Rice University
Department of Mathematics

Introduction to Ring Theory

June 11, 2021

Chapter 1

Fundamentals of Rings

1.1 Introduction to Rings

Definition 1.1.1: Rings

A ring is a non-empty set with two operations, $+$ and $\cdot$. The $+$ operation is commutative, associative, has an identity, and inverses for all elements. The $\cdot$ operation is associative. Both operations have two distributive rules, namely, for all a, b, c,

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$

If multiplication is commutative, then it is a commutative ring. If in addition, multiplication has an identity, and an inverse for all except the additive inverse, then it is a field.

Unless specified otherwise, we will assume our rings have a multiplicative identity.

Definition 1.1.2: Zero Divisors and Units

Let R be a ring. A nonzero element $a \in R$ is called a **zero divisor** if there exists a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.

An element $u \in R$ is called a **unit** in R if there is a $v \in R$ such that $uv = vu = 1$– that is, u has a multiplicative inverse. The set of units in R is denoted R^X.

Every element besides 0 is a unit in a field. We can also see that units form a group under multiplication.

Notice that zero divisors and units are distinct concepts– a zero divisor can never be a unit.

Definition 1.1.3: Integral Domain

A commutative ring is called an **integral domain** if it has no zero divisors.

Proposition 1.1.1

Let $a, b, c \in R$ be elements of a ring with a not a zero divisor. Then

$$ab = ac \implies a = 0 \text{ or } b = c$$

In particular, if R is an integral domain this always holds.

Exercise 1.1.1

Prove that any finite integral domain is a field.
(Hint: consider $x \mapsto ax$ for a nonzero)

1.2 Subring, Ideals, Quotient rings, Ring homomorphisms

Definition 1.2.1: Subring

A subring is a subset S of a ring R which is a ring under the restriction of the operations in R. We denote this by $S \leq R$.

Remark 1.2.1

$S \leq R$ nonempty is a subring if and only if $a, b \in S \implies a+b, ab, -a \in S$. This is equivalent to $a, b \in S \implies a-b, ab \in S$.

Definition 1.2.2: Ideal

An ideal is a subring $I \leq R$ which is closed under multiplication with elements of R. Notationally, we say that $I \triangleleft R$.

Remark 1.2.2

I nonempty is an ideal if and only if $a, b \in I \implies a - b \in I$, which is equivalent to $a \in I, r \in R \implies ar, ra \in I$.

Exercise 1.2.1

Show that a field has only trivial ideals.

Definition 1.2.3: Principal Ideal

If R is commutative and has an identity, then the principal ideal generated by c is the ideal $(c) = \{rc \mid r \in R\}$.

This is the smallest ideal containing c.

Definition 1.2.4: Ring Homomorphism

Let R, S be rings. A map $\varphi : R \to S$ that preserves operations is a **ring homomorphism**. In other words,

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

Note that $\varphi(0) = 0$ and $\varphi(-a) = -\varphi(a)$. Furthermore, the kernel of a ring homomorphism is an ideal

Definition 1.2.5: Isomorphism

Let R, S be rings. A function $\varphi : R \to S$ that is bijective and a ring homomorphism is a **isomorphism**. If there exists a isomorphism between two rings, we say the rings are **isomorphic**.

Proposition 1.2.1: Equivalence of Isomorphism

A ring homomorphism $\varphi : R \to S$ is an isomorphism if and only if $\mathrm{Ker}\varphi = \{0\}$ and $\mathrm{Im}\varphi = S$

This is of course equivalent to φ being bijective.

Definition 1.2.6: Residue Class

The equivalence class of the integer a with the congruence relation, denoted by $\overline{a}_n$, is the set

$$\{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$

In other words, the set of integers congruent to $a \pmod n$ is the **residue class** of the integer a modulo n.

We can arbitrarily pick an element from a residue class as our representative when working with other residue classes– this greatly simplifies calculations.

Definition 1.2.7: Coset

Let $I \triangleleft R$. A **coset** denoted $r + I$ is the set

$$\{r + i \mid i \in I\}.$$

Proposition 1.2.2

Two cosets are either equal or disjoint.

We define addition and multiplication of cosets by

$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I)(s + I) = rs + I$$

Definition 1.2.8: Sum and Products of Ideals

Let $I, J \triangleleft R$. Then we define:

$$I + J := \{a + b \mid a \in I,\ b \in J\},$$
$$IJ := \{a_1b_1 + a_2b_2 + \ldots + a_nb_n \mid a_i \in I,\ b_i \in J,\ n \in \mathbb{Z}_+\}$$
$$I^n = \left\{ \sum_{j=1}^{m} \{a_1a_2 \ldots a_n \mid a_i \in I\}_j \mid m \in \mathbb{Z}_+ \right\}$$

Equivalently, we can inductively define $I^n = II^{n-1}$.

Definition 1.2.9: Quotient Ring

Let $I \triangleleft R$. We notate by R/I the **quotient ring**, which is the ring with all of the cosets of I as elements, using the coset addition and multiplication defined above.

Theorem 1.2.1: First Isomorphism Theorem

Let $\varphi : R \to S$ be a ring homomorphism. Then $R/\mathrm{Ker}\varphi \cong \mathrm{Im}\varphi$.

Proof. We know that

$$a + \mathrm{Ker}\varphi = b + \mathrm{Ker}\varphi \iff \varphi(a) = \varphi(b).$$

Let $\psi : R/\mathrm{Ker}\varphi \to \mathrm{Im}\varphi$ be the map defined by $a + I \mapsto \varphi(a)$. This map is well-defined and bijective. Now it suffices to show that ψ is a ring homomorphism.

$$\psi\left((a + \mathrm{Ker}\varphi) + (b + \mathrm{Ker}\varphi)\right) = \psi\left((a + b) + \mathrm{Ker}\varphi\right) = \varphi(a + b) = \varphi(a) + \varphi(b)$$

which is equivalent to the sum of elements of ψ, as desired. One can check that multiplication holds the same as well. ■

This means that the homomorphism is completely determined by R.

Definition 1.2.10: Natural Homomorphism

Let $I \triangleleft R$ be an ideal of R. There exists a **natural homomorphism** $\varphi : R \to R/I$ defined by $\varphi : a \mapsto a + I$.

1.3 Direct Sums of Rings

Definition 1.3.1: Direct Sum

The **direct sum** of two rings $R_1 \oplus R_2$ (or direct product $R_1 \times R_2$) is the ring of all ordered pairs (r_1, r_2), with $r_i \in R_i$, with addition and multiplication defined by adding and multiplying the components:

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \quad (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2).$$

One can check that this indeed satisfies the properties of a ring.

Definition 1.3.2: Projection

The **projection** subsets are defined by

$$R_1^* := \{(r_1, 0) \mid r_1 \in R_1\}$$
$$R_2^* := \{(0, r_2) \mid r_2 \in R_2\}$$

These projection subsets are isomorphic to R_1, R_2 respectively. Furthermore, R_1^*, R_2^* are ideals in $R_1 \oplus R_2$, and every $c \in R_1 \oplus R_2$ has a unique decomposition $c = c_1 + c_2$ with $c_i \in R_i$.

Proposition 1.3.1: Unique Decompositions

If I, J are ideals in a ring R such that every $r \in R$ can be uniquely written as $r = i + j$, with $i \in I$, $j \in J$, then $R \cong I \oplus J$

Theorem 1.3.1: More Isomorphism Theorems

Let R be a ring.

- *(Second Isomorphism Theorem for Rings)* Let $A \leq R$ and $B \triangleleft R$. Then

$$A + B \leq R$$
$$A \cap B \triangleleft A$$
$$(A + B)/B \cong A/(A \cap B)$$

- *(Third Isomorphism Theorem for Rings* Let $I, J \triangleleft R$ with $I \subset J$. Then

$$J/I \triangleleft R/I$$
$$(R/I)/(J/I) \cong R/J$$

- Let $I \triangleleft R$. Then there is a correspondence between subrings $A < R$ that contain an ideal I and the subrings of R/I by $A \leftrightarrow A/I$. Furthermore, if $A \leq R$ contains I, then $A \triangleleft R$ if and only if $A/I \triangleleft R/I$.

