Alireza Salehi Golsefidy

Algebra: ring and field theory

Contents

Chapter 1

Lecture 1

In this lecture, we start with a *pseudo-historical note* on algebra. Next *ring* is defined and some examples are briefly mentioned. *Ring of polynomials* and *direct product of rings* are discussed. Then basic properties of ring operations are discussed. At the end, we define *subrings*, ring *homomorphism*, and ring *isomorphism*

1.1 Introduction: a pseudo-historical note

A large part of algebra has been developed to systematically study zeros of polynomials. The word *algebra* comes from the name of a book by *al-Khwarizmi*, a Persian mathematician, [1] where al-Khwarizmi essentially gave algorithms to find zeros of linear and quadratic equations. Khayyam, another Persian mathematician, made major advances in understanding of zeros of cubic equations. In the 16th century, Italian mathematicians came up with formulas for zeros of general cubic and quartic equations. The cubic case was solved by del Ferro, and Ferrari solved the quartic case.[2] In 1824, Abel proved that there is *no* solutions in radicals to a general polynomial equation of degree at least 5. In 1832, Galois used *symmetries* (group theory) of *system of numbers* of zeros of a polynomial to systematically study them, and he gave the precise condition under which solutions can be written using radicals (and the usual operations $+, -, \cdot, /$).

Another problem which had a great deal of influence on shaping modern algebra is Fermat's last conjecture: there are no *positive integers* x, y, z such that $x^n + y^n = z^n$ if n is an integer more than 2. As you can see this problem has two new directions:

1. it is a *multi-variable* equation,
2. it is a *Diophantine* equation. This means we are looking for *integer* solutions instead of complex or real solutions.

The first direction was important in the development of the *algebraic geometry*, and the second one was played a crucial role in the development of *algebraic number theory*.

[1] I am Persian, and so I have to start with this!

[2] In the book *A History of Algebra; from al-Khwarizmi to Emmy Noether*, by van der Waerden, you can read about the very interesting history of the solution of cubic equations by del Ferro, Tartaglia, and Cardano.

In this course, I often try to put what we learn in the perspective of these *pseudo-historical* remarks.

1.2 Rings: definition and basic examples.

As we mentioned earlier, our hidden agenda is to understand zeros of a polynomial. Say $p(x)$ is a polynomial with rational coefficients. We would like to *understand* properties of a zero $\alpha \in \mathbb{C}$ of $p(x)$. What exactly does understanding mean here? Whatever it means, we would expect to be able to do basic arithmetic with α: *add and multiply*, and find out if we are getting the same values or not. As we see later, this means we want to understand various properties of the *subring* of $\mathbb{C}$ that is *generated* by α.

Definition 1.2.1. *1. A ring $(R, +, \cdot)$ is a set R with two binary operations: $+$ (addition) and $\cdot$ (multiplication) such that the following holds:*

(i) $(R, +)$ is an abelian group.

(ii) (Associative) For every $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iii) (Distributive) For every $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (b + c) \cdot a = b \cdot a + c \cdot a.$$

2. We say R is a unital *ring if there is $1 \in R$ such that $1 \cdot a = a \cdot 1$ for every $a \in R$.*

3. We say R is a commutative *ring if $a \cdot b = b \cdot a$ for every $a, b \in R$.*

Basic examples.

The set $\mathbb{Z}$ of integers, the set $\mathbb{Q}$ of rational numbers, the set $\mathbb{R}$ of real numbers, and the set $\mathbb{C}$ of complex numbers are unital commutative rings.

Some non-examples.

The set of non-negative integers $\mathbb{Z}^{\geq 0}$ is not a ring as $(\mathbb{Z}^{\geq 0}, +)$ is not an abelian group.

The set of even integers $2\mathbb{Z}$ is a commutative ring, but it is not unital.

For an integer n more than 1, the set $\mathrm{M}_n(\mathbb{R})$ of n-by-n matrices with real entries is a unital ring, but it is not commutative. In fact, for every ring R and positive integer n, the set $\mathrm{M}_n(R)$ of n-by-n matrices with entries in R with the usual matrix addition and multiplication forms a ring. Moreover, if R is unital, then $\mathrm{M}_n(R)$ is also unital.

Ring of integers modulo n.

