

MA3203 Rings and Fields

Notes by Chan Heng Huat

April 22, 2003

Contents

1	Rings	5
1.1	Rings	5
1.2	Elementary results	9
1.3	Subrings, Ideals, Homomorphisms and Quotient rings	11
1.4	Maximal Ideals	20
1.5	Prime ideals	22
2	Polynomial Rings	23
2.1	Polynomial Rings over a field	23
2.2	The Polynomial ring $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$	32
3	Unique Factorization Domain	37
3.1	Principal Ideal Domain and Unique Factorization Domain	37
3.2	Polynomial rings over a Unique Factorization Domain	40
4	Fields	45
4.1	Examples of Fields	45
4.2	Characteristic of a field	46
4.3	A very brief excursion into Vector Spaces	46
4.4	Field Extensions	48
4.5	Finite Extension and Algebraic Extension	52
4.6	Constructibility	54
4.7	Roots of Polynomials	55
5	Groups and fields	59
5.1	Classification of Finite abelian groups	59
5.2	Wedderburn's Theorem	62

Chapter 1

Rings

Remarks : Lecture 1 of this course is missing.

1.1 Rings

Definition. A commutative ring is an integral domain if $a \cdot b = 0$ implies that $a = 0$ or $b = 0$.

This definition looks simple enough and is usually taken for granted. The reason being that the commutative rings which we know are integral domains. Now, the following example shows that we may get into trouble if we are not careful enough.

Consider the finite ring \mathbb{Z}_6 . Note that

$$[2] = [2] \cdot [4].$$

Therefore

$$[2] \cdot ([2] - [4]) = [0].$$

Eliminating $[2]$ gives $[2] = [0]$. This is clearly a contradiction. The reason why we are led to this situation is because \mathbb{Z}_6 is not an integral domain. In fact the reason behind this is that 6 is not a prime number.

The following result gives us a criterion for which the finite ring \mathbb{Z}_n is an integral domain.

Theorem 1.1.1. If n is composite, then \mathbb{Z}_n is not an integral domain.

Proof. If n is composite, then there exist a prime $p|n$, or $n = pk$. This implies that

$$[0] = [p][k].$$

But both $[p]$ and $[k]$ are not zero. This shows that \mathbb{Z}_n is not an integral domain.

The converse is true.

Theorem 1.1.2. If n is a prime then \mathbb{Z}_n is an integral domain.

Before we prove this result, we recall that if a and b are integers, then $d = \gcd(a, b)$ (greatest common divisor of a and b) is defined as the unique positive integer such that

- (1). $d|a, d|b$,
- (2). If $c|a$, and $c|b$ then $c|d$.

To prove Theorem 1.1.2, we need the following Lemma:

Lemma 1.1.3. If $\gcd(a, b) = 1$ then there exist x and y such that $ax + by = 1$.

Proof. Recall the set of integers is a cyclic group under addition. Note that a subgroup of a cyclic group is cyclic (Herstein's book p. 55, exercise 13). Now, suppose $S = \{ax + by, x, y \in \mathbb{Z}\}$. We check that S is a subgroup of \mathbb{Z} . This can be shown by proving that for any $h, k \in S$, $-h + k \in S$. This follows from the fact that

$$-h + k = -ax - by + ax' + by' = a(-x + x') + b(-y + y')$$

if $h = ax + by$ and $k = ax' + by'$. Hence, S is a cyclic group generated by, say d . In other words any element in S is of the form kd for some $k \in \mathbb{Z}$. Now since $a = a \cdot 1 + b \cdot 0$, and $b = a \cdot 0 + b \cdot 1$, $a = kd$ and $b = k'd$ for some integers k and k' . This implies that $d|a$ and $d|b$ and so, $d|\gcd(a, b)$. Therefore, $d|1$ and hence, $d = \pm 1$. This shows that $1 \in S$ and so there exist x and y such that $ax + by = 1$.

Proof of Theorem 1.1.2. We first make a simple observation. Note that if p is a prime then $\gcd(a, p) = 1$ if and only if $p \nmid a$.

Now, suppose $[a][b] = [0]$, and that $[a] \neq [0]$. Then $p \nmid a$ and therefore, $\gcd(a, p) = 1$. This implies, by Lemma 1.1.3, that there exist x and y such that $ax + py = 1$. Hence,

$$[a][x] + [py] = [1].$$

Therefore,

$$[a][x] = [1].$$

Multiplying both sides by $[b]$ gives

$$[a][b][x] = [b].$$

Since $[ab] = [0]$, this gives $[b] = [0]$ and therefore, \mathbb{Z}_p is an integral domain.

Note that Theorem 1.1.2 is indeed Euclid's Lemma, which says that if p is a prime dividing ab then $p|a$ or $p|b$.

Definition : A *Division Ring* R is a ring such that $(R \setminus \{0\}, \cdot)$ is a group.

When the above multiplicative group is commutative (or abelian), we call the division ring a *field*.

The fields that we have seen so far are $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$.

We now prove that

Theorem 1.1.4. $(\mathbb{Z}_p, +, \cdot)$ is a finite field.

The proof of this result follows immediately from the fact that if $[a] \in \mathbb{Z}_p$ is non-zero, then $p \nmid a$ and therefore $\gcd(a, p) = 1$. Hence, by Lemma 1.1.3, there exist x and y such that $ax + py = 1$ and so, $[a][x] = 1$, which implies that $[a]$ has multiplicative inverse. This argument is essentially that given in the proof of Theorem 1.1.2.

Example 1.1.4. We have shown that the set of 2×2 matrices are not commutative under multiplication. However if we restrict our attention to the subset

$$M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\},$$

then we can easily check that $(M, +, \cdot)$ is a field. It turns out this is *isomorphic* to the field \mathbb{C} .

We now consider a division ring which is not commutative.

Example 1.1.5. Consider the set

$$\mathcal{Q} = \{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \mid a_i \in \mathbb{R}\}.$$

Here $\mathbf{ii} = \mathbf{jj} = \mathbf{kk} = -1$, $\mathbf{ij} = \mathbf{k}$, $\mathbf{jk} = \mathbf{i}$, $\mathbf{ki} = \mathbf{j}$, $\mathbf{ji} = -\mathbf{k}$, $\mathbf{kj} = -\mathbf{i}$, and $\mathbf{ik} = -\mathbf{j}$. The multiplication rule then gives

$$(a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k})(b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}) = c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k},$$

where

$$\begin{aligned}c_0 &= a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 \\c_1 &= a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 \\c_2 &= a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 \\c_3 &= a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0.\end{aligned}$$

The verification of the fact that $(\mathcal{Q}, +, \cdot)$ is a ring is straightforward but tedious (especially for associativity of the multiplicative operation). We now prove that $(\mathcal{Q} \setminus \{0\}, \cdot)$ is a group by showing that every nonzero element in \mathcal{Q} has an inverse. By taking $a_0 = b_0, a_1 = -b_1, a_2 = -b_2, a_3 = -b_3$, we see that

$$c_0 = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

and that $c_i = 0, i = 1, 2, 3$. Hence

$$(a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k})(a_0 - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k}) = c_0.$$

Note that $c_0 \neq 0$ since $a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ is nonzero. Hence, the element

$$\frac{a_0}{c_0} - \frac{a_1}{c_0}\mathbf{i} - \frac{a_2}{c_0}\mathbf{j} - \frac{a_3}{c_0}\mathbf{k}$$

is the multiplicative inverse of $c_0 \neq 0$ since $a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$. Hence, \mathcal{Q} is a division ring. Note that $\mathbf{ij} = -\mathbf{ji}$ and so, the ring is non-commutative.

It is possible to identify the quaternion ring with the set of matrices

$$M = \left\{ \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ -a_1 & a_0 & -a_3 & a_2 \\ -a_2 & a_3 & a_0 & -a_1 \\ -a_3 & -a_2 & a_1 & a_0 \end{pmatrix}, a_i \in \mathbb{R} \right\}.$$

With this identification, the associativity follows from associativity of matrix multiplication.

Remarks. One can deduce the identity

$$(a_0^2 + a_1^2 + a_2^2 + a_3^2)(b_0^2 + b_1^2 + b_2^2 + b_3^2) = (c_0^2 + c_1^2 + c_2^2 + c_3^2),$$

with c_i 's are given as above in terms of a_j 's and b_k 's. This identity can of course be proved by brute force. The identity is due to L.Euler and can be used to prove the famous Lagrange Theorem, which states that every positive integer is a sum of four squares.

1.2 Elementary results

We know since the beginning of our contact with numbers that $(-1)(-1) = 1$. However, when we try to recall the reason behind this, we probably don't remember anyone telling us why this is true. In this lecture, we will learn the proof of this simple statement. Note that this statement should not be taken as an AXIOM.

Suppose R is a ring with unit 1_R . Then

Lemma 1.2.1. Let $a, b \in R$.

$$(a) \quad a \cdot 0_R = 0_R \cdot a = 0_R,$$

$$(b) \quad a \cdot (-b) = (-a) \cdot b = -(a \cdot b),$$

$$(c) \quad (-a)(-b) = a \cdot b.$$

Note that Lemma 1.2.1 (c) implies $(-1)(-1) = 1$ for $R = \mathbb{Z}$.

Proof of (a). Note $0 + 0 = 0$ (we have set $0 = 0_R$ for simplicity). Therefore by the distributive law, $a0 + a0 = a0$. Hence, $a0 = 0$, as required. The result $0a = 0$ can be proved in a similar way.

Proof of (b). Note that

$$a(b + (-b)) = a0 = 0,$$

by (a). Therefore, by the distributive law,

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

Adding $-(ab)$ to both sides and using the fact that $ab + (-(ab)) = 0$, we conclude that $a(-b) = -(ab)$. The rest of the statement follows in a similar way.

Proof of (c). Now,

$$(-a)(-b + b) = 0.$$

Therefore,

$$(-a)(-b) + (-a)(b) = 0.$$

By (b), $(-a)b = -(ab)$ implies that

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

Adding ab to both sides yield, $(-a)(-b) = ab$, which is what we want to show.

Lemma 1.2.2. In any ring R ,

$$(a + b)^2 = a^2 + ba + ab + b^2.$$

Note that the formula we are familiar with is

$$(x + y)^2 = x^2 + 2xy + y^2.$$

But the rings we dealt with before are all commutative rings. When R is not commutative, we find that

$$(a + b)(a + b) = (a + b)a + (a + b)b = a^2 + ba + ab + b^2,$$

which is Lemma 1.2.2.

Lemma 1.2.3. Suppose $x^2 = x$ holds for all $x \in R$. Then R is commutative.

Remarks.

1. Note that the result is rather “neat” since a single condition could determine the commutativity of a ring.
2. The more general result, which is due to N. Jacobson, is true. This states that if for every $a \in R$, there is an integer $n(a)$, such that $a^{n(a)} = a$, then R is commutative.
3. The ring R which has elements satisfying $x^2 = x$ for all $x \in R$ is called a Boolean ring.

Proof of Lemma 1.2.3. Note that for any $x, y \in R$,

$$(x + y)^2 = x^2 + xy + yx + y^2, \tag{1.2.1}$$

by Lemma 1.2.2. Note that by hypothesis, $(x+y)^2 = (x+y)$, $x^2 = x$, $y^2 = y$, and so,

$$x + y = x + xy + y.$$

This implies that

$$xy + yx = 0. \tag{1.2.2}$$

Next, set $x = y$ in (1.2.1), we obtain

$$(x + x)^2 = x^2 + x^2 + x^2 + x^2 = 4x^2.$$

But by hypothesis, $(x+x)^2 = (x+x)$ and $4x^2 = 4x$. Hence, we have $2x = 4x$, which implies that $2x = 0$ for all $x \in R$. Returning to (1.2.2), we find that

$$0 = xy + yx = xy + yx + 2(-yx) = xy - yx.$$

Hence, $xy = yx$ for all $x, y \in R$.

1.3 Subrings, Ideals, Homomorphisms and Quotient rings

Definition. If R is a ring, then a subring of R is a subset S of R which is a ring if the operations $a \cdot b$ and $a + b$ are the operations of R applied to $a, b \in S$.

Theorem 1.3.1. Let S be a non-empty subset of R . If $a \cdot b \in S$ and $a \pm b \in S$, then S is a subring of R .

Remarks. The statement $ab \in S$ and $a + b \in S$ simply implies that \cdot and $+$ are binary operations on S . The statements $a + b \in S$ and $a - b \in S$ says that S is an additive subgroup of R .

Proof. We must first show that S is an additive group under $+$. Note that since $+$ is a binary operation on S , we conclude that if $a \in S$, $a - a \in S$ (since $a - b \in S$ for all $a, b \in S$) and so, $0 \in S$. This shows the existence of identity since $0 + a = a = a + 0$. Next, $0 \in S$ and $a \in S$ implies that $0 - a \in S$. This implies that $-a \in S$ and so, S contains additive inverse of a for any $a \in S$. This shows the existence of inverses. Finally the Associative law holds in

S since it holds for elements in R . (Note that this proof is essentially the same as the proof of the criterion for showing that a subset of a group is a subgroup. See Herstein's book, p. 55, Exercise 15).

Next, $a \cdot b \in S$ for all $a, b \in S$. Furthermore, associative law for \cdot holds since it holds for elements in R . Finally distributive laws hold since S is a subset of R and that distributive laws hold for elements in R . This completes the proof of the Theorem.

Example 1.3.1. \mathbb{Z} is a subring of \mathbb{Q} and \mathbb{Q} is a subring of \mathbb{R} .