1.4 Important Ring Examples

Quadratic Integer Rings

Let D be a rational number that is not a perfect square in $\mathbb{Q}$ and define

$$\mathbb{Q}(\sqrt{D}) = \left\{ a + b\sqrt{D} \mid a, b \in \mathbb{Q} \right\}$$

as a subset of $\mathbb{C}$. One can check that the set is closed under subtraction and under the multiplication defined by

$$(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$$

shows that it is closed under multiplication. Hence $\mathbb{Q}(\sqrt{D}) \leq \mathbb{C}$ as a subring (and of $\mathbb{R}$ if $D > 0$) and hence is commutative with identity.

The assumption that D is not a square allows us to write every element of $\mathbb{Q}(\sqrt{D})$ uniquely in the form $a + b\sqrt{D}$. Furthermore, if a, b are not both zero, then $a^2 - Db^2 \neq 0$, and because

$$(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$$

then if $a + b\sqrt{D} \neq 0$ we have

$$(a + b\sqrt{D})^{-1} = \frac{a - b\sqrt{D}}{a^2 - Db^2}.$$

This shows that every nonzero element in the commutative ring is a unit and hence $\mathbb{Q}(\sqrt{D})$ is a field called a **quadratic field**.

The rational number D can be written by $D = q^2 D'$ for some rational number q and a unique integer D', where $z^2 \not| D'$ for all $z \in \mathbb{Z}_+$ greater than 1. We call D' the **squarefree part** of D. Because $\sqrt{D} = q\sqrt{D'}$ it holds that $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$, and hence we can use squarefree integers instead in the definition of the quadratic field.

Let D be a squarefree integer. One can check that

$$\mathbb{Z}[\sqrt{D}] = \left\{ a + b\sqrt{D} \mid a, b \in \mathbb{Z} \right\}$$

forms a subring of the quadratic field $\mathbb{Q}(\sqrt{D})$. In the case where $D \equiv 1 \pmod 4$, then we can form a slightly larger subring by

$$\mathbb{Z}\left[\frac{1 + \sqrt{D}}{2}\right] = \left\{ a + b\frac{1 + \sqrt{D}}{2} \mid a, b \in \mathbb{Z} \right\}.$$

Now define

$$\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$
$$\omega = \begin{cases} \sqrt{D} & D \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \pmod 4 \end{cases}.$$

We call $\mathcal{O}$ the **ring of integers** in the quadratic field $\mathbb{Q}(\sqrt{D})$– despite the fact that elements are not actually integers. This terminology arises because the properties of $\mathcal{O}$ are similar to those of $\mathbb{Z} \leq \mathbb{Q}$ as subrings. In fact, we will later see that it is the *integral closure* of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{D})$.

In the special case where $D = -1$, we obtain the ring $\mathbb{Z}[i]$ of **Gaussian integers**. We will cover the Gaussian integers later, as they have important ties to number theory.

Definition 1.4.1: Field Norm

Define the **field norm** $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ by

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Q}$$

This norm gives a notion of size in the field. For example, when $D = -1$, the norm of $a + bi$ is $a^2 + b^2$.

One can check that N is **multiplicative**– that is, $N(\alpha\beta) = N(\alpha)N(\beta)$. We can also see that on the subring $\mathcal{O}$ the field norm is given by

$$N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = \begin{cases} a^2 - Db^2 & D \equiv 2, 3 \pmod 4 \\ a^2 + ab + \frac{1-D}{4}b^2 & D \equiv 1 \pmod 4 \end{cases}$$
$$\overline{\omega} = \begin{cases} -\sqrt{D} & D \equiv 2, 3 \pmod 4 \\ \frac{1-\sqrt{D}}{2} & D \equiv 1 \pmod 4 \end{cases}$$

And hence $N(\alpha)$ is in fact an integer for every $\alpha \in \mathcal{O}$. This in fact characterizes the units of $\mathcal{O}$– if $\alpha \in \mathcal{O}$ has field norm $N(\alpha) = \pm 1$, then

$$(a + b\omega)^{-1} = \pm(a + b\overline{\omega})$$

and hence α is a unit. The multiplicative property directly tells us that the converse holds, and hence $\alpha \in \mathcal{O}$ is a unit if and only if $N(\alpha) = \pm 1$.

In number theory, finding solutions to the equation $x^2 - Dy^2 = \pm 1$ is equivalent to the determination of units in $\mathcal{O}$.

Exercise 1.4.1

Show that if $D > 0$ then the group of units $\mathcal{O}^\times$ is always infinite. Find a class of units in $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ that exemplifies this.

Show that $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ has only a finite number of elements, and list them. Are there other values of D with more units than $\{\pm 1\}$?

Polynomial Rings

Definition 1.4.2: Polynomial Ring

Let R be a commutative ring. We define a **polynomial** in x to be the formal sum

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

where $n \geq 0$ and $a_i \in R$. If $a_n \neq 0$, then the polynomial is of **degree** n, and $a_n x^n$ is te **leading term** (a_n is the **leading coefficient**). Furthermore, we say the polnyomial is **monic** if $a_n = 1$.

The set of all such polynomials is called the **ring of polynomials in** $\mathbb{R}$ and will be denoted $R[x]$. We define addition and multiplication by the standard version from algebra:

$$(a_n x^n + \ldots + a_1 x + a_0) + (b_n x^n + \ldots + b_1 x + b_0) = (a_n + b_n)x^n + \ldots + (a_1 + b_1)x + (a_0 + b_0)$$
$$(a_0 + a_1 x + a_2 x^2 + \ldots) \times (b_0 + b_1 x + b_2 x^2 + \ldots) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots$$

That is, the coefficient in the product of x^k is $\sum_{i=0}^{k} a_i b_{k-i}$.

We can see that $R \leq R[x]$ as the **constant polynomials**. Notice further that $R[x]$ is also a commutative ring.

Proposition 1.4.1

Let R be an integral domain and let $p(x), q(x) \in R[x]$ be nonzero polynomials. Then the degree of $p(x)q(x) = \deg p(x) + \deg q(x)$.

The units of $R[x]$ are exactly the same units of R, and $R[x]$ is an integral domain.

If R has zero divisors, then $R[x]$ does as well. We can also see that $S \leq R \implies S[x] \leq R[x]$.

Example 1.4.1

Consider the polynomial ring $(\mathbb{Z}_3[x]$. This ring consists of nonnegative powers of x with coefficients in $\{0, 1, 2\}$ with calculations being done in modulus 3. For example, let

$$p(x) = x^2 + 2x + 1 \quad q(x) = x^3 + x + 2.$$

Then

$$p(x) + q(x) = x^3 + x^2$$
$$p(x)q(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2$$

Polynomials behave very differently even under simple modulus structures.

We will see more of polynomial rings after building more theory.

Matrix Rings

Definition 1.4.3: Matrix Rings

Let R be a ring and $n \in \mathbb{Z}_+$. We define $M_n(R)$ to be the set of all $n \times n$ matrices with entries in R. The element $A \in M_n(R)$ is an $n \times n$ square array of elements of R whose entry in row i and column j is $A_{ij} \in R$. We see that this set of matices becomes a ring under the usual matrix addition and multiplication, called the **matrix ring of rank** n.

Notice that if $n \geq 2$, then $M_n(R)$ is not commutative, regardless of the commutativity of R. Furthermore, it will also have zero divisors.

We say $A \in M_n(R)$ is a **scalar matrix** if $a_{ii} = a$ for all $i \in \{1, \ldots, n\}$, and $a_{ij} = 0$ if $i \neq j$. This forms a subgring of $M_n(R)$, and is in fact isomorphic to R. If R is commutative, the scalar matrices commute with all elements of $M_n(R)$.

Note that the units of $M_n(R)$ are the invertible $n \times n$ matrices– this forms a subgroup called the **general linear group of degree n over R** (written by $GL_n(R)$).

Similar to polynomial rings, if $S \leq R$, then $M_n(S) \leq M_n(R)$. Another subring is the set of upper triangular matrices.