The set $\mathbb{Z}_n$ of integers modulo n is another important ring. Let us recall that the residue class $[a]_n$ of a modulo n consists all the integers of the form $nk + a$ where k is an integer. In group theory, you have learned that $\mathbb{Z}_n = \{[0]_n, \ldots, [n-1]_n\}$ can be identified with the quotient group $\mathbb{Z}/n\mathbb{Z}$, and the residue class $[a]_n$ of a modulo n

is precisely the coset $a + n\mathbb{Z}$ of the (normal) subgroup $n\mathbb{Z}$. Let us also recall that for every $a, a', b, b' \in \mathbb{Z}$ and positive integer n the following holds:

$$\left.\begin{array}{r} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{array}\right\} \Rightarrow aa' \equiv bb' \pmod{n}.$$

This implies that the following is a well-defined binary operator on $\mathbb{Z}_n$:

$$[a]_n \cdot [b]_n := [ab]_n$$

for every a and b in $\mathbb{Z}$. It is easy to check that $(\mathbb{Z}_n, +, \cdot)$ is a unital commutative ring.

Exercise 1.2.2. *Work out the details of why $\mathbb{Z}_n$ is a ring.*

Ring of Polynomials.

As we have mentioned earlier, polynomials play an indispensable role in algebra. Notice that we can and will work with polynomials with coefficients in an arbitrary ring R. The set of all polynomials with coefficients in a ring R and an indeterminant x is denoted by $R[x]$. Therefore

$$R[x] := \{a_n x^n + \cdots + a_0 |\ n \in \mathbb{Z}^{\geq 0}, a_0, \ldots, a_n \in R\}.$$

We sometimes write $\sum_{i=0}^n a_i x^i$ instead of $a_n x^n + \cdots + a_0$. In some arguments it is more convenient to write a polynomial as an infinite sum $\sum_{i=0}^\infty a_i x^i$ with an understanding that $a_{n+1} = a_{n+2} = \cdots = 0$ for some non-negative integer n. Based on our experience of working with polynomials with real or complex coefficients, we define the following operations:

$$\Big(\sum_{i=0}^\infty a_i x^i\Big) + \Big(\sum_{i=0}^\infty b_i x^i\Big) := \sum_{i=0}^\infty (a_i + b_i) x^i \qquad \text{(addition)}$$

$$\Big(\sum_{i=0}^\infty a_i x^i\Big)\Big(\sum_{i=0}^\infty b_i x^i\Big) := \sum_{n=0}^\infty \big(\sum_{i=0}^n a_i b_{n-i}\big) x^n \qquad \text{(multiplication)}$$

for every $\sum_{i=0}^\infty a_i x^i, \sum_{i=0}^\infty b_i x^i \in R[x]$. It is easy to see that $(R[x], +, \cdot)$ is a ring.

Example 1.2.3. *Compute* $([2]_4 x + [1]_4)([2]_4 x^2 + [3]_4 x + [1]_4)$ *in* $\mathbb{Z}_4[x]$.

Solution. We start the computation as if the coefficients were real numbers and use the distribution law. Moreover to simplify our notation, we drop the decoration $[\ ]_4$, but we remember that computation of coefficients should be done in $\mathbb{Z}_4$. Hence:

$$\begin{aligned} &([2]_4 x + [1]_4)([2]_4 x^2 + [3]_4 x + [1]_4) \\ &\qquad = (2 \cdot 2)x^3 + (2 \cdot 3 + 1 \cdot 2)x^2 + (2 \cdot 1 + 1 \cdot 3)x + (1 \cdot 1) \\ &\qquad = x + 1. \end{aligned}$$

□

Exercise 1.2.4. *1. Compute* $(x+1)^3$ *in* $\mathbb{Z}_3[x]$.

2. *Suppose* p *is prime. Compute* $(x+1)^p$ *in* $\mathbb{Z}_p[x]$.

   (Hint. By the binomial expansion the coefficient of x^i in $(x+1)^p$ is $\binom{p}{i}$. Argue why $\binom{p}{i}$ is zero in $\mathbb{Z}_p$ if $1 \le i \le p-1$.)

Warning. Prior to this course, you have viewed a polynomial $f \in R[x]$ as a function from R to R. There is, however, a subtle difference between polynomials and functions. For instance, $x, x^2, \ldots$ are distinct elements of $\mathbb{Z}_2[x]$, but all of them are the same functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$. Notice that *two polynomials* $\sum_{i=0}^{\infty} a_i x^i$ *and* $\sum_{i=0}^{\infty} b_i x^i$ *are equal if and only if* $a_i = b_i$ *for every non-negative integer* i.

Nevertheless, later we will see that viewing polynomials as functions is extremely useful.