Example 1.3.2. The set of even integers is a subring of \mathbb{Z} but the set of odd integers is not, since the sum of two odd integers is even (and therefore $+$ is not a binary operation on the set of odd integers).

Example 1.3.3. Let R be the ring of 2×2 matrices over \mathbb{R} . The subset

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

is a subring of R .

Example 1.3.4. Let R be the set of all real-valued continuous functions on the interval $[-1, 1]$. The addition being defined as $(f + g)(x) = f(x) + g(x)$ and the multiplication is $f \cdot g(x) = f(x)g(x)$, $x \in [-1, 1]$. Let S denote the set of all real-valued differentiable functions on the interval $[-1, 1]$. Then S is a subring of R .

Our next object is a special type of subrings. They play a very important role in constructing new rings from the known ones.

Definition. An *ideal* I is a subset of R such that

- (a) I is an additive subgroup of R .
- (b) For any $r \in R$ and any $a \in I$, $ra \in I$ and $ar \in I$.

Note that an ideal is a subring : Suppose I is an ideal. Then since I is an additive subgroup of R , $a \pm b \in I$. Also, if $a, b \in I$, $ab \in I$ since I is a subset of R and we may apply (b) with either $a \in R$ or $b \in R$.

However, a subring is not necessarily an ideal. It is clear that \mathbb{Z} is a subring of \mathbb{Q} . But \mathbb{Z} is not an ideal of \mathbb{Q} . For example if we take $\frac{1}{2} \in \mathbb{Q}$ and $1 \in \mathbb{Z}$, $\frac{1}{2} \notin \mathbb{Z}$.

Example 1.3.5. The subset of R which contains only the element 0 is called the zero ideal of R . The set R is itself an ideal of R . These are called the *trivial* ideals of R .

Example 1.3.6. The only ideals of a field R are the trivial ideals. (The converse is true for commutative ring with unit. If R is a commutative ring with unit with only trivial ideals, then R is a field).

Example 1.3.7. Let R be any commutative ring. Let $a \in R$. Then the set $aR := \{ar \mid r \in R\}$ is an ideal of R . This shows that the subset $d\mathbb{Z}$ is an ideal of \mathbb{Z} for any integer d .

Example 1.3.8. Let

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$

Let

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \right\}.$$

Then I is an ideal of R .

Example 1.3.9. Let R be the ring of all real-valued continuous functions on the closed interval $[-1, 1]$. Let $I = \{f \in R \mid f(0) = 0\}$. Then I is an ideal of R .

Homomorphisms

Let φ be a mapping from $(R, +, \cdot)$ to $(R', +', \cdot')$ which satisfies

(a) $\varphi(a + b) = \varphi(a) +' \varphi(b)$,

(b) $\varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b)$.

A mapping satisfying (a) and (b) is called a *ring homomorphism*.

We usually suppress the $'$ and write $\varphi : R \rightarrow R'$, is a ring homomorphism if

$$(a) \quad \varphi(a + b) = \varphi(a) + \varphi(b),$$

$$(b) \quad \varphi(ab) = \varphi(a)\varphi(b).$$

The first result for homomorphisms is :

Theorem 1.3.2. If $\varphi : R \rightarrow R'$ is a homomorphism, then

$$\text{Ker } \varphi := \{r \in R : \varphi(r) = 0\} \quad \text{is an ideal of } R$$

and

$$\text{Im } \varphi := \{\varphi(r) | r \in R\} \quad \text{is a subring of } R'.$$

Proof. We first show that $K = \text{Ker } \varphi$ is an ideal of R . Suppose $k, k' \in K$. Then

$$\begin{aligned} \varphi(k \pm k') &= \varphi(k) \pm \varphi(k') \\ &= 0 + 0 = 0 \end{aligned}$$

since φ is a homomorphism. Therefore, $k \pm k' \in K$. Next, suppose $k \in K$ and $r \in R$, then

$$\varphi(kr) = \varphi(k)\varphi(r) = 0\varphi(r) = 0,$$

since φ is a homomorphism. Hence, $kr \in K$. Similarly, $rk \in K$. Therefore, K is an ideal of R .

Next, we show that $T := \text{Im } \varphi$ is a subring of R' . Let $a, b \in T$. Then $a = \varphi(r), b = \varphi(r')$ for some $r, r' \in R$. Therefore, since φ is a homomorphism,

$$a \pm b = \varphi(r) \pm \varphi(r') = \varphi(r \pm r').$$

This shows that $a \pm b \in T$. Next,

$$ab = \varphi(r)\varphi(r') = \varphi(rr'),$$

since φ is a homomorphism. Hence, this implies that $ab \in T$. Therefore, T is a subring of φ .

Example 1.3.10. Let d be any positive integer and let $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_d$ be defined as $\varphi(a) = [a]$, for any $a \in \mathbb{Z}$. One verifies easily that φ is a homomorphism, with $\text{Ker } \varphi = d\mathbb{Z}$, (the set of multiples of d) and $\text{Im } \varphi = \mathbb{Z}_d$.

Example 1.3.11. Let

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

Define $\varphi : R \rightarrow \mathbb{R}$ by

$$\varphi \left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \right) = a.$$

This can be shown to be a homomorphism. What is the kernel and image of φ ?

Definitions. A homomorphism $\varphi : R \rightarrow R'$ is said to be *injective* if $\text{Ker } \varphi = \{0\}$. It is said to be *surjective* if $\text{Im } \varphi = R'$. A homomorphism that is both injective and surjective is called an *isomorphism*.

Note that if φ is injective then φ is one to one. For if $r, r' \in R$ is such that $\varphi(r) = \varphi(r')$. Then $\varphi(r) - \varphi(r') = 0$ implies that $\varphi(r - r') = 0$. But since $\text{Ker } \varphi = \{0\}$, this implies that $r - r' = 0$ and so, $r = r'$.

Examples 1.3.10 and 1.3.11 are not isomorphisms. They are both surjective homomorphisms but not injective.

Example 1.3.12. The map $\varphi : \mathbb{C} \rightarrow \mathbb{C}$ given by $\varphi(a + ib) = a - ib$ is an isomorphism. This is called the complex conjugation of a complex number.

Example 1.3.13. Let

$$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

The map $\varphi : R \rightarrow \mathbb{C}$ given by

$$\varphi \left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + ib,$$

is an isomorphism.

Note that isomorphism identifies rings which appear to be different but have essentially the same structure (see Example 1.3.13).

Cosets, Ideals and Quotient Rings

Let I be an ideal of R . We shall construct a ring, called the quotient ring of R by I .

Let

$$r + I := \{r + a \mid a \in I\}.$$

The set $r + I$ is called the coset of I in R . Note that the representative r in the coset $r + I$ is not unique. In fact, if $s \in r + I$, $r + I = s + I$. ($s \in r + I$, implies that $s = r + i$, for some $i \in I$. Therefore, $s + I \subset r + i + I = r + I$. Next, $r = s - i \in s + I$, implying that $r + I \subset s - i + I = s + I$. Hence, $s + I = r + I$.)

Next, set

$$Q := \{r + I \mid r \in R\},$$

that is, Q contains all the cosets of I in R . Given Q , we wish to define two binary operations on Q so that $(Q, +_Q, \cdot_Q)$ is a ring. Define, for $r + I, r' + I \in Q$,

$$(r + I) +_Q (r' + I) = (r + r') + I,$$

and

$$(r + I) \cdot_Q (r' + I) = rr' + I.$$

We must check that these operations are well-defined. That is to say, if we choose $s \neq r$ such that $s + I = r + I$ and $s' \neq r'$ such that $s' + I = r' + I$, is

$$(s + I) +_Q (s' + I) = (r + r') + I?$$

Is

$$(s + I) \cdot_Q (s' + I) = rr' + I?$$

The checking that $(Q, +_Q, \cdot_Q)$ is then routine.

We are now ready to establish some of the main Theorems associated with Homomorphisms. The most important result is perhaps the following result, which is sometimes known as the *First Isomorphism Theorem*.

Theorem 1.3.3. Let the mapping $\varphi : R \rightarrow R'$ be a homomorphism with kernel K .

Recall from Lecture 6 that we have constructed using an ideal I of a ring R , the quotient ring Q , denoted by R/I . This is a ring with the set of cosets of I , with operations $+_Q$ and \cdot_Q defined by

$$(r + I) +_Q (s + I) = (r + s) + I,$$

and

$$(r + I) \cdot_Q (s + I) = rs + I.$$

1.3. SUBRINGS, IDEALS, HOMOMORPHISMS AND QUOTIENT RINGS 17

We will now suppress the subscripts and write $+$, \cdot for the operation of the quotient ring instead of $+_{\mathcal{Q}}$, $\cdot_{\mathcal{Q}}$.

We are now ready to prove one of the most important results in this course.

Theorem 1.3.3. (First Isomorphism Theorem for rings)

Let $\varphi : R \rightarrow R'$ be a ring homomorphism. Then

$$R/\text{Ker } \varphi \simeq \text{Im } \varphi.$$

Proof. To prove this result, it suffices to construct an isomorphism Ψ from $R/\text{Ker } \varphi$ to $\text{Im } \varphi$. We let

$$\Psi(r + K) = \varphi(r),$$

where $K = \text{Ker } \varphi$. We will then verify :

Step 1. Ψ is well defined,

Suppose $s \in r + K$, or $s + K = r + K$, that is, we have chosen a different coset representative for $r + K$. Then $s = r + k$ for some $k \in K$. Therefore,

$$\Psi(s + K) = \varphi(s) = \varphi(r + k) = \varphi(r) + \varphi(k) = \varphi(r).$$

Hence $\Psi(s + K) = \Psi(r + K)$ and so, Ψ is well defined.

Step 2. Ψ is a ring homomorphism,

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

Similarly,

$$\Psi((r + K) \cdot (s + K)) = \Psi(r + K)\Psi(s + K).$$

Step 3. Ψ is an injection,

It suffices to show that $\text{Ker } \Psi$ is the zero element of R/K , which is $0 + K = K$. Let $\Psi(r + K) = 0$. Then this implies that $\varphi(r) = 0$. Hence, $r \in K$ and $r + K = K$.

Step 4. Ψ is a surjection.

Let $b \in \text{Im } \varphi$. Then $b = \varphi(r)$ for some $r \in R$. Therefore $\Psi(r + K) = \varphi(r) = b$, and hence Ψ is surjective.

Example 1.3.14. Consider the homomorphism $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$. Applying Theorem 1.3.3 yields

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$$

Example 1.3.15. Let R be the ring of real-valued continuous function on $[-1, 1]$. Let $\varphi : R \rightarrow \mathbb{R}$, be defined by $\varphi(f) = f(0)$. Note that φ is a surjective homomorphism with Kernel $I = \{f \in R \mid f(0) = 0\}$. By Theorem 1.3.3, $R/I \simeq \mathbb{R}$.

Example 1.3.16. Let

$$\mathcal{H}(\mathbb{Z}) = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{Z}\}.$$

Here \mathbf{i} , \mathbf{j} and \mathbf{k} satisfies the usual multiplication rules of the quaternions. Suppose

$$I_p := \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in p\mathbb{Z}\}.$$

Then

$$\mathcal{H}(\mathbb{Z})/I_p \simeq \mathcal{H}(\mathbb{Z}_p),$$

where

$$\mathcal{H}(\mathbb{Z}_p) = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{Z}_p\}.$$

We have seen that if I is an ideal of a ring R then R/I is a ring. Our next result shows that there is a one to one correspondence between ideals in R/I and ideals in R which contains I .

Theorem 1.3.4. (Correspondence Theorem) Let I be an ideal of R . $\varphi : R \rightarrow R/I$ be the homomorphism $\varphi(r) = r + I$. If J is an ideal of R

containing I , then J/I is an ideal of R/I . Conversely, if J' is an ideal of R/I , then there is an ideal J in R containing I such that $J' \simeq J/I$.

Proof. One direction is clear. If J is an ideal of R containing I , I is an ideal of J and we could form the ring J/I , which is a subring of R/I . Take $j + I \in J/I$ and $r + I \in R/I$, then $(r + I)(j + I) = rj + I \in J/I$, since J is an ideal of R which implies that $rj \in J$. Similarly $jr + I \in J/I$. Therefore J/I is an ideal of R/I .

Conversely, suppose J' is an ideal of R/I . Let

$$J := \{r \in R \mid \varphi(r) \in J'\}.$$

Note that J is an ideal of R . Furthermore, J contains I . Consider the map $\psi : J \rightarrow J'$, with $\psi(j) = \varphi(j)$. If $\varphi(j) = j + I = I$ then $j \in I$. Hence, $\text{Ker } \varphi = I$. Now the homomorphism is surjective (take $j + I \in J'$, then $\varphi(j) = j + I \in J'$ implies that $j \in J$, or $\psi(j) = j + I$) hence $J/I \simeq J'$.

We will give an application of Theorem 1.3.4. in our Section 4.

We conclude our Section with two more results, known as the Second and Third Isomorphism Theorems. As we will see, they are consequences of the First Isomorphism Theorem.

Theorem 1.3.5. (Second Isomorphism Theorem) Let A be a subring of R and I be an ideal of R . Then $A + I = \{a + i \mid a \in A, i \in I\}$ is a subring of R , I is an ideal of $A + I$, and

$$(A + I)/I \simeq A/(A \cap I).$$

Proof.

Step 1. $A + I$ is a ring. It suffices to check that $(a + i) \pm (a' + i') \in A + I$ and $(a + i)(a' + i') \in A + I$ for $a, a' \in A, i, i' \in I$.