Group Rings

Definition 1.4.4: Group Rings

Let R be a commutative ring and G a finite group. The **group ring RG of G** is the set of all sums

$$RG = \{a_1 g_1 + a_2 g_2 + \ldots + a_n g_n \mid a_i \in R, g_i \in G\}$$

We define addition and multiplication by

$$(a_1 g_1 + a_2 g_2 + \ldots + a_n g_n) + (b_1 g_1 + b_2 g_2 + \ldots + b_n g_n) = (a_1 + b_1) g_1 + (a_2 + b_2) g_2 + \ldots + (a_n + b_n) g_n$$
$$(a_1 g_1 + \ldots + a_n g_n)(b_1 g_1 + \ldots + b_n g_n) = \sum_{g_i g_j = g_k} (a_i b_j) g_k$$

where the multiplication is the natural construction derived from defining $(a g_i)(b g_j) = (ab)(g_i g_j)$.

RG is commutative if and only if G is commutative. We can see $R \leq RG$ by the "constant" sums of $a_i e_G$. In fact, $G \leq RG$ as well by taking $a_i = e_R$, and because elements of G has inverses, G is a subgroup of the group of units of RG.

If $|G| > 1$ then RG has zero divisors, given by

$$(1 - g)(1 + g + \ldots + g^{m-1}) = 1 - g^m = 1 - 1 = 0$$

where g is an element with order $m > 1$.

If S is a subring of R then $SG \leq RG$. Similarly, if $H \leq G$, then $RH \leq RG$.

Example 1.4.2: $\mathbb{Z}D_8$

Let $G = D_8$ be the dihedral group of order 8 and $R = \mathbb{Z}$. Some example of elements in $\mathbb{Z}D_8$ could be $\alpha = r + r^2 - 2s$ and $\beta = -3r^2 + rs$, and one can see that

$$\alpha + \beta = r - 2r^2 - 2s + rs$$
$$\alpha\beta = (r + r^2 - 2s)(-3r^2 + rs) = r(-3r^2 + rs) + r^2(-3r^2 + rs) - 2s(-3r^2 + rs) = -3 - 5r^3 + 7r^2 s + r^3 s$$

Example 1.4.3: $\mathbb{R}Q_8$

An interesting example is the group ring $\mathbb{R}Q_8$. This ring is distinct from the Hamilton quaternions $\mathbb{H}$ even though $Q_8 \subset \mathbb{H}$. The unique element of order 2 in Q_8 is NOT the additive inverse of 1 in $\mathbb{R}Q_8$, even though it is in $\mathbb{H}$. It also contains zero divisors and hence is not a division ring.

However, if one takes the quotient $\mathbb{R}Q_8/\left(1 + (-1), i + (-i), j + (-j), k + (-k)\right)$, then it is isomorphic to $\mathbb{H}$.

In other words, we only apply the group operation between elements of the group ring when multiplying two elements. The group elements hence serve as sort of a basis, that interacts multiplicatively via the group action.

Rings of Fractions

Let R be a commutative ring. Recall that if we have a non-zero non-zero divisor element $a \in R$, then $ab = ac \implies b = c$. This property is similar to division even if a is not a unit. Our goal will be to define a larger ring $Q \geq R$ so that elements like a are units. This becomes particularly useful when R is an integral domain, as then Q becomes a field known as the **field of fractions** or **quotient field**.

Theorem 1.4.1

Let R be a commutative ring and $D \subset R$ a subset without 0, zero divisors, and is closed under multiplication. Then there is a commutative ring Q such that $R \leq Q$ and for all $d \in D$, $d \in Q$ is a unit.

Furthermore, every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. If $D = R - \{0\}$, then Q is a field.

The ring Q is the smallest ring containing R in which all elements of D become units. That is, let S be a commutative ring and $\varphi : R \to S$ be an injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi \mid_R = \varphi$. In other words, any other ring that makes D into units must contain an isomorphic copy of Q.

We call the ring Q the **ring of fractions of** D and denote it by $D^{-1}R$. If R is integral, then Q is the **field of fractions** of R.

What does this actually look like? Caution must be exercised, as when dealing with fractions we are dealing with equivalence classes. Hence we will define an equivalence class on (r, d) with $r \in R$ and $d \in D$ by

$$\frac{r}{d} = \{(a, b) \mid a \in R,\ b \in D,\ rb = ad\}$$

Then Q is the set of equivalence classes $\frac{r}{d}$. Then we define addition and multiplication by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

We leave it as an exercise to verify that this indeed gives Q the structure of a commutative ring. We embed R into Q by defining

$$\iota : R \to Q \quad \iota : r \mapsto \frac{rd}{d}$$

for any $d \in D$. This is obviously in the equivalence class of $\frac{re}{e}$, so the choice of d does not matter. This is a ring homomorphism and is in fact injective because d is not a zero divisor, and so this tells us that $\iota(R) \leq Q$ is isomorphic to R.

We can also see that $d \in D$ has a multiplicative inverse in Q as desired. That is,

$$\left(\frac{de}{e}\right)^{-1} = \frac{e}{de}$$

and one can see that every element of Q can be written by $r \cdot d^{-1}$ for some $r \in R$ and $d \in D$.

Remark 1.4.1

Recall that if $A \subset F$ is a subset of a field, then the intersection of all the subfields of F containing A is a subfield of F called the **subfield generated by** A.

This subfield is the smallest subfield of F containing A.

Corollary 1.4.1

Let R be an integra domain and Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R then the subfield of F generated by R' is isomorphic to Q.

1.5 Properties of Ideals

Definition 1.5.1

Let $A \leq R$ be a subset of a ring R.

- The **ideal generated by** A is the smallest ideal of R containing A, written by (A).
- $$RA = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}_+\}$$
  $$AR = \{a_1r_1 + a_2r_2 + \ldots + a_nr_n \mid a_i \in A,\ r_i \in R,\ n \in \mathbb{Z}_+\}$$
  $$RAR = \{r_1a_1r_1' + r_2a_2r_2' + \ldots + r_na_nr_n' \mid r_i, r_i' \in R,\ a_i \in A,\ n \in \mathbb{Z}_+\}$$
  are the **left, right, and two-sided ideal generated by** A.
- If $|A| = n < \infty$, then (A) is a **finitely generated ideal**.
- If $|A| = 1$ then (A) is a **principal ideal**.

If $A = \{a_1, a_2, \ldots\}$ then we write $(A) = (a_1, a_2, \ldots)$ for simplicity. Notice that $b \in R$ is in (a) if and only if $b = ra$ for some $r \in R$, which is equivalent to $(b) \subset (a)$.

Proposition 1.5.1

Let $I \triangleleft R$. Then $I = R$ if and only if there exists a unit $u \in I$.

If R is commutative, then R is a field if and only if the only ideals of R are 0 and R.

Corollary 1.5.1

If R is a field and R' an arbitrary ring, then any nonzero ring homomorphism $\varphi : R \to R'$ is injective.

Definition 1.5.2: Maximal Ideal

A proper ideal M of a ring R is a **maximal ideal** of R if there does not exist another ideal of R that contains M besides R itself.

Every proper ideal is containd in a maximal ideal.

Theorem 1.5.1: Classification of Maximal Ideals

Let R be a commutative ring with identity and M an ideal in R. Then M is a maximal ideal of R if and only if R/M is a field.

Definition 1.5.3: Prime Ideal

A proper ideal P in a commutative ring R is a **prime ideal** if whenever $ab \in P$, then either $a \in P$ or $b \in P$.

Note that it is possible to define prime ideals in a noncommutative setting.

Proposition 1.5.2

Let R be a commutative ring with identity $1_R \neq 0$. Then P is a prime ideal in R if and only if R/P is an integral domain.

As an example, note that every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$, and that $\mathbb{Z}_n$ is an integral domain only when n is prime. This is why ideals of the form $\mathbb{Z}_p$ are viewed as prime ideals.

Corollary 1.5.2

Every maximal ideal in a commutative ring with identity is also a prime ideal.

Chinese Remainder Theorem

All rings are assumed to be commutative in this section.

An important question in number theory is the notion in $\mathbb{Z}$ of two integers n, m being relatively prime. In the integers, it turns out that this question is equivalent to the equation $nx + my = 1$ having solutions in $\mathbb{Z}$. We can extend this question to arbitrary rings, and if we view $\mathbb{Z}$ as an ideal, then the problem is equivalent to $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ as ideals. This motivates a more general definition:

Definition 1.5.4: Comaximal

The ideals $A, B \triangleleft R$ are said to be **comaximal** if $A + B = R$.

