} \frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) &= \frac{a}{b} \cdot \frac{cf+de}{df} \\ &= \frac{acf + ade}{bdf} \\ &= \frac{abcf + abde}{b^2df} \\ &= \frac{ac}{bd} + \frac{ae}{bf} \\ &= \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}. \end{aligned}$$

Hence, the operation is distributive. This implies that the quotient is a field. □

Theorem 1.3.12. *Let R be an integral domain. Then, there exists a field* $\mathrm{Quot}(R)$ *and an injective ring homomorphism* $\iota\colon R \to \mathrm{Quot}(R)$ *such that for any injective ring homomorphism* $f\colon R \to K$ *into a field* K*, there exists a unique field homomorphism* $F\colon \mathrm{Quot}(R) \to K$ *such that* $F \circ \iota = f$.

Proof. Let $\mathrm{Quot}(R) = R \times R \setminus \{0\}/\sim$. Define the map $\iota\colon R \to \mathrm{Quot}(R)$ by $\iota(r) = \frac{r}{1}$. For $r_1, r_2 \in R$, we have

$$\begin{aligned} \iota(r_1) + \iota(r_2) &= \frac{r_1}{1} + \frac{r_2}{1} = \frac{r_1 \cdot 1 + 1 \cdot r_2}{1 \cdot 1} = \frac{r_1 + r_2}{1} = \iota(r_1 + r_2) \\ \iota(r_1) \cdot \iota(r_2) &= \frac{r_1}{1} \cdot \frac{r_2}{1} = \frac{r_1 r_2}{1} = \iota(r_1 r_2). \end{aligned}$$

Moreover, $\iota(1) = \frac{1}{1}$, meaning that ι is a ring homomorphism. Now, let $r \in \ker \iota$. In that case,

$$\iota(r) = \frac{r}{1} = \frac{0}{1}.$$

So, $(r, 1) \sim (0, 1)$, meaning that $r = 0$. So, $\ker \iota$ is trivial, which implies that ι is injective.

Now, let $f\colon R \to K$ be an injective ring homomorphism. Define the map $F\colon \mathrm{Quot}(R) \to K$ by

$$F(\tfrac{a}{b}) = f(a)f(b)^{-1}.$$

The map is well-defined- we have $b \neq 0$, and since f is injective, we must have $f(b) \neq 0$, i.e. it is a unit. Now, for $\frac{a}{b}, \frac{c}{d} \in \mathrm{Quot}(R)$,

$$\begin{aligned} F(\tfrac{a}{b} + \tfrac{c}{d}) &= F(\tfrac{ad+bc}{bd}) \\ &= f(ad + bc)f(bd)^{-1} \\ &= [f(a)f(d) + f(b)f(c)] \cdot f(b)^{-1}f(d)^{-1} \\ &= f(a)f(b)^{-1} + f(c)f(d)^{-1} \\ &= F(\tfrac{a}{b}) + F(\tfrac{c}{d}), \end{aligned}$$

and

$$\begin{aligned} F(\tfrac{a}{b} \cdot \tfrac{c}{d}) &= F(\tfrac{ac}{bd}) \\ &= f(ac)f(bd)^{-1} \\ &= [f(a)f(b)^{-1}] \cdot [f(c)f(d)^{-1}] \\ &= F(\tfrac{a}{b})F(\tfrac{c}{d}). \end{aligned}$$

So, F is a ring homomorphism. Moreover, for all $r \in R$,

$$F(\iota(r)) = F(\tfrac{r}{1}) = f(r)f(1)^{-1} = f(r) \cdot 1 = f(r),$$

meaning that $F \circ \iota = f$.

Next, we show that the field homomorphism is unique. So, let $G\colon \mathrm{Quot}(R) \to K$ such that $G \circ \iota = f$. In that case, for $\frac{a}{b} \in \mathrm{Quot}(R)$,

$$G(\tfrac{a}{b}) = G(\tfrac{a}{1} \cdot \tfrac{1}{b}) = G(\tfrac{a}{1})G(\tfrac{b}{1})^{-1} = f(a)f(b)^{-1} = F(\tfrac{a}{b}).$$

This implies that $G = F$, meaning that F is unique. □

Definition 1.3.13. Let R be an integral domain. Then, the field $\mathrm{Quot}(R)$ is the *field of fractions* in R, or the *quotient field* of R.

1.4 Polynomial Rings

Proposition 1.4.1. *Let R be a commutative ring. Then, R is an integral domain if and only if $R[x]$ is an integral domain.*

Proof. First, assume that R is not an integral domain. In that case, there exist $a, b \in R$ non-zero such that $ab = 0$. Hence, $a, b \in R[x]$ still satisfy $ab = 0$. So, $R[x]$ is not an integral domain.