Step 2. I is an ideal of $A + I$. Take $i \in I, a + i' \in A + I$, clearly, $i(a + i') = ia + ii' \in I$.

Step 3. To establish the isomorphism, define

$$\Psi : A \rightarrow (A + I)/I,$$

by

$$\Psi(a) = a + I.$$

Verify that Ψ is a homomorphism. Note that $\Psi(a) = 0$ if and only if $a + I = I$, or $a \in I$. Therefore, $\text{Ker } \Psi = A \cap I$. Clearly, Ψ is surjective. Hence by the First Isomorphism Theorem we conclude the result.

Theorem 1.3.6. (Third Isomorphism Theorem) Let I be an ideal of R and let K be any ideal contained in I . Then

$$R/K \Big/ I/K \simeq R/I.$$

Proof. We have seen from the Correspondence Theorem that if I is an ideal of R containing K , then I/K is an ideal of R/K and so, the left hand side makes sense. Define $\Psi : R/K \rightarrow R/I$ by

$$\Psi(r + K) = r + I.$$

First, we check that Ψ is well defined. Suppose $s \in r + K$, i.e., $s = r + k$ for some $k \in K$. Then

$$\Psi(s + K) = s + I = r + k + I = r + I,$$

since $k \in K \subset I$. It is clear that Ψ is a surjective homomorphism with Kernel I/K . Hence the result by the First Isomorphism Theorem.

1.4 Maximal Ideals

Definition A *maximal ideal* M of R is a proper ideal of R such that the only ideals containing M are M itself and R .

It is not difficult to show that for each prime p , $p\mathbb{Z}$ is a maximal ideal of \mathbb{Z} . (See Example 1.4.1.)

In Example 1.3.6, we have seen that every field has exactly two ideals, (0) and R . We now show that

Lemma 1.4.1. If R is a commutative ring with unit and such that (0) and R are its only ideals, then R is a field.

Proof. Let $a \neq 0 \in R$. Then we have seen that Ra is an ideal. Since $1 \cdot a \in Ra$, $Ra \neq (0)$. Therefore, $Ra = R$. This implies that $1 = ba = ab$ for some $b \in R$ and so, R is a field.

Theorem 1.4.2. Let R be a ring. Then R/M is a field if and only if M is a maximal ideal of R .

Proof. R/M is a field if and only if the zero ideal of R/M and R/M are the only two ideals of R/M , by Lemma 1.4.1 and Example 1.3.6. But by Theorem 1.3.4, the last statement is equivalent to saying that there are exactly two ideals in R that contains M , or that the only ideals containing M is M and R and this simply implies that M is maximal.

Example 1.4.1. Let $R = \mathbb{Z}$. The field $\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$. Hence, $p\mathbb{Z}$ is a maximal ideal of \mathbb{Z} .

Example 1.4.2. Let $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Let $M = 3\mathbb{Z}[i]$. Then M is a maximal ideal.

Solution. Suppose N is an ideal of R that contains M and $N \neq M$. Then there exist an element $r + is \in N$ such that $3 \nmid r$ or $3 \nmid s$. Now, $(r + is)(r - is) = r^2 + s^2 \in N$ since N is an ideal. Furthermore, $3 \nmid r^2 + s^2$ (look at all the possibilities for $r^2 + s^2$ modulo 3 subject to the condition that $3 \nmid r$ or $3 \nmid s$). Therefore $t := r^2 + s^2$ is coprime to 3 and so there exist integers u , and v such that $ut + 3v = 1$. Since $t, 3 \in N$, this implies that $1 \in N$. Hence, $N = R$. Therefore, M is maximal.

Is $5\mathbb{Z}[i]$ maximal?

Example 1.4.3. Let R be the ring of all real valued continuous functions on the interval $[-1, 1]$. We have shown that if $M = \{f \in R \mid f(0) = 0\}$ then R/M is a field isomorphic to \mathbb{R} . This shows that M is a maximal ideal.

1.5 Prime ideals

Definition. An ideal P is said to be a prime ideal if it satisfies the condition that for any nonzero elements $a, b \in R$, $ab \in P$ implies that either $a \in P$ or $b \in P$.

The above definition is motivated by Euclid's Lemma, which states that if a prime number $p|ab$ then $p|a$ or $p|b$. Note that we have proved this Lemma when we show that \mathbb{Z}_p is an integral domain. Now, if we translate the condition $p|a$ to the statement the ideal $p\mathbb{Z}$ contains a . Then Euclid's Lemma becomes $ab \in p\mathbb{Z}$ implies either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. Replacing $p\mathbb{Z}$ by P we see that this is precisely the definition of prime ideals.

Theorem 1.5.1. Let R be a commutative ring with unit. Then R/P is an integral domain if and only if P is a prime ideal.

Proof. Suppose P is a prime ideal. Let

$$(a + P)(b + P) = 0 + P.$$

This implies that $ab \in P$. But P is a prime ideal and so either $a \in P$ or $b \in P$. This translates to either $a + P = P$ or $b + P = P$ and this implies that R/P is an integral domain. Conversely, if R/P is an integral domain, then $ab \in P$ implies $(a + P)(b + P) = 0 + P$. Since R/P is an integral domain, either $a + P = P$ or $b + P = P$. In other words, either $a \in P$ or $b \in P$. Hence, P is a prime ideal.

Example 1.5.1. Note that it follows from Theorem 1.4.1 that M is maximal implies that R/M is a field, this implies that R/M is an integral domain, and therefore M is a prime ideal. Hence, every maximal ideal is a prime ideal.

A prime number is defined as a number divisible by 1 and itself. With this definition, prime number should actually be called "maximal" number!

Chapter 2

Polynomial Rings

2.1 Polynomial Rings over a field

Let F be a field. By the ring of polynomials in x over F , we mean the set of all formal expressions

$$p(x) = a_0 + a_1x + \cdots + a_nx^n, n \geq 0, a_i \in F.$$

This set is denoted by $F[x]$. One can make this set into a ring by defining addition and multiplication on $F[x]$. Let

$$p(x) = a_0 + a_1x + \cdots + a_nx^n, a_n \neq 0$$

and

$$q(x) = b_0 + b_1x + \cdots + b_mx^m, b_m \neq 0.$$

Without loss of generality, suppose $n \geq m$. Write

$$p(x) + q(x) = \sum_{k=0}^n (a_k + b_k)x^k.$$

Define

$$p(x) \cdot q(x) = \sum_{k=0}^{m+n} c_k x^k,$$

where

$$c_k = \sum_{j=0}^k a_j b_{k-j}.$$

Here, $a_s = 0$ if $s > n$ and $b_s = 0$ if $s > m$. With this two operations, $F[x]$ is commutative ring with unit. We will show that this ring behaves very much the same as that of the integers \mathbb{Z} . In particular, gcd of two polynomials exist and can be found by analogue of the Euclidean Algorithm as in the case of integers. We will also show that $F[x]$ is a Principal Ideal Domain, namely, that each ideal in $F[x]$ is generated by one polynomial, i.e., if I is an ideal then $I = p(x)F[x]$ for some polynomial $p(x)$. We will then show that every element in $F[x]$ can be expressed uniquely in terms of irreducible polynomials, unique up to a constant in F . As we study the ring $F[x]$, we will prove more general results. We are aiming to show “Every Euclidean Domain is a Principal Ideal Domain. Every Principal Ideal Domain is a Unique Factorization Domain.”

Definition. If $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $n \geq 0$, $a_n \neq 0$, we define $\deg p(x)$ equals to n . We will adopt the convention that $\deg c = 0$ if $c \neq 0 \in F$. If $c = 0$, we set $\deg 0 = -\infty$.

Lemma 2.1.1. If $p(x)$ and $q(x)$ are non-zero elements of $F[x]$, then $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$.

Lemma 2.1.2. If $p(x)$ and $q(x)$ are non-zero elements of $F[x]$, then $\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x))$.

Theorem 2.1.3. $F[x]$ is an integral domain.

Proof. Suppose $p(x)q(x) = 0$ and $p(x) \neq 0$ and $q(x) \neq 0$. Then By Lemma 2.1.1, $\deg p(x)q(x)$ is a finite number. But $\deg 0$ is $-\infty$, contradicting to the assumption that $p(x)q(x) = 0$.

Theorem 2.1.4. Given the polynomials $f(x), g(x) \in F[x]$, where $g(x) \neq 0$, there exist polynomials $q(x), r(x) \in F[x]$ such that

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

with either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof. We proceed by Induction on $\deg f(x)$. First fix the polynomial $g(x)$. Suppose $f(x) = 0$ or $\deg f(x) < \deg g(x)$, then $f(x) = 0g(x) + f(x)$. So we may assume that $\deg f(x) \geq \deg g(x)$.

Suppose the statement is true for any polynomials with degrees less than or equal to $n - 1$. Let $f(x)$ be a polynomial of degree n . Write

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

and

$$g(x) = b_0 + b_1x + \cdots + b_mx^m,$$

with $a_n \neq 0$ and $b_m \neq 0$ and $n \geq m$. Since F is a field b_m^{-1} exists and the polynomial

$$F(x) := f(x) - b_m^{-1}a_nx^{n-m}g(x) \quad (*)$$

has degree $n - 1$. Hence, there exist $q(x)$ and $r(x)$ such that

$$F(x) = q(x)g(x) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg g(x)$. But by (*),

$$f(x) = (q(x) + b_m^{-1}a_nx^{n-m})g(x) + r(x),$$

hence the result.

We now have two rings, \mathbb{Z} and $F[x]$ satisfying similar property, namely, “*Division Algorithm*” holds. We are therefore led to the next special collection of rings.

Definition. An integral domain R with identity is called an *Euclidean domain* (ED) if for every $a \neq 0 \in R$, there is a nonnegative integer $d(a)$ such that

1. For all $a, b \in R$ both nonzero, $d(a) \leq d(ab)$.
2. For any $a, b \in R$, both nonzero, there exist $t, r \in R$, such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

Note that in \mathbb{Z} our function $d(r) := |r|$. In $F[x]$, $d(f(x)) = \deg f(x)$.

In \mathbb{Z} we have seen that every ideal of \mathbb{Z} is generated by one element, i.e., if I is an ideal of \mathbb{Z} then $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. This follows from the fact that \mathbb{Z} is a cyclic group. We will next show that if I is an ideal of $F[x]$, then $I = f(x)F[x] := \{f(x)g(x) | g(x) \in F[x]\}$. In other words, every ideal in $F[x]$ is also generated by one element. Since once again this is a property of both $F[x]$ and \mathbb{Z} , we give the following definition of a new collection of rings.

Definition. An integral domain R with identity is a *Principal Ideal Domain* (PID) if every ideal I in R is generated by one element, namely, $I = aR$ for some $a \in R$. An ideal generated by one element is called a principal ideal.

Note that we have already seen that \mathbb{Z} is a Principal Ideal Domain. We next show the more general statement that every Euclidean Domain is a Principal Ideal Domain and deduce that $F[x]$ is a Principal Ideal Domain as a Corollary.

Theorem 2.1.5. Every Euclidean Domain is a Principal Ideal Domain.

Proof. Let I be an ideal of an Euclidean Domain R . If $I = (0)$ then choose the generator to be 0. Suppose I is a nonzero ideal. Then since $d(\cdot)$ (in the case of $F[x]$, this is the degree of $f(x) \in F[x]$) is nonnegative, there is an element $r \in I$ for which $d(r)$ is minimal. Pick any element $a \in I$. Then by the Division Algorithm, $a = qr + r'$, with either $r' = 0$ or $d(r') < d(r)$. Note that since I is an ideal, $r \in I$, implies that $qr \in I$. Therefore, $r' = a - qr \in I$. This says that $d(r') \geq d(r)$, by the minimality of $d(r)$. Hence, $a = qr + r'$ can only be satisfied if $r' = 0$. Hence $a = qr$. Therefore, $I \subset rR \subset I$. Hence, $I = rR$ and so, it is a principal ideal.

Corollary 2.1.6. The ring $F[x]$ is a Principal Ideal Domain.

In general a Principal Ideal Domain may not be a Euclidean Domain. For example the ring $\mathbb{Z} \left[\frac{\sqrt{-19}+1}{2} \right]$ is a Principal Ideal Domain but not an ED.

Example 2.1.1. The ring $\mathbb{Z}[i]$ is an Euclidean Domain, and hence a Principal Ideal Domain.

We now summarize what we know about $F[x]$. We know that

1. $F[x]$ is a commutative ring with identity,
2. $F[x]$ is an integral domain,
3. $F[x]$ is an Euclidean Domain,
4. $F[x]$ is a Principal Ideal Domain.

Our next aim is to show that for every $f(x) \in F[x]$, $f(x)$ can be expressed uniquely (up to product of elements in F) in terms of a special collection of polynomials known as “irreducible polynomials”. This result should be

viewed as an analogue of the Fundamental Theorem of Arithmetic, which states that every integer is expressible uniquely (up to ± 1) as a product of primes. Note that irreducible polynomials will play the role of primes in $F[x]$. Before we define Irreducible polynomials, we need the notion of Divisibility.

Definition. Let $f(x), g(x) \in F[x]$. We say that $g(x)$ divides $f(x)$ if $f(x) = g(x)q(x) + r(x)$ implies that $r(x) = 0$. In other words, $g(x)$ divides $f(x)$ if $f(x) = g(x)q(x)$ for some $q(x) \in F[x]$. The notation for this is $g(x)|f(x)$.