Recall that if $A = (a)$ and $B = (b)$, then the product of the ideals can be calculated to be $AB = (ab)$.

Theorem 1.5.2: Chinese Remainder Theorem

Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$\begin{aligned} R &\to R/A_1 \times R/A_2 \times \ldots \times R/A_k \\ r &\mapsto (r + A_1, r + A_2, \ldots, r + A_k) \end{aligned}$$

is a ring homomorphism with $\mathrm{Ker}\varphi = A_1 \cap A_2 \cap \ldots \cap A_k$. If or each $i, j \in \{1, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and

$$\begin{aligned} A_1 \cap A_2 \cap \ldots \cap A_k &= A_1 A_2 \ldots A_k \\ &\implies R/(A_1 A_2 \ldots A_k) \cong R/A_1 \times R/A_2 \times \ldots \times R/A_k. \end{aligned}$$

Proof. ■

Since the isomorphism is an isomorphism of rings, it follows that the units on both sides must be isomorphic. Because the units in direct products of rings are the elements with units in all coordinates, it follows that we have an isomorphism on the group of units.

Corollary 1.5.3

Let $n \in \mathbb{Z}_+$ and let $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

by ring isomorphism, and so

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$

We can use this to prove some remarkable results. For example, it directly gives us the formula for the Euler φ-function:

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k})$$

and hence shows that φ is a multiplicative function when a and b are relatively prime positive integers. Combining the above with the simple fact that

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$$

gives us the value of φ on all positive integers.

Chapter 2

Ideal Theory of Rings

2.1 Additional Structure on Integral Domains

Definition 2.1.1: Norm of Integral Domain

Let R be an integral domain. Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0)$ is called a **norm** on the integral domain R. If $N(a) > 0$ for $a \neq 0$ then N is a **positive norm**

This is a pretty loose construction, and an integral domain can have many norms on it.

Definition 2.1.2: Euclidean Function

An integral domain R is a **Euclidean Domain** if there exists a norm called the **Euclidean function** $N : R \setminus \{0\} \to \mathbb{N}$ that satisfies $\forall a, b \in R \setminus \{0\}$:

$$N(ab) \geq \max\{N(a), N(b)\}$$
$$\exists q, r \in R \text{ such that } a = qb + r \text{ and } [r = 0 \text{ or } N(r) < N(b)]$$

We call the element q the **quotient** and the element r the **remainder**.

The existence of a Euclidean function is integral to constructing a Euclidean algorithm to perform division of elements $a, b \in R$. We can perform successive divisions to get

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

where r_n is the last nonzero remainder. This r_n always exists as the norms form a decreasing sequence of nonnegative integers. However, these elements are not necessarily unique.

Proposition 2.1.1

Every ideal in a Euclidean Domain is principal. That is, if $I \triangleleft R$ is a nontrivial ideal in R, then $I = (d)$ for some nonzero element of I with minimum norm.

This also makes it convenient to show an integral domain is not a Euclidean Domain by simply finding a non-principal ideal. Moreover, it motivates the notion of greatest common divisors from $\mathbb{Z}$ into comumutative rings.

Definition 2.1.3: Greatest Common Divisor

Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$. Then a is said to be a **multiple** of b if there exists an element $x \in R$ with $a = bx$. In this case, we say b **divides** a (or is a **divisor** of a) written $b \mid a$.

A **greatest common divisor** of a, b is a nonzero element d such that

$$d \mid a,\ d \mid b$$
$$d' \mid a\ d' \mid b \implies d' \mid d$$

We will denote a greatest common divisor by $\gcd(a, b)$, or sometimes simply (a, b) if it is clear from context.

If $gcd(a, b) = 1_R$, then we say that a and b are **relatively prime**.

We can easily extend this to finite sequences of elements $(a_1, a_2, \ldots, a_n)$.

Recall that in a ring $b \mid a \iff a \in (b) \iff (a) \subset (b)$. Hence, we can discuss greatest common factors in terms of ideals. That is, if $I = (a, b)$ is the ideal of R generated by a, b, then $d = \gcd(a, b)$ if $I \subset (d)$ and if $I \subset (d') \implies (d) \subset (d')$. Thus, it is the unique smallest principal ideal containing a and b. However, it may not exist in all rings.

Proposition 2.1.2: Sufficient Conditions for Existence

If $a, b \in R$ are nonzero elements in a commutative ring such that $I = (a, b) = (d)$, then d is the greatest common divisor of a, b.

Obviously this is a sufficient and not a necessary condition. But it also clarifies why (a, b) is used both for ideals and greatest common divisors. Any integral domain that satisfies the above condition for all ideals of two elements is called a **Bezout Domain**.

Proposition 2.1.3

Let R be an integral domain. If two elements $d, d' \in R$ generate the same principal ideal, i.e. $(d) = (d')$, then $d' = ud$ for some unit $u \in R$. In particular, this tells us that greatest common divisors are unique up to units.

Theorem 2.1.1

Let R be a Euclidean Domain and let $a, b \in R$ be nonzero. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a, b described earlier. Then $d = \gcd(a, b)$ and $(d) = (a, b)$. That is, d can be written as an R-**linear combination** of a, b:

$$d = ax + by$$

for some $x, y \in R$.

Notice that x, y are not unique in this case. One can show that that if x_0, y_0 are solutions to

$$ax + by = N$$

then any other solutions are of the form

$$x = x_0 + m\frac{b}{(a, b)}$$
$$y = y_0 - m\frac{a}{(a, b)}$$

for $m \in \mathbb{Z}$. This is really strong as it gives a complete solution of the first order Diophantine equation provided we have one solution. Our work here essentially tells us that $ax + by = N$ is solvable in integers x, y if and only if $\gcd(a, b) \mid N$.

Proof. ■

Finally, we discuss a definition that is useful to determine whether an integral domain is a Euclidean Domain.

Definition 2.1.4: Universal Side Divisor

Let R be an integral domain, and define $\tilde{R} = R^\times \cup \{0\}$. We say an element $u \in R - \tilde{R}$ is a **universal side divisor** if for every $x \in R$ there is a $z \in \tilde{R}$ such that

$$u \mid x - z$$

That is, every x can be written

$$x = qu + z$$

where z is either zero or a unit.

Proposition 2.1.4

Let R be an integral domain that is not a field. If R is a Euclidean Domain, then there exist universal side divisors in R.

It is often simpler to show that an integral domain can't have universal side divisors by assuming one exists of minimal norm, finding candidates, then showing they fail to satisfy the necessary properties.

Exercise 2.1.1

Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field with quadratic integer ring $\mathcal{O}$ and field norm N.

- Suppose $D \in \{-1, -2, -3, -7, -11\}$. Prove that $\mathcal{O}$ is a Euclidean Domain with respect to N.
- Suppose that $D \in \{-43, -67, -163\}$. Prove that $\mathcal{O}$ is not a Euclidean Domain with respect to any norm.

These numbers are specially chosen because they are the only negative values of D that makes every ideal in $\mathcal{O}$ principal.

Principal Ideal Domains

Definition 2.1.5: Principl Ideal Domain

A **Principal Ideal Domain** is an integral domain in which every ideal is principal.

We have already shown that every Euclidean Domain is a Principal Ideal Domain. The converse does not hold. The biggest difference from a practicality angle is that while PIDs have gcds, there is no algorithm to compute them.

Proposition 2.1.5

Let R be a Principal Ideal Domain and let $a, b \in R$ be nonzero. Let d be a generator for the principal ideal generated by a, b. Then $d = \gcd(a, b)$ and can be written as an R-linear combination

$$d = ax + by$$

for $x, y \in R$. Finally, d is unique up to multiplication by a unit.

Recall that maximal ideals are always prime ideals but the converse is not true in general. Fortunately, PIDs have enough structure so this holds.

Proposition 2.1.6

Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Proof. ■

Corollary 2.1.1

If R is any commutative ring such that $R[x]$ is a PID, then R is necessarily a field.

Proof. ■

We construct some definitions that help us distinguish PIDs and EDs.