Direct product of rings

Suppose $R_1, \ldots, R_n$ are rings. Then the set

$$R_1 \times \cdots \times R_n := \{(r_1, \ldots, r_n) |\, r_1 \in R_1, \ldots, r_n \in R_n\}$$

with operations

$$\begin{aligned}(r_1, \ldots, r_n) + (r'_1, \ldots, r'_n) :=& (r_1 + r'_1, \ldots, r_n + r'_n)\\ (r_1, \ldots, r_n) \cdot (r'_1, \ldots, r'_n) :=& (r_1 \cdot r'_1, \ldots, r_n \cdot r'_n)\end{aligned}$$

is a ring, and it is called the *direct product* of R_i's. Notice the operations in the i-th component are done in R_i.

Example 1.2.5. *Compute* $(2,2) \cdot (3,3)$ *in* $\mathbb{Z}_5 \times \mathbb{Z}_6$.

Solution. We notice that $2 \cdot 3 = 1$ in $\mathbb{Z}_5$ and $2 \cdot 3 = 0$ in $\mathbb{Z}_6$. Hence we have $(2,2) \cdot (3,3) = (1,0)$ in $\mathbb{Z}_5 \times \mathbb{Z}_6$. □

1.3 Basic properties of operations in a ring.

Here we see that some basic computations hold in every ring, and a unital ring R has a unique identity, which is sometimes denoted by 1_R.

Lemma 1.3.1. *Suppose* R *is a ring and* 0 *is the neutral element of the abelian group* $(R, +)$. *Then for every* $a, b \in R$*, the following hold:*

1. $0 \cdot a = a \cdot 0 = 0$.

2. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$.

3. $(-a) \cdot (-b) = a \cdot b$.

Proof. (1) Since $0 = 0 + 0$, we have $0 \cdot a = (0 + 0) \cdot a$ for every $a \in R$. Hence by the distribution law, we have

$$0 \cdot a = (0 \cdot a) + (0 \cdot a).$$

As $(R, +)$ is a group, we deduce that $0 = 0 \cdot a$. Similarly we have

$$a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0), \text{ which implies that } 0 = a \cdot 0.$$

(2) To show $(-a) \cdot b = -(a \cdot b)$, we need to argue why $(a \cdot b) + ((-a) \cdot b) = 0 :$

$$\begin{aligned}(a \cdot b) + ((-a) \cdot b) =&(a + (-a)) \cdot b && \text{(distribution law)}\\ =&0 \cdot b\\ =&0 && \text{(by the first part).}\end{aligned}$$

By a similar argument, we can deduce that $a \cdot (-b) = -(a \cdot b)$.

(3) Using the second part twice, we obtain the last part as follows:

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

This finishes the proof. □

Lemma 1.3.2. *Suppose R is a unital ring. Then there is a unique element $1_R \in R$ such that*

$$1_R \cdot a = a \cdot 1_R = a \tag{1.1}$$

for every $a \in R$.

Proof. Suppose both 1 and $1'$ satisfy (1.1). Then

$$\begin{aligned}1 =&1 \cdot 1' && \text{(as } 1' \text{ satisfies (1.1))}\\ =&1' && \text{(as 1 satisfies (1.1)),}\end{aligned}$$

and the claim follows. □

Exercise 1.3.3. *Suppose $R_1, \dots, R_n$ are unital rings. Show that $(1_{R_1}, \dots, 1_{R_n})$ is the identity of $R_1 \times \cdots \times R_n$.*

1.4 Subring and homomorphism.

Whenever you learn a new structure, you should look for subsets that share the same properties (they are often called *sub-*), and more importantly *maps* that preserves those properties (they are often called *homomorphisms*).

Definition 1.4.1. *Suppose $(R, +, 0)$ is a ring. A subset S of R is called a* subring *of R if*

1. *$(S, +)$ is a subgroup of $(R, +)$.*
2. *S is closed under multiplication. This means that for every $a, b \in S$, we have $ab \in S$.*

Warning In your book, having an identity is part of the definition of a ring. As a result a subring of a ring R should contain the identity of R. In our course, we do not make that assumption for subrings.

Example 1.4.2. *$\mathbb{Z}$ is a subring of $\mathbb{Q}$. $\mathbb{Q}$ is a subring of $\mathbb{R}$. $\mathbb{R}$ is a subring of $\mathbb{C}$.*

Exercise 1.4.3.