Remarks.

1. Note that the notion of divisibility exists for all Euclidean domain.
2. We observe that if $g(x)|f(x)$, then the ideal $(g(x))$ contains $(f(x))$. Hence, we may also define divisibility for Principal Ideal Domain. Namely, we say that $g(x)|f(x)$ if $(g(x))$ contains $(f(x))$.

With the notion of Divisibility, we can now give the definition of a Greatest Common Divisor.

Definition. We say that a polynomial is *monic* if the leading coefficient is 1, i.e., $f(x)$ is monic if $f(x) = a_0 + a_1x + \cdots + x^n$. The *Greatest Common Divisor* of two nonzero polynomial is the monic polynomial $d(x)$, (denoted by $\gcd(f(x), g(x)) = d(x)$), such that

- (a) $d(x)|f(x)$ and $d(x)|g(x)$,
- (b) If $h(x)|f(x)$ and $h(x)|g(x)$ then $h(x)|d(x)$.

The condition for $d(x)$ to be monic is required for otherwise, \gcd may not be unique.

Theorem 2.1.7. Suppose $f(x)$ and $g(x)$ are two nonzero polynomials in $F[x]$, then $\gcd(f(x), g(x))$ exists. Furthermore, there exist $s(x)$ and $t(x)$ such that

$$\gcd(f(x), g(x)) = f(x)s(x) + g(x)t(x).$$

Proof. Consider the set

$$J := (f(x)) + (g(x)) := \{f(x)u(x) + g(x)v(x) | u(x), v(x) \in F[x]\}.$$

Since $(f(x))$ and $(g(x))$ are ideals, we know that J is an ideal. From Corollary 2.1.6, we know that $F[x]$ is a Principal Ideal Domain, hence, $J = (d_1(x))$ for some $d_1(x) \in F[x]$. $d_1(x)$ may not be monic. Suppose $d_1(x) = a_0 + a_1x + \cdots + a_nx^n$. Let $d(x) = a_n^{-1}d_1(x)$, so that $d(x)$ is monic. Note that $(d(x)) = (d_1(x))$. Since $J = (d(x))$ there exist $s(x)$ and $t(x)$ such that

$$\gcd(f(x), g(x)) = f(x)s(x) + g(x)t(x),$$

proving the second statement. To prove the first statement, i.e., that $d(x)$ is the $\gcd(f(x), g(x))$, we note that $f(x) \in J = (d(x))$. Hence, $d(x)|f(x)$. Similarly, $d(x)|g(x)$. Next, suppose $h(x)|f(x)$ and $h(x)|g(x)$ then $h(x)|(f(x)s(x) + g(x)t(x))$ implies that $h(x)|d(x)$. Hence $d(x)$ is indeed the greatest common divisor of $f(x)$ and $g(x)$.

The above Theorem does not tell us how to find $d(x) = \gcd(f(x), g(x))$. Our next task is to determine $d(x)$.

We first note that if $f(x) = g(x)q(x) + r(x)$ (this is guaranteed by Theorem 2.1.4) then $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$. Let $d(x) = \gcd(f(x), g(x))$ and $d_1(x) = \gcd(g(x), r(x))$.

Now, $d(x)|f(x)$ and $d(x)|g(x)$ implies that $d(x)|(f(x)-g(x)q(x))$ or $d(x)|r(x)$. Hence, $d(x)|d_1(x)$ by the definition of $d_1(x)$. On the other hand, $d_1(x)|g(x)$ and $d_1(x)|r(x)$ implies that $d_1(x)|f(x)$, and hence $d_1(x)|d(x)$. Therefore, $d_1(x) = u(x)d(x)$ and $d(x) = v(x)d_1(x)$. This implies that $u(x)v(x) = 1$. Since $\deg v(x)u(x) = \deg v(x) + \deg u(x) = 0$, we conclude that $v(x)$ and $u(x)$ are both constants in F . But now $d_1(x)$ and $d(x)$ are both monic implies that $u(x) = v(x) = 1$. Now, the important thing to note is that $\deg r(x)$ is smaller than that of $g(x)$. Hence, by repeating the above procedure, we may write

$$\begin{aligned} f(x) &= g(x)q(x) + r(x), r(x) = 0 \quad \text{or} \quad \deg r(x) < \deg g(x), \\ g(x) &= r(x)q_1(x) + r_1(x), r_1(x) = 0 \quad \text{or} \quad \deg r_1(x) < \deg r(x), \\ &\vdots \\ r_{n-1}(x) &= r_n(x)q_{n+1}(x) + r_{n+1}(x), r_{n+1}(x) = 0 \quad \text{or} \quad \deg r_{n+1}(x) < \deg r_n(x). \end{aligned}$$

Note that since $\deg r_k(x)$ is decreasing, we will eventually arrive at a stage where $r_k(x) = 0$ for some k . Then $\gcd(f(x), g(x)) = \gcd(g(x), r(x)) = \gcd(r(x), r_1(x)) = \cdots = \gcd(r_{k-1}(x), 0) = r_{k-1}(x)$. An example will clarify the above algorithm (known as the Euclidean Algorithm).

Example 2.1.2. Find the $\gcd(x^2 - 1, 2x^7 - 4x^5 + 2)$.

We say that two polynomials $f(x)$ and $g(x)$ are *relatively prime* if $\gcd(f(x), g(x)) = 1$.

Theorem 2.1.8. Two polynomials $f(x)$ and $g(x)$ are relatively prime if and only if there exist $a(x), b(x) \in F[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1.$$

Proof. If $f(x)$ and $g(x)$ are relatively prime, then $\gcd(f(x), g(x)) = 1$ and this implies that there exist $a(x), b(x) \in F[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1,$$

by Theorem 2.1.7. Conversely, if

$$a(x)f(x) + b(x)g(x) = 1,$$

then since $\gcd(f(x), g(x))$ divides $f(x)$ and $g(x)$, it divides 1. Hence the $\gcd(f(x), g(x))$ has degree 0 and therefore must be in F . Since gcd is monic, the result follows.

Note that Theorem 2.1.8 is just an analogue of the statement that “For any two nonzero integers a, b , $\gcd(a, b) = 1$ if and only if $1 = ax + by$ for some $x, y \in \mathbb{Z}$.”

Corollary 2.1.9. If $q(x)$ and $f(x)$ are relatively prime, and if $q(x)|f(x)g(x)$ then $q(x)|g(x)$.

Proof. There exist $a(x), b(x)$ such that

$$a(x)q(x) + f(x)b(x) = 1.$$

Multiplying both sides by $g(x)$ yields the result.

We are now ready to define the analogue of prime numbers in $F[x]$.

Definition. A polynomial $p(x)$ of positive degree is *irreducible* if it cannot be written as a product of two polynomials of positive degree.

Note that this is the same as saying that the monic polynomials dividing $p(x)$ is 1 and $p(x)$. This certainly reminds us of the definition of prime numbers in \mathbb{Z} .

Now, since $F[x]$ is a Principal Ideal Domain, the above definition of $p(x)$ implies that the ideal $(p(x))$ is a maximal ideal of $F[x]$, since there are precisely two ideals containing $(p(x))$, i.e., $(p(x))$ and $F[x]$. Hence $(p(x))$ is a prime ideal. (Every maximal ideal is a prime ideal.) Thus if $a(x)b(x) \in (p(x))$ then either $a(x) \in (p(x))$ or $b(x) \in (p(x))$, and we have

Theorem 2.1.10. (Analogue of Euclid’s Lemma). Suppose $p(x)$ is an irreducible polynomial. Then $p(x)|a(x)b(x)$ implies that $p(x)|a(x)$ or $p(x)|b(x)$.

A generalization of this theorem can be proved by Induction, i.e.,

Theorem 2.1.11. Suppose $p(x)$ is an irreducible polynomial. Then $p(x)|a_1(x)a_2(x) \cdots a_k(x)$ then $p(x)|a_j(x)$ for some j .

We are now ready to establish the fact that every element in $F[x]$ can be factorized into irreducible polynomials unique up to rearrangement of terms.

Theorem 2.1.12. Let $f(x) \in F[x]$ be of positive degree. Then $f(x)$ is irreducible in $F[x]$ or $f(x)$ is the product of irreducible polynomials in $F[x]$. In fact,

$$f(x) = ap_1^{\alpha_1}(x) \cdots p_k^{\alpha_k}(x),$$

where a is the leading coefficient of $f(x)$, $p_1(x), \dots, p_k(x)$ are irreducible polynomials in $F[x]$, $\alpha_j > 0$ for all $1 \leq j \leq k$, and this factorization in this form is unique up to the order of the $p_i(x)$.

Proof. The existence of the representation is proved by Induction on the degree of $f(x)$. As for the uniqueness, suppose the uniqueness for the product of polynomials holds for those with degree less than degree of $f(x)$ (note that the uniqueness for degree 1 polynomials is clear) . Suppose

$$f(x) = ap_1^{\alpha_1}(x) \cdots p_k^{\alpha_k}(x) = aq_1^{\beta_1}(x) \cdots q_s^{\beta_s}(x),$$

where a is the leading coefficient of $f(x)$, where $p_i(x)$ and $q_j(x)$ are monic irreducibles. Now, since $p_1(x)$ divides the right hand side, $p_1(x)$ divides some $q_j(x)$. Without loss of generality we suppose $p_1(x)|q_1(x)$. Since $q_1(x)$ is irreducible, $p_1(x) = q_1(x)$. By Induction, we have a unique factorization for $f(x)/p_1(x)$, and hence, our factorization for $f(x)$ is also unique.

We have seen that both \mathbb{Z} and $F[x]$ satisfy the “*Unique factorization property*”. We will study this Unique factorization property in more details in Chapter 3.

We have seen from the definition of irreducible $p(x)$ that $(p(x))$ is a maximal ideal. If on the other hand, M is a maximal ideal, $M = (q(x))$ for some $q(x) \in F[x]$ since $F[x]$ is a Principal Ideal Domain. If $q(x)$ is not irreducible, $q(x) = a(x)b(x)$, and hence $M = (q(x)) \subset (a(x))$, $a(x)$ being polynomial of positive degree. This implies that M is not maximal. The contradiction implies that $q(x)$ is irreducible. Hence, all maximal ideals are generated by irreducible polynomials. From Theorem 1.3.5, we have seen that if M is a maximal ideal of a commutative ring R with identity, then R/M is a field. What is the field $F[x]/(p(x))$ if $p(x)$ is irreducible?

So far, we have defined polynomial rings $F[x]$ over a field F . In general, we may define polynomial rings $R[x]$ over a commutative ring R which is not necessarily a field. When R is not a field, many results which are true for $F[x]$ may not be true for $R[x]$. For example if the ring $R = \mathbb{Z}$, then $R' = \mathbb{Z}[x]$ is not even a Principal Ideal Domain since the ideal $2R' + xR'$ is not Principal. Therefore, $\mathbb{Z}[x]$ is not Euclidean.

Proof of the fact that $2R' + xR'$ is not principal. Suppose the contrary. Then $2R' + xR' = uR'$ for some $u \in R'$. This implies that $2 = uf$, $f \in R'$. This implies that u is a constant. (It will be proved later that $\mathbb{Z}[x]$ is a Unique factorization domain). Since $\mathbb{Z}[x]$ is a unique factorization domain, $u = 1$ or 2 . But $u = 1$ implies that $2R' + xR' = R'$, a contradiction. Therefore $u = 2$. But if $u = 2$, x is clearly not in $2R'$. Hence, $2R' + xR'$ is not principal.

In this ring, $2\mathbb{Z}[x]$ is a prime ideal but not maximal since

$$2\mathbb{Z}[x] \subset 2\mathbb{Z}[x] + x\mathbb{Z}[x].$$

2.2 The Polynomial ring $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$

In the previous section, we have seen that the irreducible polynomials in $F[x]$ form the prime ideals of $F[x]$. However, given a polynomial $f(x)$ it is not at all clear whether it is irreducible or not. When $F = \mathbb{Q}$ we happen to have a good way to determine the irreducibility of certain polynomials. We will study this method, known as the Eisenstein Criterion, in this section.

Lemma 2.2.1. Let $f(x) \in \mathbb{Q}[x]$; then

$$f(x) = \frac{u}{m}(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0),$$

where u, m, a_0, \dots, a_n are integers such that

$$\gcd(u, m) = 1 \quad \text{and} \quad \gcd(a_1, \dots, a_n) = 1.$$

Proof. Let

$$f(x) = \frac{A_n}{B_n} x^n + \cdots + \frac{A_0}{B_0}, \quad A_i, B_i \in \mathbb{Z}.$$

Suppose

$$U = \gcd\left(A_1 \frac{B}{B_1}, A_2 \frac{B}{B_2}, \dots, A_i \frac{B}{B_i}, \dots, A_0 \frac{B}{B_0}\right),$$

where $B = B_0 \cdot B_1 \cdots B_n$, then

$$f(x) = \frac{U}{B}(a_n x^n + \cdots + a_0),$$

where $a_i \in \mathbb{Z}$. Clearing common factors in U and B yields the desired result.

The next result is yet another application of the First Isomorphism Theorem.

Lemma 2.2.2. If R is any ring and I is an ideal of R , then $I[x]$, the polynomial ring in x over I , is an ideal of $R[x]$. Furthermore,

$$R[x]/I[x] \simeq R/I[x],$$

where $R/I[x]$ is the polynomial ring over R/I .