Definition 2.1.6: Dedeking-Hasse Norm

Define N to be a **Dedekind-Hasse norm** if N is a positive norm and for every $a, b \in R$ nonzero either $a \in (b)$ or there exists $s, t \in R$ with $0 < N(sa - tb) < N(b)$ (that is, a nonzero element in the ideal (a, b) with norm smaller than b).

This is a weakening of the Euclidean condition. R is an ED with respect to a positive norm N if it is always possble to satisfy the above condition with $s = 1$.

Proposition 2.1.7

The integral domain R is a PID if and only if R has a Dedeking-Hasse norm.

Example 2.1.1

Unique Factorization Domain

Unique Factorization Domains capture the idea that some rings admit a proper factorization on elements.

Definition 2.1.7: Reducibility and Primes

Let R be an integral domain

- Suppose $r \in R$ is nonzero and not a unit. Then r is called **irreducible in** R if for all $a, b \in R$, $r = ab$ implies that either a or b is a unit. Otherwise, we say r is **reducible**.
- Let $p \in R$ be nonzero. We say it is **prime in** R if the ideal (p) is a prime ideal. An equivalent statement is that p is not a unit and if $p \mid ab$, then $p \mid a$ or $p \mid b$.
- If $a = ub$ for $a, b \in R$ and $u \in R$ a unit, then we say a and b are **associates**.

Proposition 2.1.8

In an integral domain, a prime element is always irreducible.

The converse does not hold in general. However, in a PID, the converse does hold.

Proof. ■

This is also a useful tool to show a ring is not a PID.

Definition 2.1.8: Proper Factorization

Let $a \in R$ be a nonzero nonunit. A **proper factorization** of a is a finite product $a = p_1 p_2 \dots p_n$, where p_i are not units of R. If this exists, we say $\{p_i\}$ are **proper factors** of a.

Of course, an irreducible element has no proper factorizations.

Definition 2.1.9: Unique Factorization Domain

An integral domain R is a **unique factorization domain** if every nonzero, non-unit element has a proper factorization

$$r = p_1 p_2 \dots p_n$$

where $\{p_i\}$ are irreducible elements and unique up to associates and reordering.

It turns out that primes are equivalent to irreducibles in a UFD as well.

Proposition 2.1.9

In a Unique Factorization Domain, a nonzero element is a prime if and only if it is an irreducible.

We will also see that UFDs admit a greatest common divisor via its factorization

Proposition 2.1.10

Let $a, b \in R$ be nonzero elements of a UFD R and suppose

$$a = u p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$
$$b = v p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$$

are prime factorizations with u, v units, primes $p_1, p_2, \dots, p_n$ distinct, and exponents $e_i, f_i \geq 0$. Then the element

$$d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_n^{\min(e_n, f_n)}$$

is a greatest common divisor of a and b.

Exercise 2.1.2

Let R be a UFD.

(a). Let b and $a_1, \dots, a_s$ be nonzero elements of R. For $d \in R$, show that

$$bd = gcd(ba_1, \dots, ba_s) \iff d = gcd(a_1, \dots, a_s)$$

(b). Let $f(x) \in R[x]$ where $f(x) = bf_1(x)$ for $f_1(x)$ **primitive** (i.e. $gcd(\text{coefficients of } f_1(x)) = 1_R$). Show that

$$b = gcd(\{\text{coefficients of } f(x)\}).$$

This leads us to the full description of the structure of these domains.

Theorem 2.1.2

Every Principal Ideal Domain is a Unique Factorization Domain. Hence, every Euclidean Domain is a Unique Factorization Domain.

Proof. ■

This forms a strict classification hierarchy by

Euclidean Domains $\subset$ **Principal Ideal Domains** $\subset$ **Unique Factorization Domains** $\subset$ **Integral Domains** $\subset$ **commutative rings**

Corollary 2.1.2

The integers $\mathbb{Z}$ are a UFD.

Corollary 2.1.3

Let R be a PID. Then there exists a multiplicative Dedekind-Hausse norm on R.

2.2 Gaussian Integers

Definition 2.2.1: Gaussian Integers

The Gaussian integers are elements of the quadratic integer ring $\mathbb{Z}[i]$. Elements of the ring are the complex numbers $a+bi \in \mathbb{C}$ with $a, b \in \mathbb{Z}$. The field norm N maps

$$a+bi \mapsto a^2+b^2$$

and hence the units$u$ are given by

$$N(a+bi) = a^2+b^2 = \pm 1 \implies u \in \{\pm 1, \pm i\}$$

In general, let $\mathcal{O}$ be a quadratic integer ring and N the associated field norm. The multiplicity of the norm gives us a natural irreducibility condition.

Exercise 2.2.1

Let $\alpha \in \mathcal{O}$ be an element such that $N(\alpha) = \pm p$ for a prime $p \in \mathbb{Z}$. Then α is irreducible in $\mathcal{O}$.

Let $\pi \in \mathcal{O}$ be a prime element. Observe that $(\pi) \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Because $N(\pi)$ is a nonzero integer, we have that $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$ for some integer prime p. Hence $\pi \mid p$ in $\mathcal{O}$– this hints that we can find the prime elements of $\mathcal{O}$ by determing how primes in $\mathbb{Z}$ factor as elements of $\mathcal{O}$.

Suppose $\pi \mid p$ in $\mathcal{O}$. Then

$$N(\pi)N(\pi') = N(p) = p^2 \implies N(\pi) = \pm p^2 \text{ or } N(\pi) = \pm p$$

If the first holds, then π' is a unit and $p = \pi$ is irreducible in $\mathbb{Z}[i]$. If the second holds, then π' is also irreducible and $p = \pi\pi'$ is the product of precisely two irreducibles.

Now returning to the case of the Gaussian integers, it follows that p factors in $\mathbb{Z}[i]$ into precisely two irreducibles if and only if $p = a^2+b^2$ for $a, b \in \mathbb{Z}$. Otherwise, it remains irreducible in $\mathbb{Z}[i]$. If $p = a^2+b^2$ then the irreducible elements in $\mathbb{Z}[i]$ are $a \pm bi$.

Example 2.2.1: Factoring an even prime

Clearly $2 = 1^2+1^2$ and so we get a factorization

$$2 = (1+i)(1-i) = -i(1+i)^2$$

In fact, $(1+i)$ and $(1-i)$ are associates– this is the only situation in which conjugate irreducibles can be associates.

Since $a^2 \equiv 0 \pmod 4$ or $a^2 \equiv 1 \pmod 4$ for any integer $a \in \mathbb{Z}$, an odd prime in $\mathbb{Z}$ that satisfies $p = a^2 + b^2$ must be congruent to $1 \pmod 4$. Hence, if p is a prime of $\mathbb{Z}$ and $p \equiv 3 \pmod 4$ then p is irreducible in $\mathbb{Z}[i]$. In fact, in the first case with $p \equiv 1 \pmod 4$, p must factor into two distinct irreducibles $(a + bi)(a - bi)$.

Lemma 2.2.1

The prime number $p \in \mathbb{Z}$ divides an integer of the form $n^2 + 1$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

The Gaussian integers admit a nice Euclidean algorithm that is key to factoring primes further.

Theorem 2.2.1

The Gaussian integers $\mathbb{Z}[i]$ form a Euclidean Domain.

Proof. We will show that $f(\alpha) = N(\alpha)$ suffices. Observe that

$$\begin{aligned} \alpha = \beta\rho + \theta &\iff \\ \frac{\alpha}{\beta} = \rho + \frac{\theta}{\beta} &\iff \\ \frac{\alpha}{\beta} - \rho = \frac{\theta}{\beta} &\iff \\ \left|\frac{\alpha}{\beta} - \rho\right| < 1 & \end{aligned}$$

Of course, this is the distance between $\frac{\alpha}{\beta}$ and ρ. But there always exists a lattice point within distance 1 of any $\mathbb{C}$, and so therefore the statement holds. ■

Theorem 2.2.2: Fermat's Theorem on sum of squares

The prime p can be written as $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ if and only if $p = 2$ or $p \cong 1 \pmod 4$. The representation of p as the sum of two squares is unique.

This is the last key piece we need to classify all prime elements of Gaussian integers.