Now, assume that $R[x]$ is not an integral domain. In that case, there exist $f, g \in R[x]$ non-zero such that $fg = 0$. Without loss of generality, assume that f and g are not constant[1]. Now, denote

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad g(x) = b_m x^m + \cdots + b_1 x + b_0,$$

for $m, n \geq 1$ and $a_n, b_m \neq 0$. In that case, since $fg = 0$, we must have $a_n b_n = 0$. So, $a_n \in R$ is a zero divisor, meaning that R is not an integral domain. $\square$

Proposition 1.4.2 (Division Algorithm)**.** *Let K be a field and let $f, g \in K[x]$ with $g \neq 0$. Then, there exist unique $q, r \in K[x]$ such that*

$$f(x) = g(x)q(x) + r(x)$$

with $r = 0$ or $\deg r < \deg g$.

Proposition 1.4.3. *Let R be a field, and let $a \in R$. Then, the map $ev_a \colon R[x] \to R$ given by $ev_a(f) = f(a)$ is a ring homomorphism, with kernel $\ker ev_a = (x - a)$.*

Proof. Let $f, g \in R[x]$. Then,

$$ev_a(f + g) = (f + g)(a) = f(a) + g(a) = ev_a(f) + ev_a(g)$$

and

$$ev_a(f \cdot g) = (f \cdot g)(a) = f(a) \cdot g(a) = ev_a(f) \cdot ev_a(g).$$

So, ev_a is a ring homomorphism.

Now, we show that $\ker ev_a = (x - a)$. So, let $f \in (x - a)$. By definition, we can find a $g \in R[x]$ such that $f(x) = (x - a)g(x)$. In that case,

$$ev_a(f) = f(a) = 0 \cdot g(a) = 0,$$

meaning that $f \in \ker ev_a$. Next, let $f \in \ker ev_a$. By the division algorithm, we can find $q, r \in R[x]$ such that

$$f(x) = (x - a)q(x) + r(x),$$

where $r = 0$ or $\deg r < 1$. So, r is a constant. Since

$$f(a) = (a - a)q(a) + r(a) \iff 0 = r(a),$$

meaning that $r = 0$. Hence, $f \in (x - a)$. So, $\ker ev_a = (x - a)$. $\square$

Corollary 1.4.4. *Let K be a field. Then, $K[x]$ is a principal ideal domain.*

[1] If either function is a constant, we can multiply by x and we still have $fg = 0$.

Proof. Let $I \subseteq K[x]$ be an ideal. If $I = \{0\}$, then $I = (0)$. Otherwise, let $f \in I$ be a polynomial of minimal degree. Now, let $g \in I$. By the division algorithm, there exist $q, r \in K[x]$ such that

$$g = qf + r,$$

with $r = 0$ or $\deg r < \deg f$. We have

$$r = g - qf \in I$$

since I is an ideal. By the minimality of the degree of f, we must have that $r = 0$. That is, $g = qf \in (f)$. Hence, $I = (f)$. □

Definition 1.4.5. Let K be a field. We say that the polynomial ring K is *algebraically closed* if every non-constant polynomial in $K[x]$ has a root in K.

Proposition 1.4.6. *Let K be a field. Then, the following are equivalent:*

1. *A non-constant polynomial in $K[x]$ of degree n has n roots in K;*
2. *K is algebraically closed;*
3. *Every non-constant polynomial in $K[x]$ splits into linear factors in $K[x]$.*

Proof. Trivially, we have (1) $\implies$ (2).

(2) $\implies$ (3) We prove this by the order of the polynomial $f \in K[x]$. So, if $f \in K[x]$ is (monic) of degree 1, then $f(x) = ax + b$, which is trivially split into linear factors in $K[x]$. Now, assume that $f \in K[x]$ has degree n, for some $n > 1$. Since K is algebraically closed, it has a root $\alpha_1 \in K$. We apply the division algorithm to find $q, r \in K[x]$ such that

$$f(x) = q(x)(x - \alpha_1) + r(x),$$

with r a constant function. We find that $r(\alpha_1) = 0$, so $r = 0$. Hence, $f(x) = q(x)(x - \alpha_1)$, so $\deg q = n - 1$. By induction, q factors into linear factors in $K[x]$, i.e.

$$q(x) = (x - \alpha_2) \dots (x - \alpha_n).$$

Hence,

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

So, the result follows.