1. *What is the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and i?*
2. *What is the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt{2}$?*
3. *What is the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt[3]{2}$?*

Definition 1.4.4. *Suppose R_1 and R_2 are two rings. Then a function $f : R_1 \to R_2$ is called a ring* homomorphism *if for every $a, b \in R_1$*

1. *$f(a+b) = f(a) + f(b)$,*
2. *$f(a \cdot b) = f(a) \cdot f(b)$.*

Warning As it has been mentioned earlier, in your book, having an identity is part of the definition of a ring. As a result a ring homomorphism between two rings A and B should send 1_A to 1_B. In this course, we refer to the ring homomorphisms that send 1_A to 1_B as *unital ring homomorphisms*.

Example 1.4.5. *For every positive integer n, $c_n : \mathbb{Z} \to \mathbb{Z}_n, c_n(a) := [a]_n$ is a ring homomorphism.*

Chapter 2

Lecture 2

In this lecture, first we show the subring criterion and present important ring homomorphisms. Next we define the kernel and the image of a ring homomorphism. The third topic is on the group of units of a ring, and the definition of a field. As an important example, we find the group of units of the ring of integers modulo n. Finally we define zero-divisors and integral domains.

2.1 More on subrings and ring homomorphisms.

We start by defining a ring isomorphism.

Lemma 2.1.1. *Suppose $f : R_1 \to R_2$ is a bijective ring homomorphism. Then $f^{-1} : R_2 \to R_1$ is a ring homomorphism.*

Proof. Since f is a bijection, it is invertible and there is the function $f^{-1} : R_2 \to R_1$. For every $a, b \in R_2$, we have

$$\begin{aligned} f(f^{-1}(a) + f^{-1}(b)) =& f(f^{-1}(a)) + f(f^{-1}(b)) \\ =& a + b. \end{aligned}$$

Hence $f^{-1}(a + b) = f^{-1}(a) + f^{-1}(b)$. Similarly we have

$$\begin{aligned} f(f^{-1}(a) \cdot f^{-1}(b)) =& f(f^{-1}(a)) \cdot f(f^{-1}(b)) \\ =& a \cdot b. \end{aligned}$$

Hence $f^{-1}(a \cdot b) = f^{-1}(a) \cdot f^{-1}(b)$. The claim follows. □

Definition 2.1.2. *A bijective ring homomorphism is called a ring* isomorphism. *We say two rings are* isomorphic *if there is a ring isomorphism between them.*

As in group theory, two isomorphic rings are essentially the same with different *labelling*!

Let us start with *subgroup criterion* from group theory.

Lemma 2.1.3 (Subgroup criterion)**.** *Suppose $(G, \cdot)$ is a group and H is a non-empty subset. If for every $h, h' \in H$, we have $hh'^{-1} \in H$, then H is a subgroup.*

We can use the subgroup criterion in order to show the *subring criterion*.

Lemma 2.1.4 (Subring criterion)**.** *Suppose R is a ring and S is a non-empty subset of R. If for every $a, b \in S$, we have*

1. *$a - b \in S$, and*
2. *$a \cdot b \in S$,*

then S is a subring.

Proof. By the subgroup criterion, we deduce that $(S, +)$ is a subgroup of $(R, +)$. Since S is also closed under multiplication, we deduce that S is a subring. □

2.2 Kernel and image of a ring homomorphism.

A good application of the subring criterion is to show that the kernel of a ring homomorphism and its image are subrings. Let us recall from group theory that the kernel of a group homomorphism f between two abelian groups A_1 and A_2 is

$$\ker f := \{a \in A_1 | \, f(a_1) = 0\},$$

and $\ker f$ is a subgroup of A_1. We also have that the image of f is

$$\operatorname{Im} f := \{f(a) | \, a \in A_1\},$$

and it is a subgroup of A_2. Since a ring homomorphism f is also an additive group homomorphism, we deduce that $\ker f$ and $\operatorname{Im} f$ are subgroups of the domain of f and the codomain of f, respectively.