Theorem 2.2.3: Prime elements of Gaussian integers

All Gaussian primes take on the form:

- $\varepsilon(1 + i)$
- εq, where q is prime and $q \equiv 3 \pmod 4$
- π where $N(\pi)$ is a prime with $N(\pi) \equiv 1 \pmod 4$

where ε is a unit.

Why is it important to classify all prime elements of $\mathbb{Z}[i]$? We will see shortly that this allows us to approach number theory questions by factoring primes in $\mathbb{Z}[i]$.

Proposition 2.2.1: Disjoint Partitions of Fields

Let F be a field. Then we can partition F into disjoint sets by taking all sets of the form

$$\left\{a, -a, a^{-1}, (-a)^{-1}\right\}$$

where $a \in F$ is non-zero. The union of all sets of this form with $\{0\}$ forms a partition of F.

Theorem 2.2.4: Two Squares Theorem

Consider the equation $x^2+y^2=n$, and let $n=2^\alpha p_1^{\beta_1}\dots p_r^{\beta_r}q_1^{\gamma_1}\dots q_s^{\gamma_s}$ be the Gaussian factorization of n. Then, $x^2+y^2=n$ is solvable in $\mathbb{Z}$ if and only if all γ_j are even. Furthermore, the number of solutions is

$$4\prod_{j=1}^{r}(\beta_j+1)$$

Proof. First, we write $n=x^2+y^2=(x+yi)(x-yi)$. Using the Gaussian factorization, we rewrite

$$n=2^\alpha p_1^{\beta_1}\cdot\ldots\cdot q_1^{\gamma_1}\cdot\ldots=(-i)^\alpha(1+i)^{2\alpha}\pi_1^{\beta_1}\overline{\pi_1}^{\beta_1}\cdot\ldots\cdot q_1^{\gamma_1}$$

Now observe that

$$\begin{aligned}(x+yi)\mid n &\implies x+yi=\varepsilon(1+i)^{\alpha'}\pi_1^{\beta_1'}\overline{\pi_1}^{\beta_1''}\cdot\ldots\cdot q_1^{\gamma_1'}\cdot\ldots\\ &\implies x-yi=\overline{\varepsilon}(1-i)^{\alpha'}\overline{\pi_1}^{\beta_1'}\pi_1^{\beta_1'}\cdot\ldots\cdot q_1^{\gamma_1}\end{aligned}$$

Then because

$$n=(x+yi)(x-yi)$$

We have

$$\begin{aligned}2\alpha=\alpha'+\alpha' &\iff \alpha'=\alpha\\ \beta_1=\beta_1'+\beta_1'' &\iff \beta_1'=0,1,\dots,\beta_1;\beta_1''=\beta_1-\beta_1'\\ \gamma_1=\gamma_1'+\gamma_1' &\iff \gamma_1\text{ even},\gamma_1'=\frac{\gamma_1}{2}\\ (-i)^\alpha=\varepsilon\overline{\varepsilon}(-i)^\alpha &\iff 1=\varepsilon\overline{\varepsilon}\text{ which always holds}\end{aligned}$$

Thus, the equation is always solvable if all the γ are even. Looking at the above, the number of solutions will be

$$1\cdot(\beta_j+1)\cdot 1\cdot 4=4\prod_{j=1}^{r}(\beta_j+1)$$

■

Chapter 3

Polynomial Rings and Reducibility

For posterity we restate the definition of a polynomial ring.

Definition 3.0.1: Polynomial Ring

Let R be a commutative ring. We define a **polynomial** in x to be the formal sum

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

where $n \geq 0$ and $a_i \in R$. If $a_n \neq 0$, then the polynomial is of **degree** n, and $a_n x^n$ is te **leading term** (a_n is the **leading coefficient**). Furthermore, we say the polnyomial is **monic** if $a_n = 1$.

The set of all such polynomials is called the **ring of polynomials in** $\mathbb{R}$ and will be denoted $R[x]$. We define addition and multiplication by the standard version from algebra:

$$(a_n x^n + \ldots + a_1 x + a_0) + (b_n x^n + \ldots + b_1 x + b_0) = (a_n + b_n)x^n + \ldots + (a_1 + b_1)x + (a_0 + b_0)$$
$$(a_0 + a_1 x + a_2 x^2 + \ldots) \times (b_0 + b_1 x + b_2 x^2 + \ldots) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots$$

That is, the coefficient in the product of x^k is $\sum_{i=0}^{k} a_i b_{k-i}$.

Recall that $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ if $p, q \neq 0$. Furthermore, the units of $R[x]$ are the units of R, and $R[x]$ is an integral domain.

Proposition 3.0.1

Let $I \triangleleft R$ be an ideal and let $(I) = I[x]$ denote the ideal in $R[x]$ generated by I. Then

$$R[x]/(I) \cong (R/I)[x]$$

and hence if I is a prime ideal of R, (I) is a prime ideal of $R[x]$.

This does not hold for maximal ideals, but (I, x) is maximal in $R[x]$ if I is maximal in R.

Definition 3.0.2: Polynomial Rings over Multiple Variables

We inductively define the **polynomial ring in the variables** $x_1, x_2, \ldots, x_n$ with coefficients in R to be

$$R[x_1, x_2, \ldots, x_n] := R[x_1, x_2, \ldots, x_n][x_n]$$

Hence, we can view polynomial rings of multiple variables as polynomial rings on a single variable, with polynomials of $n-1$ variables as coefficients.

We say a polynomial is **homogeneous** if all its terms have the same degree. If f is a nonzero polynomial in n variables, the sum of all monomial terms in f of degree k is called the **homogeneous component of** f **of degree** k.

3.1 Polynomial Rings over Fields

Let $R = F$ be a field. We can define a natural norm on $F[x]$ by

$$N(p(x)) = \deg(p(x)).$$

Theorem 3.1.1

Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. This implies that if $a(x), b(x) \in F[x]$ with $b(x)$ nonzero, then

$$a(x) = q(x)b(x) + r(x)$$

where $q(x), r(x) \in F[x]$ are unique polynomials, and $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$.

Proof. ■

Of course, this tells us that $F[x]$ is a PID and a UID.

In fact, the quotient and remainder in the division algorithm are *independent of field extensions*. That is, if $F \subset E$ is a field extension, then $b(x) \mid a(x)$ in $E[x]$ if and only if $b(x) \mid a(x)$ in $F[x]$, and $\gcd(a(x), b(x))$ is the same in both fields.

Proposition 3.1.1

The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition 3.1.2

Let $g(x) \in F[x]$ be nonconstant and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \dots f_k(x)^{n_k}$$

be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \dots \times F[x]/(f_k(x)^{n_k}).$$

Notice that if $f(x)$ has roots $\alpha_1, \alpha_2, \dots, \alpha_k$ in F, then $f(x)$ has $(x-\alpha_1)\dots(x-\alpha_k)$ as a factor. In other words, a polynomial of degree n over a field has at most n roots in F.

Proposition 3.1.3

A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then $F^\times$ is a cyclic group.

Proof. ■

Corollary 3.1.1

Let p be a prime. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes $\pmod p$ is cyclic.

Corollary 3.1.2

Let $n \geq 2$ be an integer with factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

with $p_1, \dots, p_r$ are distinct. Then

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times,$$

in particular $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$ for all $\alpha \geq 2$.

Finally, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$ for all odd primes p.

These describe the group theory structure of the automorphism group of the cyclic group $\mathbb{Z}_n$, as $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. ■

3.2 Polynomial Rings and UFDs

Definition 3.2.1: Primitive

A polynomial $f(x) \in R[x]$ is **primitive** if $\gcd(\{\text{coeff of } f(x)\}) = 1_R$

Recall that since R is an integral domain, one can form its field of fractions by

$$F := \mathrm{Frac}(R) = \left\{ \frac{r}{s} \mid r, s \in R,\ s \neq 0 \right\}$$

Lemma 3.2.1: Gauss' Lemma

Let R be a UFD with $F = \mathrm{Frac}(R)$.

- If $f(x), g(x) \in R[x]$ are primitive, then so is $f(x) \cdot g(x)$.
- Take $f(x) \in R[x]$. Then $f(x) = \varphi(x)\psi(x) \in F[x]$ with $\deg(\varphi)\deg(\psi) \geq 1 \iff f(x) = \psi(x)\varphi(x)$ in $R[x]$.