(3) $\implies$ (1) Let $f \in K[x]$ be of degree n. We know that

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

So, f has n roots- $\alpha_1, \alpha_2, \dots, \alpha_n \in K$.

□

Theorem 1.4.7 (Fundamental Theorem of Algebra)**.** *The field $\mathbb{C}$ is algebraically closed.*

Proposition 1.4.8. *Let R and S be rings, $s \in S$ and let $f\colon R \to S$ be a ring homomorphism. Then, there exists a unique ring homomorphism $F\colon R[x] \to S$ such that $F(a) = f(a)$ for all $a \in R$ and $F(x) = s$.*

Proof. Define the map F as follows: for

$$g(x) = a_n x^n + \cdots + a_1 x + a_0,$$

define

$$F(g) = f(a_n)s^n + \cdots + f(a_1)s + f(a_0).$$

Clearly, F is a ring homomorphism with $F(x) = s$, and $F(a) = f(a)$ for all $a \in R$.

Now, let $F'\colon R[x] \to S$ be a ring homomorphism such that $F'(a) = f(a)$ for all $a \in R$ and $F(x) = s$. In that case, for $g \in R[x]$ satisfying

$$g(x) = a_n x^n + \cdots + a_1 x + a_0,$$

we have

$$\begin{aligned} F'(g) &= F'(a_n x^n + \cdots + a_1 x + a_0) \\ &= F'(a_n)F'(x)^n + \cdots + F'(a_1)F'(x) + F'(a_0) \\ &= f(a_n)s^n + \cdots + f(a_1)s + a_0 = F(g). \end{aligned}$$

So, F is unique. □

Definition 1.4.9. Let K be a field. The field of fractions $\mathrm{Quot}(K[x])$ is called the *field of rational fractions over K*.

Definition 1.4.10. Let K be a field, and let $f, g \in K[x]$. We say that g *divides* f if there exists a $q \in K[x]$ such that $f = gq$. If so, we write $g \mid f$.

Definition 1.4.11. Let K be a field and let $f, g \in K[x]$. The *greatest common divisor* (gcd) of f and g is a polynomial $d \in K[x]$ such that:

- $d \mid f$ and $d \mid g$;
- if $e \mid f$ and $e \mid g$, then $e \mid d$.

We denote $\gcd(f, g) = d$.

Theorem 1.4.12. *Let K be a field and let $f, g \in K[x]$ be non-zero. Then, there exist $a, b \in K[x]$ such that $af + bg = \gcd(f, g)$.*

Definition 1.4.13. Let R be an integral domain and let $f \in R[x]$ be a non-constant polynomial. We say that f is *irreducible over R* if $f \in R[x]$ is irreducible.

Theorem 1.4.14. *Let K be a field. Then, $f \in K[x]$ factorises into irreducible factors, and the factorisation is unique up to reorder and multiplication by non-zero constants.*

Proposition 1.4.15. *Let K be a field and let $f \in K[x]$ be a non-constant polynomial. If $\alpha_1, \dots, \alpha_k$ are the roots of f in K, with multiplicities $m_1, \dots, m_k$, then*

$$f(x) = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \dots (x - \alpha_k)^{m_k} q(x),$$

where $q \in K[x]$ has no roots. In particular, a polynomial of degree n has at most n roots in K, counted with multiplicities.

Lemma 1.4.16 (Gauss' Lemma)**.** *Let $f \in \mathbb{Z}[x]$ be a polynomial that is irreducible over $\mathbb{Z}$. Then, f is irreducible over $\mathbb{Q}$.*

Proof. Let f be reducible over $\mathbb{Q}$. In that case, $f = gh$, for $g, h \in \mathbb{Q}[x]$. Since $g, h \in \mathbb{Q}[x]$, we can find an $N \in \mathbb{Z}_{\geq 1}$ such that $Nf = g'h'$, for $g', h' \in \mathbb{Z}[x]$. Now, denote

$$\begin{aligned} f(x) &= a_n x^n + \dots + a_1 x + a_0 \\ g'(x) &= b_s x^s + \dots + b_1 x + b_0 \\ h'(x) &= c_t x^t + \dots + c_1 x + c_0. \end{aligned}$$

We claim that for any prime p dividing N, either $p \mid b_i$ for all $0 \leq i \leq s$ or $p \mid c_j$ for all $0 \leq j \leq t$. Assume, for a contradiction, that this is not the case. In that case, there exist minimal $0 \leq i \leq s$ and $0 \leq j \leq t$ such that $p \nmid b_i c_j$. Then,

$$N \cdot a_{i+j} = (b_0 c_{i+j} + \dots + b_{i-1} c_{j+1}) + b_i c_j + (b_{i+1} c_{j-1} + \dots + b_{i+j} c_0).$$