Lemma 2.2.1. *Suppose $f : R_1 \to R_2$ is a ring homomorphism. Then the kernel $\ker f$ of f is a subring of R_1 and the image $\operatorname{Im} f$ of is a subring of R_2. Moreover for every $a \in A$ and $x \in \ker f$, we have that ax and xa are in $\ker f$.*

Remark 2.2.2. *Notice that the* moreover *part of Lemma 2.2.1 is much stronger than saying* $\ker f$ *is closed under under multiplication. Later, when we are studying* ideals *we will come back to this extra property of kernels.*

Proof of Lemma 2.2.1. From group theory, we know that $\ker f$ and $\operatorname{Im} f$ are additive subgroups. It is enough to show that they are closed under multiplication. We show a stronger result for $\ker f$, and we will come back to this property when we define an ideal of a ring. For every $a \in \ker f$ and every $a' \in R_1$, we have

$$f(a \cdot a') = f(a) \cdot f(a') = 0 \cdot f(a') = 0, \text{ and so } a \cdot a' \in \ker f.$$

For every $b, b' \in \operatorname{Im} f$, there are $a, a' \in R_1$ such that $b = f(a)$ and $b' = f(a')$. Therefore

$$b \cdot b' = f(a) \cdot f(a') = f(a \cdot a') \in \operatorname{Im} f.$$

This completes the proof. □

Example 2.2.3. *Find the kernel of* $c_n : \mathbb{Z} \to \mathbb{Z}_n, c_n(a) := [a]_n$.

Solution. You have seen this in group theory: $a \in \ker c_n$ if and only if $c_n(a) = 0$. This means $a \in \ker c_n$ if and only if $[a]_n = [0]_n$. Hence $a \in \ker f$ if and only if a is a multiple of n. Therefore $\ker c_n = n\mathbb{Z}$. □

Example 2.2.4. *Notice that* $c_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x], c_n(\sum_{i=0}^{\infty} a_i x^i) := \sum_{i=0}^{\infty} c_n(a_i) x^i$ *is a ring homomorphism. Find the kernel of* c_n.

Proof. Before we describe the kernel of c_n, let us point out that every ring homomorphism $f : A \to B$ can be extended to a ring homomorphism, which by the abuse of notation is also denoted by f, between $A[x]$ and $B[x]$: $f : A[x] \to B[x]$ such that $f(\sum_{i=0}^{\infty} a_i x^i) := \sum_{i=0}^{\infty} f(a_i) x^i$ (Justify for yourself why this is the case).

Now notice that $\sum_{i=0}^{\infty}$ is in the kernel of c_n if and only if for every i, a_i is in the kernel of c_n. Hence $\ker c_n = n\mathbb{Z}[x]$, which means it consists of polynomials that are multiple of n. □

2.3 A special ring homomorphism

Let's recall a notation from group theory before going back to ring theory. In group theory, you have learned that if $(G, \cdot)$ is a group and $g \in G$, then the cyclic group generated by g is

$$\{g^n |\ n \in \mathbb{Z}\},$$

and

$$e_g : \mathbb{Z} \to G, e_g(n) := g^n \tag{2.1}$$

is a group homomorphism. You have also learned that when we have an *abelian group* A, we often use the *additive* notation. The cyclic (additive) subgroup generated by $a \in A$ is

$$\{na |\ a \in \mathbb{Z}\},$$

where na is defined as follows: for a positive integer n we set

$$na := \underbrace{a + \cdots + a}_{n\text{-times}},$$

for a negative integer n, we set

$$na := \underbrace{(-a) + \cdots + (-a)}_{(-n)\text{-times}},$$

and for $n = 0$, $na = 0$. In the additive setting the group homomorphism e_g which is given in (2.1) is as follows:

$$e_a : \mathbb{Z} \to A, e_a(n) := na. \tag{2.2}$$

Since a ring $(R, +, \cdot)$ with addition $+$ is an abelian group, we can use the same notation as in group theory. This means for $n \in \mathbb{Z}$ and $a \in R$, we can talk about $na \in R$.

Warning. For a ring R, an integer n, and $a \in R$, na should not be confused with a ring multiplication $n \cdot a$. As it is explained above, this concept is borrowed from group theory. Notice that the ring multiplication is only defined for two elements of R, and it is not defined for an integer and an element of R.

Lemma 2.3.1. *Suppose R is a unital ring with the identity element 1_R. Then*

$$e : \mathbb{Z} \to R, \quad e(n) := n1_R$$

is a ring homomorphism.

Proof. From group theory, we know that e is an abelian group homomorphism. So it is enough to show that for every integers m and n we have $e(mn) = e(m) \cdot e(n)$. This is done by a case-by-case consideration, and is not particularly interesting!

Case 1. $m = 0$ or $n = 0$.