The elements of the ring R become units in the UFD $F[x]$.

Corollary 3.2.1

Let R be a UFD. The irreducible elements of $R[x]$ are of two types:

- nonzero scalar polynomials that are irreducible as elements of R
- primitive polynomials in $R[x]$ that are irreducible in $F[x]$

Essentially, a polynomial $p(x)$ with $\deg(p(x)) \geq 1$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.

Theorem 3.2.1

R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.

Proof. ■

By induction, it holds that $R[x_1, x_2, \dots, x_n]$ is a UFD if and only if R is a UFD.

3.3 Irreducibility Criteria

If R is an integral domain, then for $f(x) \in R[x]$ monic, of degree > 0, is irreducible if and only if $f(x)$ cannot be factored as a product of two polynomials of deg ≥ 1. Fortunately, we have a few tools to get irreducibility of polynomials, such as Gauss' Lemma.

Another direction we can take is roots:

Proposition 3.3.1

Let $f(x) \in F[x]$ for F a field. Then

- $f(x)$ has a degree 1 factor if and only if $f(x)$ has a root α in F, i.e. $\exists \alpha \in F$ such that $f(\alpha) = 0$
- $f(x)$ of degree 2 or 3 is reducible if and only if $f(x)$ has a root in F

If we look at $R = \mathbb{Z}$ and $F = \mathbb{Q}$ specifically, we have more options.

Proposition 3.3.2: Rational Root Test

Let $f(x) = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x]$.

- If $\frac{r}{s} \in \mathbb{Q}$ with $gcd(r, s) = 1$ and $\frac{r}{s}$ is a root of $f(x)$, then $r \mid a_0$ and $s \mid a_n$.
- If $f(x) \in Z[x]$ is monic and if $f(\alpha) \neq 0$ for all $\alpha \in \mathbb{Z}$ dividing α_0, then $f(x)$ has no roots in $\mathbb{Q}$.

Unfortunately, while these theorems are powerful, they are relatively dependent on the polynomial being of low degree. Ideals can help us extend these ideas to higher degree polynomials.

Proposition 3.3.3

Let R be an integral domain, and let $I \triangleleft R$ be a proper ideal of R. Take $f(x) \in R[x]$ a monic polynomial of degree ≥ 1. If the image of $f(x)$ in $(R/I)[x]$ is irreducible, then $f(x)$ is irreducible in $R[x]$.

While nice, unfortunately many irreducible polynomials are reducible when modulated by the ideal.

Theorem 3.3.1: Eisenstein-Schonemann Criteria

Let P be a prime ideal of an integral domain R, and take

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

to be a monic polynomial in $R[x]$ of degree ≥ 1. Suppose $a_{n-1}, \ldots, a_1, a_0 \in P$ and $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.

A trick we can use to help apply this is that if $f(x)$ doesn't satisfy the criteria, use $f(x - c)$ and try again. If it is (ir)reducible for $f(x - c)$, it is ir(reducible) for $f(x)$.

3.4 Noetherian Rings and Grobner Basis

Definition 3.4.1: Noetherian and Artinian Rings

A ring is **Noetherian** if it satisfies the ascending chain condition; there is no infinite strictly increasing chain $I_1 < I_2 < \ldots$ of ideals of R.

A ring is **Artinian** if it satisfies the descending chain condition; there is no infinitely strictly chain $I_1 > I_2 > \ldots$ of ideals of R.

For the sake of this section, we will only need to deal with Noetherian rings. We will see both types however when working with modules.

Proposition 3.4.1: Equivalent Definitions

A ring R is Noetherian if and only if every ideal of R is finitely generated.

A ring R is Artinian if and only if it is Noetherian and every prime ideal is maximal.

Principal ideal domains are Noetherian because every ideal in such a ring is generated by one element. A Noetherian ring always has a finite chain of increasing prime ideals– in an Artinian ring, the chain terminates immediately.

Corollary 3.4.1

Let R be a Noetherian ring. Every proper ideal I of R is contained in a maximal ideal.

Theorem 3.4.1: Hilbert Basis Theorem

Let R be a Noetherian ring. The polynomial ring $R[x]$ is Noetherian.

Proposition 3.4.2: Quotients of Noetherian

Let R be a Noetherian ring, and let I be an ideal of R. Any ring that is isomorphic to the quotient ring $\overline{R} = R/I$ is Noetherian.

Corollary 3.4.2

Let P be a polynomial ring in a finite number of variables over the integers/field. Any ring R that is isomorphic to the quotient ring P/I is Noetherian.

Lemma 3.4.1

Let R be a ring, let I be an ideal of the polynomial ring $R[x]$. The set A whose elements are the leading coefficients of the nonzero polynomials in I, together with the zero element of R, is an ideal of R, the **ideal of leading coefficients**.

Proof. ■

Because a field is clearly Noetherian, we get an interesting result:

Corollary 3.4.3

Every ideal in the polynomial ring $F[x_1, x_2, \ldots, x_n]$ is finitely generated.

The colection of leading coefficients of polynomials in $I \triangleleft R[x]$ form a useful ideal in R that characterizes I. We can utilize this to study $F[x_1, x_2, \ldots, x_n]$, but we need to exercise caution– we need an ordering on the monomials in order to determine the leading term of a polynomial.

Definition 3.4.2: Monomial Ordering

A **monomial ordering** is a well ordering on the set of polynomials that satisfies $mm_1 \geq mm_2$ whenever $m_1 \geq m_2$ for monomials m, m_1, m_2.

Definition 3.4.3: Leading Terms

Fix a monomial ordering on the polynomial ring $F[x_1, x_2, \ldots, x_n]$. The **leading term** of a nonzero polynomial $f \in F[x_1, x_2, \ldots, x_n]$, denoted $LT(f)$, is the monomial term of maximal order in f. The **multidegree of** f, denoted $\partial(f)$, is the multidegree of the leading term of f.

If I is an ideal in $F[x_1, x_2, \ldots, x_n]$, the **ideal of leading terms**, denoted $LT(I)$, is the ideal generated by the leading terms of all the elements in the ideal:

$$LT(I) = (LT(f) \mid f \in I).$$

It is clear that the choice of ordering affects the leading term and hence the multidegree of a polynomial. Notice that $\partial(fg) = \partial f + \partial g$ when f and g are nonzero, and hence $LT(fg) = LT(f) + LT(g)$.

By construction, $LT(I)$ is generated by monomials. We refer to these kinds of ideals as **monomial ideals**.

Exercise 3.4.1

Show that a polynomial $p(x)$ is contained in the monomial ideal $(f_1(x), f_2(x), \ldots, f_n(x))$ (where $f_i(x)$ is a monomial) if and only if each of the monomial terms of $p(x)$ is a multiple of one of the generators $f_i(x)$.

If $I = (f_1, \ldots, f_m)$, notice that $LT(I)$ contains the ideals of each of the leading terms:

$$(LT(f_1), \ldots, LT(f_m)) \subset LT(I).$$

This inequality can in fact be strict.

Example 3.4.1

The intuition behind this strange fact is that while a smaller polynomial may not be in $(LT(f_1), LT(f_2), \ldots, LT(f_n))$, one could potentially generate polynomials by canceling out the leading terms of f_1, f_2. Hence it is natural to look for a basis that generates these smaller polynomials as well.

Definition 3.4.4: Grobner Basis

A **Grobner basis** for an ideal I in $F[x_1, \ldots, x_n]$ is a finite set of generators $\{g_1, \ldots, g_m\}$ for I whose leading terms generate the ideal of all leading terms in I:

$$I = (g_1, \ldots, g_m) \quad LT(I) = (LT(g_1), \ldots, LT(g_m)).$$

Notice that it is a basis in the sense that it is a set of generators– it is not a basis in the sense of vector spaces.

A Grobner basis allows for every polynomial to be written uniquely as a sum of elements in I and remainder r. Hence, it is a tool that allows us to give back more structure to multivariable polynomial rings.