Proof. It is clear that $I[x]$ is an ideal of $R[x]$. Define $\varphi : R[x] \rightarrow R/I[x]$ by

$$\varphi(f(x)) = \varphi(a_n x^n + \cdots + a_0) = (a_n + I)x^n + \cdots + (a_0 + I).$$

It can be checked that this is a surjective homomorphism of rings and clearly the $\text{Ker } \varphi = I[x]$. By the First Isomorphism Theorem, we conclude the result.

Corollary 2.2.3. $\mathbb{Z}[x]/p\mathbb{Z}[x] \simeq \mathbb{Z}/p\mathbb{Z}[x]$.

We are now ready to prove the two major results in this Section.

Theorem 2.2.4. (Gauss' Lemma) Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial and $f(x) = a(x)b(x)$, where $a(x)$ and $b(x)$ are in $\mathbb{Q}[x]$. Then $f(x) = a_1(x)b_1(x)$ are monic polynomials in $\mathbb{Z}[x]$ and $\deg a_1(x) = \deg a(x)$ and $\deg b_1(x) = \deg b(x)$.

This result tells us that to determine if the monic polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$, it suffices to determine if $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Suppose $f(x) = a(x)b(x)$ in $\mathbb{Q}[x]$. Then from Lemma 2.2.1, we may write

$$a(x) = \frac{u_1}{v_1}a_1(x) \quad \text{and} \quad b(x) = \frac{u_2}{v_2}b_1(x),$$

with $a_1(x), b_1(x) \in \mathbb{Z}[x]$ and $u_1, u_2, v_1, v_2 \in \mathbb{Z}$. We write

$$f(x) = \frac{u}{v}a_1(x)b_1(x),$$

where u/v is the product $u_1u_2/(v_1v_2)$ in its lowest term. Hence,

$$vf(x) = ua_1(x)b_1(x).$$

Suppose $v = 1$, then since $f(x)$ is monic, then $1 = ua'_nb'_m$, where a'_n and b'_m are the coefficients of $a_1(x)$ and $b_1(x)$ respectively. Therefore, $u = 1, a'_n = b'_m = 1$ (We may choose the coefficient to be positive integers). Therefore, $f(x)$ is a product of monic polynomials in $\mathbb{Z}[x]$.

Suppose $v \neq 1$. Then since v and u are relatively prime integers, there exist a prime p which divides v but not u . If

$$a_1(x) = a'_nx^n + a'_{n-1}x^{n-1} + \cdots + a'_0,$$

then by our construction, we have $\gcd(a'_0, \dots, a'_n) = 1$ and hence there exist an i such that $p \nmid a'_i$. Similarly there exist a j such that $p \nmid b'_j$, where

$$b_1(x) = b'_nx^n + b'_{n-1}x^{n-1} + \cdots + b'_0.$$

Now, since $p|v$, $vf(x)$ is the zero polynomial in $(\mathbb{Z}/p\mathbb{Z})[x]$. However, since $p \nmid a'_i$ and $p \nmid b'_j$, the polynomial $a_1[x]$ and $b_1[x]$ are both nonzero polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$. Since $(\mathbb{Z}/p\mathbb{Z})[x]$ is an integral domain, this is impossible. Hence $v = 1$.

In general it is hard to determine if a polynomial is irreducible, even over \mathbb{Z} . In the next Theorem, we prove a Criterion which enables us to deduce the irreducibility of certain polynomials.

Theorem 2.2.5. (Eisenstein Criterion) Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a non-constant polynomial with integer coefficients. Suppose that there is some prime p such that $p|a_0, \dots, p|a_{n-1}$, but $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. By Gauss' Lemma, it suffices to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$. Suppose $f(x) = a(x)b(x)$, with $a(x)$ and $b(x)$ monic. By the map φ given in the proof of Lemma 2.2.2, the polynomial $f(x)$ is mapped to the polynomial x^n in $(\mathbb{Z}/p\mathbb{Z})[x]$. Since $a(x)b(x)$ is represented by x^n and x is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$, this shows that x^n is the unique factorization of the image of $a(x)$ and $b(x)$ under φ in $(\mathbb{Z}/p\mathbb{Z})[x]$. Therefore, $a(x) = x^{n-k} + pA(x)$ and $b(x) = x^k + pB(x)$, for some $A[x], B[x] \in \mathbb{Z}[x]$. But this implies that the constant term in $a(x)b(x)$ is divisible by p^2 , which is a contradiction.

Example 2.2.1. The polynomial $x^n - p$ for any p is irreducible in $\mathbb{Q}[x]$.

Example 2.2.2. The polynomial $x^{11} - 6x^4 + 12x^3 + 36x - 6$ is irreducible in $\mathbb{Q}[x]$.

Example 2.2.3. The polynomial $5x^4 - 7x + 7$ is irreducible in $\mathbb{Q}[x]$.

Example 2.2.4. The polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Chapter 3

Unique Factorization Domain

3.1 Principal Ideal Domain and Unique Factorization Domain

We have seen that both \mathbb{Z} and $F[x]$, where F is a field, satisfies certain “Unique Factorization Property”. In fact, if we follow closely the proof of Theorem 2.1.10, we could easily show that every Euclidean Domain has such a “Unique Factorization property”. In this Chapter, however, we will prove a much stronger result, namely that every Principal Ideal Domain has “Unique Factorization Property.” We will first make the following definitions.

Definition. Let R be an integral domain and $a, b \in R$ be two nonzero elements. We say that a divides b if $b = ac$ for some $c \in R$. The notation is $a|b$.

Definition. Let R be an integral domain with identity 1. An element $u \in R$ is called a *unit* of R if there exists an element $v \in R$ such that $uv = 1$, or in other words, u divides 1. Two elements $a, b \in R$ are called *associates* if $a = bu$ for some unit $u \in R$.

Example 3.1.1. The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. $i + 1$ is an associate of $i - 1$.

Example 3.1.2. The units in \mathbb{Z}_8 are 1, 3, 5, 7. 6 is an associate of 2.

Definition. A nonzero element $p \in R$ that is not a unit is called an irreducible of R if in any factorization $p = ab$, either a or b is a unit. In other words, if b divides p , b is an associate of p .

Example 3.1.3. The irreducibles in \mathbb{Z} are the primes $\pm 2, \pm 3, \pm 5 \cdots$ and the irreducibles in $F[x]$ are the irreducible polynomials. The irreducibles in \mathbb{Z}_8 are 2 and 6.

From the above example, we see that when $R = \mathbb{Z}$, we have 2 is associated with -2 , both of which are irreducibles. We now note that being associates is an equivalence relation. Therefore we may choose a representative from each equivalence class, forming a subset of the set of irreducibles. We call this subset *a complete set of irreducibles* or *a complete set of primes*.

Example 3.1.4. A complete set of irreducibles of \mathbb{Z} is $\{2, 3, 5, 7 \cdots\}$. A complete set of irreducibles of $F[x]$ are the set of monic irreducible polynomials. A complete set of irreducibles of \mathbb{Z}_8 is $\{2\}$.

We are now ready to state the definition of Unique Factorization Domain.

Definition. Let Π be a complete set of irreducibles. An integral domain R is a Unique Factorization Domain if every nonzero nonunit element $a \in R$ can be expressed uniquely as $a = up_1p_2 \cdots p_n$, with $p_i \in \Pi$ and u a unit of R .

We are now ready to establish the main result in this section. Recall that R is a Principal Ideal Domain if R is an integral domain such that every ideal of R is principal.

Theorem 3.1.1. Every Principal Ideal Domain is a Unique Factorization Domain.

As a Corollary, we have

Corollary 3.1.2. Every Euclidean Domain is a Unique Factorization Domain. In particular, \mathbb{Z} and $F[x]$ are Unique Factorization Domain if F is a field.

There are some difficulties which we need to overcome. First, we need to find the complete set of irreducibles for the Principal Ideal Domain R . Next

3.1. PRINCIPAL IDEAL DOMAIN AND UNIQUE FACTORIZATION DOMAIN 39

we need to show that every element in R can be written in terms of a finite product of the irreducibles. Finally, we show that the factorization is unique up to units.

Proof. Step 1. We first recall some set theoretic notation. Given $\{A_k | k \in K\}$, we denote $\cup_{k \in K} A_k$ to be the set of all x such that $x \in A_j$ for at least one $j \in K$.

We first show that if R is a Principal Ideal Domain, then R satisfies the Ascending Chain Condition (ACC), namely, if

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots, \quad (*)$$

is a chain of ideals, then the chain must “stabilize”, that is, there exist a k such that $I_j = I_k$ for all $j \geq k$. So, suppose $(*)$ is such a chain. Let $I = \cup_j I_j$. Since R is a Principal Ideal Domain, $I = Ra$ for some $a \in R$. But since $a \in I$, $a \in I_k$ for some k . Hence, I_j contains a for $j \geq k$ and $Ra \subset I_j \subset I = (a)$, giving $I_j = I_k$ for $j \geq k$.

Step 2. We next show that irreducibles exist in a Principal Ideal Domain. Suppose a is a nonunit and a is nonzero. If irreducibles do not exist, then $a = a_1 b_1$ and $Ra \subseteq Ra_1$. By assumption, a_1 is not an irreducible, and so, $a_1 = a_2 b_2$ and

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots$$

is an infinite chain of ideals. This is impossible by Step 1 and hence there must be some a_k that is irreducible. Hence irreducibles exist. Furthermore, the above argument shows that $a = a_k c$ where a_k is irreducible. By the repeating the above argument, we find that a is a finite product of irreducibles. Hence, $a = up_1 p_2 \cdots p_k$ for some unit u .

Step 3. Now the ideal generated by irreducibles must be maximal. For if $(p_1) \subset J$, then since R is a Principal Ideal Domain, $J = (u)$ for some $u \in R$. Hence, $p_1 = ur$, for some $r \in R$. But p_1 is irreducible and hence, $u = p_1$ or a unit. Therefore, (p_1) is a maximal ideal. Now, maximal ideals are prime ideals. Hence if $ab \in (p_1)$, either $a \in (p_1)$ or $b \in (p_1)$.

Step 4. We now prove uniqueness. Let Π be a complete set of irreducibles. Suppose

$$a = a = up_1 p_2 \cdots p_k = vq_1 q_2 \cdots q_l,$$

where $p_i, q_j \in \Pi$. Since $p_1 p_2 \cdots p_k \in (q_1)$, there exist a p_i , say p_1 such that $p_1 \in (q_1)$. So $p_1 = q_1 u$. But p_1 is irreducible and q_1 is nonunit, hence, u must be a unit and p_1 is an associate of q_1 . Since we have chosen our $p_i, q_j \in \Pi$, we conclude that $p_1 = q_1$. Therefore,

$$u p_2 \cdots p_k = v q_2 \cdots q_l.$$

Continuing the process, we arrive at

$$u^{-1} v q_{k+1} q_{k+2} \cdots q_l = 1,$$

assuming that $l > k$. Hence all the q_j are units for $j > k$. Therefore there are only k irreducibles on the right hand side. Since all the irreducibles are from the complete set of irreducibles, we conclude that $u^{-1} v = 1$ and so, the representation of a as irreducibles in Π is unique.

From Theorem 3.1.1, we now see that there are many rings which are Unique Factorization Domain. In particular, the ring $\mathbb{Z} \left[\frac{1+\sqrt{-19}}{2} \right]$ is a Unique Factorization Domain since it is a Principal Ideal Domain (which is not a Euclidean Domain). We will show in the next section that if we have a Unique Factorization Domain, we can create infinitely number of them.

3.2 Polynomial rings over a Unique Factorization Domain

Field of Quotients of an integral domain

We now discuss briefly how we construct a field out of an integral domain. Let R be an integral domain. Let $\mathcal{F} = \{(a, b) | a \in R, b \in R \setminus \{0\}\}$. Define an equivalence relation \sim on \mathcal{F} as follows : $(a, b) \sim (c, d)$ if and only if $ad = bc$.

Let F be the collection of all the equivalence classes $\{(a, b)\}$ or simply $\{[a, b]\}$. We now make F into a ring by define the operations $+_F$ and \cdot_F as follow :

$$[a, b] +_F [c, d] = [ad + bc, bd],$$

and

$$[a, b] \cdot_F [c, d] = [ac, bd].$$

One must check that the operations are well defined. It turns out that F is a field and we call it the field of Quotients of R .

Example 3.2.1. The field of quotients of \mathbb{Z} is \mathbb{Q} . The field of quotients of $\mathbb{Q}[x]$ is $\mathbb{Q}(x)$, which contains fractions where both denominators and numerators are in $\mathbb{Q}[x]$.

Our main aim in this section is to give a proof of

Theorem 3.2.1. Let R be a Unique Factorization Domain. Then $R[x]$ is also a Unique Factorization Domain.

To proceed with our proof, we need a few Lemmas.

Definition. Let R be an integral domain. A polynomial in $R[x]$ is called primitive if the common divisors of its coefficients are all units.

Suppose R is a Unique Factorization Domain and let Π be a complete set of irreducibles. It is clear that if every polynomial $f(x)$ in $R[x]$ can be written as $f(x) = cg(x)$ where $g(x)$ is a primitive (by just factoring out the common divisor of the coefficients via the irreducibles in Π), unique up to a factor of a unit. We say that $c := c(f)$ is the *content* of f . When $f(x)$ is primitive, we simply set $c(f) = 1$.

Example 3.2.1. The polynomial $3x^2 + 4x - 1$ is primitive. The polynomial $-15x^3 + 3x + 9$ is not primitive. But we have $-15x^3 + 3x + 9 = 3(-5x^3 + x + 3)$.