By the minimality of N, we find that $p \mid b_k$ for $0 \leq k \leq i - 1$ and $p \mid c_l$ for $0 \leq l \leq j - 1$. Since $p \nmid b_i c_j$, we must have that $p \nmid N \cdot a_{i+j}$, meaning that $p \nmid N$. This is a contradiction. So, either $p \mid b_i$ for all $0 \leq i \leq s$ or $p \mid c_j$ for all $0 \leq j \leq t$. So, we can go through the prime factorisation of N to cancel each prime number from the factorisation, and still find either $f = gh$ or $f = (-g)h$. Either way, f is reducible in $\mathbb{Z}$. $\square$

Proposition 1.4.17 (Eisenstein's Criterion)**.** *Let*

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be a polynomial of degree n. If there exists a prime p such that:

- *$a_0, a_1, \dots, a_{n-1}$ are divisible by p;*
- *a_n is not divisible by p;*
- *a_0 is not divisible by p^2.*

Then, f is irreducible over $\mathbb{Q}$.

Proof. Let f be of degree $n > 1$, with $f = gh$, where

$$\begin{aligned} g(x) &= b_r x^r + b_{r-1} x^{r-1} + \dots + b_0 \in \mathbb{Z}[x], \\ h(x) &= c_s x^s + c_{s-1} x^{s-1} + \dots + c_0 \in \mathbb{Z}[x]. \end{aligned}$$

We have $p \mid a_0$ and $p^2 \nmid a_0$, with $a_0 = b_0 c_0$, p must divide precisely one of b_0 and c_0. Without loss of generality, assume that $p \nmid b_0$ and $b \mid c_0$. Similarly, since $p \nmid a_n = b_r c_s$, we have $p \nmid b_r$ and $p \nmid c_s$. So, there exists a minimal $m \leq s$ such that $p \mid c_m$, and $p \mid c_k$ for $0 \leq k < m$. In that case,

$$a_m = b_0 c_m + (b_1 c_{m-1} + \cdots + b_m c_0).$$

We know that $p \nmid b_0$ and $p \nmid c_m$, so $p \nmid b_0 c_m$. Hence, $p \nmid a_m$. So, we find that $m = n$. Therefore, $\deg g = 0$, meaning that f is irreducible over $\mathbb{Z}$. So, Gauss' Lemma tells us that f is irreducible over $\mathbb{Q}$. $\square$

Proposition 1.4.18. *Let R be an integral domain, $f \in R[x]$ and let $a \in R$. Then, $f(x)$ is irreducible over R if and only if $f(x+a)$ is irreducible over R.*

Proof. Assume that $f(x)$ is reducible over R. In that case, there exist non-constant polynomials $g, h \in R[x]$ such that $f(x) = g(x)h(x)$. In that case, $f(x+a) = g(x+a)h(x+a)$. Since $\deg(g(x+a)) = \deg(g(x))$ and $\deg(h(x+a)) = \deg(h(x))$, we find that $f(x+a)$ is reducible over R. Similarly, if $f(x+a)$ is reducible over R, then $f(x+a) = f((x+a)-a)$ is reducible over R. $\square$

Proposition 1.4.19. *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ and let p be a prime not dividing a_n. Let $f + p\mathbb{Z} \in \mathbb{F}_p[x]$ be given by*

$$(f + p\mathbb{Z})(x) + (a_n + p\mathbb{Z})x^n + \cdots + (a_1 + p\mathbb{Z})x + (a_0 + p\mathbb{Z}).$$

If $f + p\mathbb{Z}$ is irreducible over $\mathbb{F}_p$, then f is irreducible over $\mathbb{Q}$.

Proof. Assume that f is reducible over $\mathbb{Q}$. In that case, $f = gh$, for non-constant polynomials g and h such that $\deg f = \deg g + \deg h$. Now, denote

$$g(x) = b_p x^p + \cdots + b_1 x + b_0, \qquad h(x) = c_q x^q + \cdots + c_1 x + c_0.$$

Since p does not divide a_n, and $a_n = b_p c_q$, p does not divide b_p and c_q. So, we have $f + p\mathbb{Z} = (g + p\mathbb{Z})(h + p\mathbb{Z})$, for $g + p\mathbb{Z}$ and $h + p\mathbb{Z}$ are non-constant polynomials. Hence, $f + p\mathbb{Z}$ is reducible over $\mathbb{F}_p$. $\square$