General Polynomial Division

Let $F[x_1, \ldots, x_n]$ be a monomial ordering and suppose $g_1, \ldots, g_m \in F[x_1, \ldots, x_n]$ is a set of nonzero polynomials. If $f \in F[x_1, \ldots, x_n]$ then we construct a set of quotients $q_1, \ldots, q_m$ and a remainder r (initially all zero) and test if $LT(f)$ is divisible by $LT(g_i)$ in order.

If $LT(g_i) \mid LT(f)$, i.e $LT\,(= a_i LT(g_i))$, then $q_i' = q_i + a_i$ and $f' = f - a_i g_i$, and reiterate.

Once the leading term $LT(f)$ is not divisible by any $LT(g_1), \ldots, LT(g_m)$, set $r' = r + LT(f)$ and $f' = f - LT(f)$ and reiterate.

The process terminates when $f = 0$ and results in a set of quotients and remainder such that:

$$f = q_1 g_1 + \ldots + q_m g_m + r.$$

Notice that $q_i g_i$ has multidegree less than or equal to the multidegree of f. Furthermore, no nonzero term in r is divisible by any $LT(g_i)$.

Unfortunately, the remainder is dependent on the choices of g_i, and is nonunique. In fact, sometimes the remainder is zero for the right choice of g_i, but not others, making it difficult to utilize the factorization. Of course, our Grobner basis is the right tool to fix this.

Theorem 3.4.2

Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and suppose $g_1, \ldots, g_m$ is a Grobner basis for the nonzero ideal $I \triangleleft R$. Then every polynomial f can be written uniquely as

$$f = f_I + 4$$

where $f_I \in I$ and no nonzero monomial term of r is divisible by $LT(g_i)$.

Both f_I and r are computed by general polynomial division by $g_1, \ldots, g_m$ and are independent of the order of g_i.

Finally, the remainder r provides a unique representative for the coset of f in $F[x_1, \ldots, x_n]/I$. This also tells us that $f \in I$ if and only if $r = 0$.

Proof. ■

Now we will see that if we have a well-defined division algorithm for some set of polynomials, that they must be a Grobner basis.

Proposition 3.4.3

Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and let $I \triangleleft R$ be nonzero. If $g_1, \ldots, g_m \in I$ such that

$$LT(I) = (LT(g_1), \ldots, LT(g_m))$$

then $g_1, \ldots, g_m \in I$ is a Grobner basis for I.

For any ideal $I \triangleleft R$ nonzero, the ideal has a Grobner basis.

Now our goal is to form some criterion to determine whether a set of generators forms a Grobner basis. Recall that our main difficulty in forming a nice basis is that it is possible to cancel leading terms of two polynomials. One way this is done is via the equation below:

$$S(f_1, f_2) := \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2.$$

where M is the monic lcm of $LT(f_1), LT(f_2)$. One can see that this in fact causes the leading terms of f_1, f_2 to cancel.

Lemma 3.4.2

Suppose $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ are polynomials with multidegree α and determined so that

$$h = a_1 f_1 + \ldots + a_m f_m$$

with constants $a_i \in F$ has strictly smaller multidegree. Then

$$h = \sum_{i=2}^{m} b_i S(f_{i-1}, f_i)$$

for some constants $b_i \in F$.

We can use this to show that a set of generators is Grobner if there are no new leading terms among $S(g_i, g_j)$.

Remark 3.4.1

Let $R = F[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_m\}$. We write $f \equiv r \pmod{G}$ if r is the remainder obtained by general polynomial division of f by polynomials $g1, \ldots, g_m$.

Proposition 3.4.4: Buchberger's Criterion

Let $R = F[x_1, \ldots, x_n]$ and fix a monomial ordering on R. If $I = (g_1, \ldots, g_m)$ is a nonzero ideal in R, then $G = \{g_1, \ldots, g)m\}$ is a Grobner basis for I if and only if $S(g_i, g_j) \equiv 0 \pmod{G}$ for $1 \leq i < j \leq m$.

Proof. ■

We can use this to form a new algorithm to find a Grobner basis.

Buchberger's Algorithm

Let $I = (g_1, \ldots, g_m)$. If $S(g_i, g_j)$ leaves a remainder of 0 when divided by $G = \{g_1, \ldots, g_m\}$ using general polynomial division, then G is a Grobner basis. Otherwise, we proceed with the algorithm.

If G is not a Grobner basis, then $S(g_i, g_j)$ has a nonzero remainder r. We increase G by appending the polynomial $g_{m+1} = r$ to form

$$G' = \{g_1, \ldots, g_m, g_{m+1}\}$$

and repeat general polynomial division.

This procedure terminates after a finite number of steps, and will result in a generating set G that satisfies Buchberger's Criterion.

If $\{g_1, \ldots, g_m\}$ is a Grobner basis for the ideal I, and $LT(g_i) \mid LT(g_j)$ for some $i \neq j$, then $LT(g_j)$ can be dropped from the list without affecting the basis.

We can assume without loss of generality that the leading term of each g_i is monic. A Grobner basis $G = \{g_1, \ldots, g_m\}$ for I where $LT(g_i)$ is monic and no leading temr divides the other is called a **minimal Grobner basis**.

A minimal Grobner basis is not unique, but the number of elements and their leading terms are unique. We can impose additional restrictions to make a basis unique.

Definition 3.4.5: Reduced Grobner Basis

Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$. A Grobner basis $\{g_1, \ldots, g_m\}$ for a nonzero ideal $I \triangleleft R$ is called a **reduced Grobner basis** if each $LT(g_i)$ is monic and $LT(g_i) \not| g_j$ for $i \neq j$.

This is of course a stronger type of minimal Grobner basis. We can turn a minimal Grobner basis into a reduced Grobner basis by replacing each g_i by its remainder after division by g_j.

Theorem 3.4.3

Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$. Then there is a unique reduced Grobner basis for every nonzero ideal $I \triangleleft R$.

This is really useful to distinguish ideals in a polynomial ring.

Corollary 3.4.4

Let $I, J \triangleleft F[x_1, \ldots, x_n]$. Then $I = J$ if and only if I, J have the same reduced Grobner basis with respect to any fixed monomial ordering on $F[x_1, \ldots, x_n]$.

Example 3.4.2

Solving Algebraic Equations

We can use Grobner bases to help solve systems of algebraic equations. Suppose $S = \{f_1, \ldots, f_m\}$ is a collection of polynomials in n variables $x_1, \ldots, x_n$, and we are trying to find a solution to the system of equations $f_i = 0$ for all $i \in \{1, \ldots, m\}$. Notice that if $(a_1, \ldots, a_n)$ is a solution to this system, then every element $f \in I$ where I is generated by S also satisfies $f_1(a_1, \ldots, a_n) = 0$.

The ideas of Grobner bases allow us to expand the theory of linear polynomial equations to nonlinear polynomial equations. The process of finding elements of the ideal I independent of variables (so as to reduce the equation similar to Gauss-Jordan elimination) is part of *elimination theory*.

Definition 3.4.6: Elimination Ideal

If $I \triangleleft F[x_1, \ldots, x_n]$, then

$$I_i = I \cap F[x_{i+1}, \ldots, x_n]$$

is called the i-th **elimination ideal** of I with respect to the ordering $x_1 > \ldots > x_n$.

Proposition 3.4.5: Elimination

Suppose $G = \{g_1, \ldots, g_m\}$ is a Grobner basis for the nonzero ideal $I \triangleleft F[x_1, \ldots, x_n]$ with respect to the lexicographic monomial ordering $x_1 > \ldots > x_n$. Then

$$G \cap F[x_{i+1}, \ldots, x_n]$$

is a Grobner basis of the i-th elimination ideal

$$I_i = I \cap F[x_{i+1}, \ldots, x_n] \subset I.$$

In particular, $I_i = 0$ if and only if $G \cap F[x_{i+1}, \ldots, x_n] = \emptyset$.

Proof. ■

Example 3.4.3

Proposition 3.4.6

If $I, J \triangleleft F[x_1, \ldots, x_n]$, then

$$tI + (1-t)J \triangleleft F[t, x_1, \ldots, x_n]$$

and

$$I \cap J = (tI + (1-t)J) \cap F[x_1, \ldots, x_n].$$

Hence $I \cap J$ is the first elimination ideal of $tI + (1-t)J$ with respect to the ordering $t > x_1 > \ldots > x_n$.