Lemma 3.2.2. (Gauss) If R is a Unique Factorization Domain, then a product of two primitive polynomials is primitive.

Proof. Let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{and} \quad g(x) = b_0 + b_1x + \cdots + b_mx^m$$

be primitive polynomials. Suppose $f(x)g(x) = c(fg)h(x)$ where $h(x)$ is primitive and $c(fg) \neq 1$. Let $p|c(fg)$ where p is an irreducible. Since $f(x)$ and $g(x)$ are both primitive, there exist minimal i, j such that $p \nmid a_i$ and $p \nmid b_j$. Consider the term c_{i+j} . Note that

$$c_{i+j} = \sum a_l b_k,$$

and by minimality of i, j , we find that p divides all the terms in c_{i+j} except $a_i b_j$. Hence p cannot divide the coefficients of $f(x)g(x)$. Therefore $c(fg) = 1$ and so $f(x)g(x)$ is primitive.

The next Lemma is very important in our proof of Theorem 3.2.1.

Lemma 3.2.3. Let R be a Unique Factorization Domain and let F be its field of quotients of R . Let $f(x) \in D[x]$ where $\deg f(x) > 0$. If $f(x)$ is an irreducible in $R[x]$, then $f(x)$ is also an irreducible in $F[x]$. (*Remember Gauss Lemma for $\mathbb{Q}[x]$?*) Also, if $f(x)$ is primitive in $R[x]$ and irreducible in $F[x]$ then $f(x)$ is irreducible in $R[x]$.

Proof. Suppose $f(x) = r(x)s(x)$, $r(x), s(x) \in F[x]$. By clearing denominators, $df(x) = r_1(x)s_1(x)$, where $r_1(x), s_1(x) \in R[x]$. Let $f(x) = c(f)g(x)$, where $g(x)$ is primitive in $R[x]$. Also, $r_1(x) = c(r_1)r_2(x)$ and $s_1(x) = c(s_1)s_2(x)$, where $r_2(x)$ and $s_2(x)$ are primitive polynomials. By Lemma 3.2.2, we conclude that $r_2(x)s_2(x)$ is primitive. Now,

$$dc(f)g(x) = c(r_1)c(s_1)r_2(x)s_2(x).$$

Therefore, $udc(f) = c(r_1)c(s_1)$, for some unit $u \in R$ and

$$df(x) = udc(f)r_2(x)s_2(x),$$

and

$$f(x) = uc(f)r_2(x)s_2(x).$$

If $f(x)$ is irreducible in $F[x]$ then $f(x)$ is certainly irreducible in $R[x]$.

We now set up the complete set of irreducibles in $R[x]$. Let Π_1 be the complete set of irreducibles in R and Π_2 be the set of primitive polynomials in $R[x]$ which are irreducible in $F[x]$, and such that no two polynomials differ by a unit in R . We let the complete set of irreducibles Π of $R[x]$ be $\Pi_1 \cup \Pi_2$.

We are now ready to complete the proof of Theorem 3.2.1.

Proof. We first suppose that $f(x) \in R[x]$. Then $f(x) \in F[x]$. Since $F[x]$ is a Unique Factorization Domain (why? Because F is a field and $F[x]$ is an Euclidean Domain and therefore a Unique Factorization Domain), we have

$$f(x) = up_1(x) \cdots p_k(x),$$

3.2. POLYNOMIAL RINGS OVER A UNIQUE FACTORIZATION DOMAIN 43

where $p_i(x) \in F[x]$ are irreducible polynomials and $u \in F$. Again clearing denominators, we conclude that

$$df(x) = aP_1(x) \cdots P_k(x), a \in R$$

where $P_i(x) \in R[x]$. Note that $P_i(x)$ are all irreducibles. Now, let $P_i(x) = c(P_i)v_iQ_i(x)$, where $Q_i(x)$ is primitive, irreducible polynomial in Π_2 . Then,

$$df(x) = UCQ_1(x) \cdots Q_k(x),$$

where U is a product of units and C is the product of irreducibles in Π_1 . Therefore, $(c(df) = c(d)c(f))$

$$udc(f) = C.$$

Therefore, $f(x) = wc(f)Q_1(x) \cdots Q_2(x) \cdots Q_k(x)$, and every polynomial is a product of elements in Π , where w is a unit in R .

Next we consider uniqueness. Suppose

$$f(x) = dp_1(x) \cdot p_k(x) = d'q_1(x) \cdots q_l(x),$$

where $p_i(x)$ and $q_j(x)$ are primitive irreducibles. Then $d = c(f)u$ and $d' = c(f)v$. Therefore, $d = d'vu^{-1}$. Next the irreducibility of $p_i(x)$ and $q_j(x)$ and the fact that we have chosen these from Π_2 shows that $p_1(x) = q_1(x), \cdots, p_k(x) = q_l(x)$, and $k = l$.

Corollary 3.2.4. Let R be a Unique Factorization Domain. Then $R[x_1, x_2, \cdots, x_n]$ is a Unique Factorization.

Incidentally we have shown that $\mathbb{Z}[x]$ is a Unique Factorization Domain which is not a Principal Ideal Domain.

Chapter 4

Fields

4.1 Examples of Fields

As indicated in Chapter 1, a field is a commutative Division Ring. We have seen the existence of both finite and infinite fields. We have also seen two ways of constructing fields. On the one hand, we can construct fields out of maximal ideals of a commutative ring with identity, on the other hand, we can construct fields out of integral domains.

We shall study in more details the properties of fields in this Chapter. We begin with a few examples :

Example 4.1.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Example 4.1.2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is a field.

Example 4.1.3. $\mathbb{Z}_p[i]$ is a finite field of p^2 elements.

Example 4.1.4. The set containing $p(x)/q(x)$ if $p(x)$ and $q(x)$ are both polynomials in $\mathbb{Q}[x]$ is a field. This is called the field of rational functions.

The field \mathbb{Q} and the field of rational functions are both constructed from Integral Domains and the fields in Example 4.1.2 and Example 4.1.3 are constructed from Maximal ideals of rings $\mathbb{Q}[x]$ and $\mathbb{Z}_p[x]$ respectively.

4.2 Characteristic of a field

Definition. A field F is said to have characteristic $p \neq 0$ if for some positive integer p , $px = 0$ for all $x \in F$, and no positive integer smaller than p enjoys this property.

If there is no p such that the above holds we say that the field F is of characteristic 0.

Theorem 4.2.1. The characteristic of a field is either 0 or a prime number.

Proof. If F has characteristic 0, we are done. Suppose there is a number n , minimal subject to the condition that $nx = 0$ for all $x \in F$. If $n = uv$, $u > 1, v > 1$, then $uv1_F = 0$. This can be viewed as $u \cdot 1_F \cdot v \cdot 1_F = 0$. Since $1 < u < n$ and $1 < v < n$, $u \cdot 1_F \neq 0$ and $v \cdot 1_F \neq 0$ and hence F is not an integral domain, and therefore cannot be a field. Hence, n is a prime number.

Remarks. Note that we only use the fact that any field is an integral domain with identity in the above proof.

Corollary 4.2.2. If D is an integral domain with identity, its characteristic is either 0 or a prime p .

Example 4.2.1. Prove Corollary 4.1.2 is true even if D is without identity.

4.3 A very brief excursion into Vector Spaces

In the discussion of fields, we need the notion of dimension. To establish the meaning of the dimension of a field over its subfield, we need to recall some basic facts of Vector Spaces.

Definition. A *Vector Space* V over a field F is an abelian group under $+$ such that for every $\alpha \in F$ and every $v \in V$, $\alpha v \in V$ and such that

1. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$, for $\alpha \in F, v_1, v_2 \in V$.

2. $(\alpha + \beta)v = \alpha v + \beta v$, for $\alpha, \beta \in F, v \in V$.
3. $\alpha(\beta v) = (\alpha\beta)v$, for $\alpha, \beta \in F, v \in V$.
4. $1v = v$ for all $v \in V$, where 1 is the identity of F .

Note that every field is a vector space.

We recall some of the basic facts and definitions you have encountered in Linear Algebra :

Fact 1. (Definition) A vector space is said to be finite dimensional if there exist a set of vectors $v_1, \dots, v_n \in V$ such that every element in $v \in V$ can be expressed uniquely as a linear combination of v_i , i.e.,

$$v = \sum_{j=1}^n \alpha_j v_j.$$

The minimal set of vectors $\{v_i\}$ satisfying the above property is called a basis of V .

Fact 2. If B and B' are the basis of V , then the number of elements in B and B' are the same. We denote this number by $\dim_F(V)$, read as the dimension of the vector space V over F .

If E is a field, then E is a vector space over itself. Now, if F is a subfield of E , we may view E as a vector space over F . If this vector space is finite dimensional, we write $[E : F] := \dim_F(E)$. The symbol $[E : F]$ is called the degree of the field E over F .

Example 4.3.1. The field $\mathbb{Z}_3[i] := \{a + ib \mid a, b \in \mathbb{Z}_3\}$ is a field having \mathbb{Z}_3 as a subfield. Note that it is a vector space of dimension 2, generated by 1 and i . Hence,

$$[\mathbb{Z}_3[i] : \mathbb{Z}_3] = 2.$$

Example 4.3.2. The field $\mathbb{Q}(\sqrt{2})$ has degree 2 over \mathbb{Q} .

4.4 Field Extensions

We have seen that $\mathbb{Q}(\sqrt{2})$ contains the field \mathbb{Q} . In general if E is a field containing the field F , we say that E is a *field extension* of F and that F is a subfield of E . We say that E is a finite extension of F if $[E : F]$, the degree of E over F , is finite. In other words, if E is a finite dimensional vector space over F .

Theorem 4.4.1. Let $F \subset E \subset L$ be three field such that both $[L : E]$ and $[E : F]$ are finite. Then L is a finite extension of F and

$$[L : F] = [L : E][E : F].$$

Proof. Consider E as a vector space over F and suppose $[E : F] = n$ and let $\{u_1, \dots, u_n\}$ be a basis of E over F . Next suppose $[L : E] = m$ and let $\{v_1, \dots, v_m\}$ be a basis of L over E . We claim that

$$B := \{u_i v_j | 1 \leq i \leq n, 1 \leq j \leq m\}$$

is a basis for the vector space L over F . Then we conclude that $[L : F] = mn$.

Step 1. We first show that any element in L can be written in terms of elements in B . Let $l \in L$. Then since L is a vector space over E ,

$$l = \sum_{i=1}^m a_i v_i, \quad a_i \in E.$$

But $a_i \in E$ implies that

$$a_i = \sum_{j=1}^n b_{i,j} u_j, \quad b_{i,j} \in F.$$

Hence,

$$l = \sum_{i=1}^m \sum_{j=1}^n b_{i,j} u_j v_i.$$

Step 2. We next prove that the elements in B are linearly independent. Suppose

$$\sum_{i=1}^n \sum_{j=1}^m b_{i,j} u_j v_i = 0.$$

Then

$$\sum_{i=1}^n \left(\sum_{j=1}^m b_{i,j} u_j \right) v_i = 0.$$

Since v_i 's are linearly independent,

$$\sum_{j=1}^m b_{i,j} u_j = 0.$$

Since u_j 's are linearly independent, $b_{i,j} = 0$.

Corollary 4.4.2. If $F \subset E \subset L$ are three fields such that $[L : F]$ is finite, then $[E : F]$ divides $[L : F]$.

Example 4.4.1. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 4 over \mathbb{Q} . Note that we may prove this by observing that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}].$$

The next Theorem shows us that every elements of a finite field extension satisfy a certain polynomial equation.

Theorem 4.4.3. Suppose that E is a finite extension of F of degree n . Then, given any element u in E there exist elements $\alpha_0, \alpha_1, \dots, \alpha_n \in F$, not all zeros, such that

$$\alpha_0 + \alpha_1 u + \dots + \alpha_n u^n = 0.$$

Proof. This follows easily from the fact that E may be viewed as a vector space of dimension n over F . In other words, consider $1, u, u^2, \dots, u^n$. These must be linearly dependent elements over F .

Definition. Let $E \subset F$ be fields. Then $a \in E$ is said to be algebraic over F if there exists a polynomial $p(x) \neq 0 \in F[x]$ such that $p(a) = 0$. An extension E of F is said to be algebraic if all the elements in E is algebraic over F .

The above Theorem says that every finite extension of F is algebraic. Is the converse true?

Example 4.4.2. Let $F = \mathbb{Q}$. We say that a is an algebraic number if a satisfies the equation $p(a) = 0$ with $p(x) \in \mathbb{Q}[x]$. The numbers $\sqrt{\sqrt{1 + \sqrt{3}}}$, $\sqrt{2} + \sqrt{3}$, $2^{1/n}$ are all algebraic numbers. It is a non-trivial fact (due to Lindemann) that π is not algebraic. A non algebraic number is called a transcendental number.

Example 4.4.3. Prove that $\cos \pi/180$ is algebraic over \mathbb{Q} .

Definition. A complex number is said to be an algebraic number if it is algebraic over \mathbb{Q} .

We will see that the set of algebraic numbers form a subfield of \mathbb{C} .

Definition. We say that a is a root of a polynomial $p(x)$ if $p(a) = 0$.

We have seen that every element in a finite field extension of F is algebraic over F , i.e., they are roots of polynomials over F . We now ask the following question : If E is any field extension of F and $a \in E$ is algebraic over F , can we generate a finite extension using a ? The answer is yes. We consider $a \in E$. Since a is algebraic over F , there exist a polynomial $f(x)$ such that $f(a) = 0$. Let $p(x)$ be a monic polynomial with minimal degree for which $p(a) = 0$. This polynomial is called the minimal polynomial for a over F .

We claim that $p(x)$ is irreducible polynomial over F . Suppose not. Then $p(x) = q(x)r(x)$ for some $q(x), r(x) \in F[x]$ with degrees less than that of $p(x)$. Now, $p(a) = 0$ implies $q(a)r(a) = 0$. Since E is a field and $q(a), r(a) \in E$, $q(a) = 0$ or $r(a) = 0$ (E being an integral domain). This contradicts the minimality of the degree of $p(x)$. We have shown that

Lemma 4.4.4. Suppose $a \in K$ is algebraic over F with minimal polynomial $p(x)$ in $F[x]$. Then $p(x)$ is irreducible in $F[x]$.

Now, we know that if $p(x)$ is irreducible then $F[x]/(p(x))$ is a field isomorphic to $F[a] = F(a)$ via the homomorphism

$$\varphi(f(x)) = f(a).$$

What is the degree $[F(a) : F]$? To find the degree, we consider $f(x) \in F[x]$. Then by the Division algorithm, $f(x) = q(x)p(x) + r(x)$, $\deg r(x) < \deg p(x) =: n$ or $r(x) = 0$. This implies that $f(a) = r(a)$ since $p(a) = 0$. Since any element of $F(a)$ is of the form $f(a)$ for some $f(x) \in F[x]$, the above shows that they can be represented using $1, a, a^2, \dots, a^{n-1}$ as $\deg r(x) < n$. Note

that $1, a, a^2, \dots, a^{n-1}$ are linearly independent. For other wise, a would satisfy a polynomial equation with degree less than n , a contradiction to n being the smallest degree of such polynomial. In conclusion, we have shown that $[F(a) : F] = n = \deg f(x)$. We have thus obtained a finite field extension from any element of a field Extension. This field extension $F(a)$ is called the field obtained by adjoining a to F . It is sometimes called a *simple extension*. We now summarize

Theorem 4.4.5. Let $F \subset E$ and suppose $a \in E$ is algebraic over F with minimal polynomial $p(x)$ such that $\deg p(x) = n$. Then $F(a)$, the field obtained by adjoining a to F , is a finite extension of F , and

$$[F(a) : F] = n.$$

Example 4.4.4. The extension $\mathbb{Q}(\sqrt{2})$ is a simple extension. The minimal polynomial of $\sqrt{2}$ over \mathbb{Q} is $x^2 - 2$. Note that this is irreducible over \mathbb{Q} .

Example 4.4.5. One might think that simple extensions are just a special example of field extension. It turns out that when F is of characteristic 0, every finite extension of F is a simple extension. Suppose $K = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, can you find an element a such that $K = \mathbb{Q}(a)$? (Answer : $a = \sqrt{2} + \sqrt{3}$, note that this is not unique.)

There is a result more general than the above form. It is known as Theorem of Primitive Element. You will learn the proof of this result in the course on Galois Theory.

Example 4.4.6. What is the degree of $\omega = \cos(2\pi/3) + i \sin(2\pi/3)$? The equation satisfied by the number is $z^3 = 1$. The polynomial splits as $(z - 1)(z^2 + z + 1)$ and we have shown that $z^2 + z + 1$ is irreducible over \mathbb{Q} . Hence the minimal polynomial of ω has degree 2. As a result, the degree $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

Example 4.4.7. Show that $\sqrt{7} + \sqrt{2}$ is algebraic. $\sqrt{7} + \sqrt{2} \in \mathbb{Q}(\sqrt{7}, \sqrt{2}) =: E$. It suffices to show that E is a finite extension. Now,

$$[\mathbb{Q}(\sqrt{2})(\sqrt{7}) : \mathbb{Q}(\sqrt{2})] = 2$$

and

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

Hence, E is finite and therefore the number is algebraic.

4.5 Finite Extension and Algebraic Extension

In this section, we will show that if $F \subset E$ are two fields, then $A(E/F)$, the set of all elements in E algebraic over F , is a subfield of E .

Theorem 4.5.1. $A(E/F)$ is a subfield of E .

Proof. Let a and b be algebraic over F . Then $F(a)$, the field constructed from the previous section is a finite extension of F . Using the same argument, $F(a)(b) = F(a, b)$ is a finite extension of $F(a)$, and hence, a finite extension of F . Therefore, every element in $F(a, b)$ is algebraic over F . Since $a \pm b, ab, a/b \in F(a, b)$, we conclude that $a \pm b, ab, a/b$ are all algebraic over F and so, they are in $A(E/F)$. Hence $A(E/F)$ is a subfield of E .

We have used the notation $F(a, b)$ and now we make it precise. When we write $F(a)$ we mean the field derived from adjoining the *root* of a certain irreducible polynomial $p(x)$ to F . So,

$$F(a) \simeq F[x]/(p(x)).$$

We now define $F(a, b) := F(a)(b)$ as the field obtained by adjoining the root of an irreducible polynomial $q(x)$ over $F(a)$. Thus,

$$F(a, b) \simeq F(a)[x]/(q(x)).$$

Note that if $Q(x)$ is the irreducible polynomial of b in $F[x]$ and if $Q(x)$ splits in $F(a)[x]$, then one of its irreducible factor must contain b as a root. This irreducible factor is $q(x)$. Hence $\deg q(x) \leq \deg Q(x)$. So, this implies that if $Q(x)$ is the irreducible polynomial of degree m in $F[x]$, then

$$[F(a, b) : F(a)] \leq m,$$

and therefore

$$[F(a, b) : F] \leq mn,$$

if a is the root of a degree n irreducible polynomial. This discussion allows us to conclude the following :

Corollary 4.5.2. If a and b in E are algebraic, and are roots of irreducible polynomials over F of degrees m and n , respectively, then $[F(a, b) : F] \leq mn$

and thus, $a \pm b, ab, a/b$ are roots of irreducible polynomials of degree at most mn .

Example 4.5.1. The element $2 \cos(\frac{\pi}{p})$ is equal to $z + 1/z$ where $z = e^{2\pi i/p}$. This element z satisfies $x^p - 1 = 0$. Therefore the minimal polynomial satisfied by $2 \cos(\frac{\pi}{p})$ is at most of degree $p - 1$ (why?). In particular, it lies in a finite extension of \mathbb{Q} and is thus, an algebraic number.

Example 4.5.2. The element $2^{1/6} + \sqrt{2}$ is an algebraic number. Note that $2^{1/6}$ satisfies a minimal polynomial of degree 6 in \mathbb{Q} and $\sqrt{2}$ satisfies one with degree 2. However the degree of the field containing $2^{1/6}$ and $\sqrt{2}$ has degree 6, not 12. Note that

$$(x^6 - 2) = (x^3 - \sqrt{2})(x^3 + \sqrt{2})$$

in $\mathbb{Q}(\sqrt{2})$.

Example 4.5.3. Is $F(a, b) = F(b, a)$? Yes, $F(b) \subset F(a)(b)$. Now, $a \in F(a)(b)$, and so, $F(b)(a) \subset F(a)(b)$. Hence the result.

We now return to Theorem 4.5.1. Let $F = \mathbb{Q}$ and $E = \mathbb{C}$. Then $A(\mathbb{C}/\mathbb{Q})$ is the set of all algebraic numbers. Note that this is not a finite field extension of \mathbb{Q} . We conclude from our discussion that the set of all algebraic numbers form a subfield of \mathbb{C} . We now prove a rather interesting fact about algebraic numbers, i.e., we have captured all algebraic numbers in $A(\mathbb{C}/\mathbb{Q})$.

Theorem 4.5.3. If $u \in \mathbb{C}$ is algebraic over $\mathcal{A} := A(\mathbb{C}/\mathbb{Q})$, then u is in \mathcal{A} .

Proof. Note that u is algebraic over \mathcal{A} implies that it satisfies a polynomial equation

$$p(x) = a_0 + \cdots + a_n x^n = 0,$$

where $a_i \in \mathcal{A}$. Since a_i are algebraic over \mathbb{Q} , we suppose that they are roots of irreducible polynomials of degrees m_i respectively. Hence, the field $\mathbb{Q}(a_1, a_2, \dots, a_n)$ is a finite extension of \mathbb{Q} of degree at most $m_1 m_2 \cdots m_n$. Now u is now in $\mathbb{Q}(a_1, a_2, \dots, a_n, u)$, which is a finite extension of \mathbb{Q} , we deduce that u is algebraic over \mathbb{Q} and hence, $u \in \mathcal{A}$.

When we don't get any more new fields by adjoining elements \mathbb{C} algebraic over \mathcal{A} to \mathcal{A} , we say that \mathcal{A} is *algebraically closed*.

4.6 Constructibility

In this Section, we are going to answer a few questions which still haunt many amateurs. We will show that

1. It is impossible to trisect an arbitrary angle using straight edge and compass.
2. It is impossible to duplicate a cube of volume 1 using just straight edge and compass. (By duplicating a cube, we mean constructing a cube doubling the volume of the original cube)

First, we need to define what we mean by construction using straight edge and compass. By straight edge, we mean that we are only allowed to use straight lines with unit length. By compass, we mean that we are allowed to use arcs with radius constructible from straight edge of unit length. We are also allowed to construct lines parallel to a given one.

Definition. The real number a is said to be constructible number if $|a|$, the absolute value of a , is a constructible length.

Lemma 4.6.1. The constructible numbers form a subfield of real numbers.

Theorem 4.6.2. In order that the real number a is constructible it is necessary that $[\mathbb{Q}(a) : \mathbb{Q}]$ be a power of 2. Equivalently the minimal polynomial of a over \mathbb{Q} must have degree a power of 2.

Corollary 4.6.3. It is impossible to duplicate a cube of volume 1.

Proof. To duplicate a cube, we have to solve $x^3 = 2$. But the degree $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$ is not a power of 2 and hence $2^{1/3}$ is not constructible.

Corollary 4.6.4. It is impossible to trisect 60° by straight edge and compass.

Proof. To trisect an angle, we consider

$$\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta.$$

Clearly, $\cos 60^\circ = \frac{1}{2}$ is constructible. If we can construct $\cos \theta$ we can trisect 60° . However, the above equation shows that $\cos 20^\circ$ satisfies the equation

$$8x^3 - 6x - 1 = 0.$$

Let $f(x) = x^3 - 3x - 1$. Then $f(2x) = 8x^3 - 6x - 1$. So if $f(x)$ is irreducible, so is $f(2x)$. But $f(x + 1)$ is irreducible by Eisenstein criterion. Hence, $8x^3 - 6x - 1$ is irreducible. Therefore, $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$ and $\cos 20^\circ$ is not constructible.

4.7 Roots of Polynomials

Let $F[x]$ be the polynomial ring over the field F . Let E be a field extension of F . If $p(x) \in F[x]$ is represented by

$$p(x) = a_0 + a_1x + \cdots + a_nx^n,$$

then we write for any $a \in E$,

$$p(a) = a_0 + a_1a + \cdots + a_na^n.$$

We say that a is a root of $p(x)$ if $p(a) = 0$.

Given $a \in E$, we have shown how to construct the field $F(a)$ via the map

$$F[x] \rightarrow F(a),$$

sending $f(x) \in F[x]$ to $f(a)$. Suppose now we start with some polynomial $f(x)$ of positive degree instead of starting with a field extension E of F . Our goal is to construct a field extension E of F for which a is a root of $f(x)$ and $a \in E$.

Lemma 4.7.1. If $a \in E$ is a root of $p(x) \in F[x]$ of degree n then $f(x) = (x - a)g(x)$, where $g(x) \in E[x]$ has degree $n - 1$. Conversely if $f(x) = (x - a)g(x)$ with $g(x) \in E[x]$ then $a \in E$.

Proof. If $a \in E$, $x - a \in E[x]$. By division algorithm, $f(x) = (x - a)g(x) + r(x)$, $r(x)$ a constant in E . But $f(a) = 0$ implies that $r(a) = 0$. The degree of $g(x)$ follows from $\deg a(x)b(x) = \deg a(x) + \deg b(x)$. Hence the result.

Conversely, if $f(x) = (x - a)g(x)$, then clearly, $f(a) = 0$ and a is a root of $f(x)$.

The next result is an important ingredient in showing that all finite subgroups of a field is cyclic.

Lemma 4.7.2. Let $f(x) \in F[x]$ have degree n , then $f(x)$ can have at most n roots in any extension E of F .

Proof. We prove by induction. If $\deg f(x) = 1$, then $f(x) = ax + b$, $a \neq 0$, and the root is $x = -ba^{-1}$.

Suppose the Theorem is true for degree of polynomials $< n$. Let $f(x)$ be a polynomial of degree n . If $f(x)$ has no root in E , then we are done. Suppose $a \in E$ such that $f(a) = 0$. Then by Lemma 4.7.1, $f(x) = (x - a)g(x)$. Now $g(x)$ has degree less than n and so there are at most $n - 1$ roots in E . Together with the root a , $f(x)$ can have at most n roots in E . This completes the proof.

It turns out that when $f(x)$ has repeated roots, namely, $f(x) = (x - a)^{k_1}g(x)$ that $f(x)$ has less than n distinct roots in E . The number k_1 is called the multiplicity of the root a .

Definition. We say that $f(x)$ splits into linear factors in E if

$$f(x) = (x - a_1)^{k_1} \cdots (x - a_m)^{k_m}.$$

Example 4.7.1. When E is a finite field, $E \setminus \{0\}$ is a finite group of order $q - 1$. We know from Group Theory that $x^{q-1} = 1$ for all $a \in E$. Hence, the polynomial $x^{q-1} - 1$ splits into linear factors in E , namely,

$$x^{q-1} - 1 = (x - a_1)(x - a_2) \cdots (x - a_{q-1}),$$

where $a_i \in E$ are distinct.

Example 4.7.2. When $E = \mathbb{Z}_p$, we have

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p - 1)).$$

Setting $x = 0$, we obtain

$$(p - 1)! \equiv -1 \pmod{p},$$

which is known as Wilson's Theorem.

We are now ready to construct a field E containing some roots of an arbitrary chosen $f(x)$.

Theorem 4.7.3. Let F be a field and $f(x)$ a polynomial of positive degree n in $F[x]$. Then there exists a finite extension E of F with $[E : F] \leq n$, in which $f(x)$ has a root.

Proof. We know that $f(x)$ is divisible by some irreducible polynomial $p(x)$. So if we can find a field E containing the roots of irreducible polynomial $p(x)$ dividing $f(x)$, we are done.

Since $p(x)$ is irreducible, $F[x]/M$ is a field, where $M = (p(x))$. Let $E = F[x]/M$. Strictly speaking F is not contained in E . But E contains an isomorphic copy of F . In fact the set $\mathcal{F} := \{u + M \mid u \in F\} \subset E$ is such a copy. (Any nonzero homomorphism from a field F to another field is injective!) So in this way, we could consider E as an extension of F .

Denote $x + M \in E$ by a . Then we can show that $\psi : F[x] \rightarrow E$ by $\psi(f(x)) = f(a)$. Note that ψ is a homomorphism. Now, if $p(x) = \sum_{k=0}^m a_k x^k$, then

$$\begin{aligned} \psi(p(x)) &= \sum_{k=0}^m a_k (x + M)^k \\ &= \sum_{k=0}^m a_k (x^k + M) \\ &= \sum_{k=0}^m a_k x^k + M = 0 + M, \end{aligned}$$

since $p(x) \in M$. Therefore, $\psi(p(x)) = 0 + M$. But on the other hand, $\psi(p(x)) = p(a)$. Hence, $a \in E$ is a root of $p(x)$. It can be shown that $[E : F] = m$, the degree of $p(x)$. (See Theorem 4.4.5.) Hence,

$$[E : F] \leq n = \deg f(x).$$

Theorem 4.7.4. Let $f(x) \in F[x]$ be of degree n . Then there exists an extension E of F of degree at most $n!$ over F such that $f(x)$ has n roots, counting multiplicities, in E . Equivalently $f(x)$ splits into linear factors in E .

Proof. We go by induction on n , the degree of $f(x)$. If $n = 1$, the result is clear. Suppose the result is true up to degree $< n$. Let $f(x)$ be a polynomial of degree n . Then by Theorem 4.7.3., there is a field E_1 such that $[E_1 : F] \leq n$ containing a root of $f(x)$. By Lemma 4.7.1, $f(x) = (x - a)g(x)$, with $g(x) \in E_1[x]$. By induction, there is an extension E_2 of E_1 such that $[E_2 : E_1] \leq (n - 1)!$ and that E_2 contains all the roots of $g(x)$. Hence, E_2 contains all the roots of $f(x)$ and

$$[E_2 : F] = [E_2 : E_1][E_1 : F] \leq n!.$$

The field E which contains all the roots of $f(x)$ is called the splitting field of $f(x)$. The above result shows that splitting field exists for any polynomial $f(x)$. This is perhaps the starting point of Galois Theory.

Example 4.7.3. The polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ splits completely in $\mathbb{Q}(e^{2\pi i/p})$. Note that the degree of this extension is $p - 1$.

Example 4.7.4. It is possible to construct a polynomial $f(x)$ of degree n for which the splitting field is of larger degree. For example, let $f(x) = x^3 - 2$. Then the roots are $\omega \cdot 2^{1/3}$, $\omega^2 \cdot 2^{1/3}$, and $2^{1/3}$, where $\omega = e^{2\pi i/3}$. The splitting field of $f(x)$ is $\mathbb{Q}(2^{1/3}, \omega)$, with degree 6 over \mathbb{Q} .

Chapter 5

Groups and fields

In this final Chapter, we investigate some relations between Groups and Fields. We will need some results from Group Theory but I will try to include all the proofs. The first result I wish to present is the fact that all finite subgroups of the multiplicative group $F^* := F \setminus \{0\}$ is a cyclic group. In other words, they are generated by one element. The second result is the proof of the surprising fact that every finite division ring is a field.

5.1 Classification of Finite abelian groups

Recall that a set G , together with a binary operation $*$, is a group if

- (i) There exists an element e such that $e * g = g = g * e$ for all $g \in G$.
- (ii) For every $g \in G$, there is an element g^{-1} such that $g * g^{-1} = e$.
- (iii) For every a, b, c , $a * (b * c) = (a * b) * c$.

A group is abelian if for every $a, b \in G$, $a * b = b * a$. In this Section, we write an abelian group additively, namely, $G = (G, +)$.

Theorem 5.1.1. Let G be a finite abelian group, Then

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_k,$$

where $|G_i| = p_1^{\alpha_i}$ divides $|G|$ exactly.

For those who have some background in Group Theory, this says that G is the direct sum of its Sylow's p -subgroups.

Proof. Let $|G| = n = \prod_{i=1}^k p_i^{e_i}$, with $p_i = \text{prime}$. Define

$$G_i = \{g \in G \mid p_i^{e_i} g = 0\}.$$

Then, check that G_i is a subgroup of G .

We claim that $G_i \cap \sum_{j \neq i} G_j = 0$.

Let $x \in G_i \cap \sum_{j \neq i} G_j$. Since $x \in G_i$,

$$p_i^{e_i} x = 0.$$

Also,

$$x \in \sum_{j \neq i} G_j,$$

so

$$x = \sum_{j \neq i} x_j$$

and

$$p_j^{e_j} x_j = 0.$$

Put

$$n_i = \frac{n}{p_i^{e_i}} = \prod_{j \neq i} p_j^{e_j}.$$

Then $n_i x_j = 0$ and so, $n_i x = 0$. But n_i and $p_i^{e_i}$ are coprime, there exist u and v such that

$$un_i + vp_i^{e_i} = 1$$

and this implies that

$$1 \cdot x = (un_i + vp_i^{e_i})x = 0.$$

Therefore $x = 0$.

Next we claim that

$$G = G_1 + \cdots + G_k.$$

As before, let

$$n_i = \frac{n}{p_i^{e_i}}.$$

Note that n_1, \dots, n_k are relatively prime. Hence, $\gcd(n_1, n_2, \dots, n_k) = 1$. Therefore,

$$1 = l_1 n_1 + \dots + l_k n_k$$

for certain $l_i \in \mathbb{Z}$. Let $g \in G$ then

$$\begin{aligned} g &= 1 \cdot g \\ &= (l_1 n_1 + \dots + l_k n_k)g \\ &= (l_1 n_1)g + \dots + (l_k n_k)g. \end{aligned}$$

Now, $l_i n_i g \in G_i$.

$$\begin{aligned} p_i^{e_i}(l_i n_i)g &= l_i(p_i^{e_i} \cdot n_i)g \\ &= l_i n g \\ &= 0, \end{aligned}$$

since $|G| = n$. Therefore, $g \in G_1 + \dots + G_k$. Hence, $G = G_1 + \dots + G_k$. Therefore,

$$G = G_1 \oplus G_2 \oplus \dots \oplus G_k$$

and G_i is a p_i group.

We next claim that if G is a finite subgroup of the multiplicative group F^* (Sorry! We are going back to the multiplicative notation.) with order p^α then G is cyclic.

Lemma 5.1.2. Suppose G is a finite subgroup of the multiplicative group F^* of order p^α , then G is cyclic.

Proof. Suppose G is not cyclic. Then $G = G_1 \oplus G_2 \oplus \dots \oplus G_k$, where G_i 's are cyclic with order a power of p , say, $|G_i| = p^{\alpha_i}$. Let $p^a = \max_i |G_i|$. Then $g^{p^a} = 1$ for all $g \in G$. Since G is a subset of a field, there can be at most p^a solutions (See Lemma 4.7.2) to the equation

$$x^{p^a} - 1 = 0.$$

This shows that $p^\alpha = p^{\alpha_1} + p^{\alpha_2} + \dots + p^{\alpha_k} \leq p^a \leq p^\alpha$, or

$$p^a = p^\alpha = p^{\alpha_1} + p^{\alpha_2} + \dots + p^{\alpha_k}.$$

But by definition of a , $\alpha_i = a$ for some i , say, $\alpha_1 = a$. Hence, $p^{\alpha_2} + \cdots + p^{\alpha_k} = 0$. Hence G is cyclic.

Theorem 5.1.3. If G is a finite subgroup of F^* then G is cyclic.

Proof. G , with order $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is a direct sum of cyclic groups, by Theorem 5.1.1 and Lemma 5.1.2. By letting $a = g_1 g_2 \cdots g_k$, where g_i generates the cyclic group of order $p_i^{\alpha_i}$, we see that G is generated by a .

Example 5.1.1. For every finite field F of characteristic p , F^* is a cyclic group.

5.2 Wedderburn's Theorem

If $a, b \in G$, (G a finite group), we say that a and b are conjugates if there exists an element $g \in G$ such that $b = g^{-1}ag$. If we say that $a \sim b$ (a is equivalent to b) if and only if a and b are conjugates, then we may conclude that \sim is an equivalent relation. Furthermore,

$$G = C_1 \cup C_2 \cup \cdots \cup C_k,$$

where C_i are the equivalence classes. More importantly,

$$|G| = |C_1| + |C_2| + \cdots + |C_k|.$$

Let $a \in C_i$. We define

$$N(a) := \{g \in G : ga = ag\}.$$

Note that $N(a)$ is a subgroup of G . We wish to establish the fact that

$$|G|/|N(a)| = |C_i|.$$

For this we set up the map

$$\varphi : G/N(a) \rightarrow C_i,$$

via

$$\varphi(gN(a)) = gag^{-1}.$$

Note that the map is onto and one to one and so the sets have the same number of elements.

In other words we have shown that

Class Equation.

$$|G| = |G|/|N_1| + \cdots + |G|/|N_k|,$$

where N_i are subgroups of G .

We need another piece of information. Recall that $x^{p-1} + \cdots + x + 1$ is irreducible over \mathbb{Q} by Eisenstein criterion when p is a prime. These are minimal polynomials of the algebraic number $e^{2\pi i/p}$. Suppose that we replace p by any arbitrary integer n . Then we define $\Phi_n(x)$ to be the minimal polynomial of $e^{2\pi i/n}$, in other words, it is the product of all primitive n^{th} roots of unity. Note that

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

These polynomials are called cyclotomic polynomials.

We first claim that $\Phi_n(x)$ is a monic polynomial with integer coefficients. Consider the polynomial $x^n - 1$. Note that every roots of $x^n - 1$ is a root of some $\Phi_d(x)$ where $d|n$ and vice versa. Hence,

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Now, $\Phi_2(x) = x + 1$ and suppose $\Phi_k(x)$ are monic with integer coefficients for $k < n$. Then

$$x^n - 1 = \Phi_n(x)g(x),$$

where $g(x)$ is monic with integer coefficients. Therefore $\Phi_n(x)$ is monic with integer coefficients.

Now, if $d|n$ then $\Phi_d(x)|g(x)$. Hence,

$$\Phi_n(x) \left| \frac{x^n - 1}{x^d - 1} \right.$$

In particular, if $x = q$, where q is a positive integer, we have

Lemma 5.2.1.

$$\Phi_n(q) \left| \frac{q^n - 1}{q^d - 1} \right.$$

Now, $\Phi_n(q) = \prod(q - \theta)$, where θ are primitive n^{th} roots of unity. Now, $|q - \theta| > |q - 1|$, hence we have

Lemma 5.2.2. For $n > 1$,

$$|\Phi_n(q)| > q - 1.$$

We are now ready to prove Wedderburn's Theorem.

Theorem 5.2.3. A finite division ring is a field.

Let K be a finite division ring. Consider

$$Z(K) = \{z \in K \mid zx = xz \text{ for all } x \in K\}.$$

Note that $Z(K)$ is a finite field, with say, q elements. Since K is a finite division ring, it can be regarded as a finite dimensional vector space over $Z(K)$. Therefore, $|K| = q^n$. Our aim is to prove that $n = 1$ so that $K = Z(K)$.

We now regard $G = K^*$ as a multiplicative group of order $q^n - 1$. Define for any $a \in G$, $N(a) = \{g \in G : ga = ag\}$. Note that $N(a) \cup \{0\}$ contains $Z(K)$ and so, it is a finite dimensional vector space over $Z(K)$, and hence has order $q^{n(a)} - 1$. By the class equation, we conclude that

$$q^n - 1 = q - 1 + \sum_{n(a) \mid n, n(a) \neq n} \frac{q^n - 1}{q^{n(a)} - 1}.$$

By Lemma 5.2.1, $\Phi_n(q)$ divides

$$q^n - 1 \quad \text{and} \quad \frac{q^n - 1}{q^{n(a)} - 1},$$

and hence, it divides $q - 1$. But $|\Phi_n(q)| > |q - 1|$ by Lemma 5.2.2, if $n > 1$. This forces $n = 1$ and we are done.