Proof of Case 1. By definition, $e(0) = 0$ (the first 0 is in $\mathbb{Z}$ and the second 0 is in R). By basics properties of ring operations (see Lemma 1.3.1), we have that $0 \cdot a = a \cdot 0 = 0$ for every $a \in R$. Therefore for $m = 0$, we have

$$e(mn) = e(0) = 0, \text{ and } e(m) \cdot e(n) = e(0) \cdot e(n) = 0 \cdot e(n) = 0,$$

and similarly for $n = 0$, we have

$$e(mn) = e(0) = 0, \text{ and } e(m) \cdot e(n) = e(m) \cdot e(0) = e(m) \cdot 0 = 0,$$

and the claim follows.

Case 2. $m, n > 0$.

Proof of Case 2. By definition, $e(mn) = 1_R + \cdots + 1_R$ where there are mn-many 1_Rs. On the other hand,

$$\begin{aligned} e(m) \cdot e(n) =& (\underbrace{1_R + \cdots + 1_R}_{m\text{-times}}) \cdot (\underbrace{1_R + \cdots + 1_R}_{n\text{-times}}) \\ =& \underbrace{1_R \cdot 1_R + \cdots + 1_R \cdot 1_R}_{mn\text{-times}} && \text{(by the distribution law)} \\ =& \underbrace{1_R + \cdots + 1_R}_{mn\text{-times}} \\ =& e(mn). \end{aligned}$$

This shows the claim in Case 2.

Case 3. $m > 0$ and $n < 0$.

Proof of Case 3. Since m is positive and n is negative, mn is negative. Hence $e(mn) = (-1_R) + \cdots + (-1_R)$ where there are $(-mn)$-many -1_Rs. On the other hand,

$$\begin{aligned}
e(m)\cdot e(n) =& \underbrace{(1_R+\cdots+1_R)}_{m\text{-times}}\cdot\underbrace{((-1_R)+\cdots+(-1_R))}_{(-n)\text{-times}}\\
=& \underbrace{1_R\cdot(-1_R)+\cdots+1_R\cdot(-1_R)}_{(-mn)\text{-times}} && \text{(by the distribution law)}\\
=& \underbrace{-(1_R\cdot 1_R)+\cdots+-(1_R\cdot 1_R)}_{(-mn)\text{-times}} && \text{(Lemma 1.3.1)}\\
=& \underbrace{(-1_R)+\cdots+(-1_R)}_{(-mn)\text{-times}}\\
=& e(mn).
\end{aligned}$$

This shows the claim in Case 3.

Case 4. $m < 0$ and $n > 0$.

This case is almost identical to Case 3.

Case 5. $m < 0$ and $n < 0$.

We leave this case as an **exercise**. □

2.4 The evaluation or the substitution map

As it has been already hinted to, polynomials can be viewed as functions. This means we can *evaluate* a polynomial. Next we make it more formal.

Proposition 2.4.1. *Suppose B is a commutative ring and A is a subring of B. Suppose $b \in B$. Then the* evaluation map

$$\phi_b : A[x] \to B, \quad \phi_b(f(x)) := f(b)$$

is a ring homomorphism.

Proof. We need to show that for every $f_1, f_2 \in A[x]$ we have

$$\begin{aligned}
\phi_b(f_1(x)+f_2(x)) =& \phi_b(f_1(x))+\phi_b(f_2(x)) && \text{and}\\
\phi_b(f_1(x)f_2(x)) =& \phi_b(f_1(x))\phi_b(f_2(x)).
\end{aligned}$$

Both are easy to be checked and we leave it as an exercise. □

Let's describe the image and the kernel of ϕ_b.

By the definition of kernel, the kernel of the evaluation map $\phi_b : A[x] \to B$ consists of polynomials that have b as a zero:

$$\ker \phi_b = \{p(x) \in A[x] |\ p(b) = 0\}.$$

This is an indication of how ring theory can help us to study zeros of polynomials.

The image of ϕ_b is

$$\operatorname{Im}\phi_b = \{p(b)|\ p(x) \in A[x]\} = \Big\{\sum_{i=0}^{n} a_i b^i \mid n \in \mathbb{Z}^+, a_0, \ldots, a_n \in A\Big\}.$$

In the next lecture we will show that the image of ϕ_b is the smallest subring of B that contains both A and b.

Chapter 3

Lecture 3

3.1 The evaluation or the substitution map

In the previous lecture we defined the evaluation map

$$\phi_b : A[x] \to B, \quad \phi_b(f(x)) := f(b)$$

where A is a subring of B and $b \in B$. We observed that

$$\ker \phi_b = \{p(x) \in A[x] \mid p(b) = 0\}.$$

Next we describe the image of ϕ_b.

Lemma 3.1.1. *Suppose A is a subring of a unital commutative ring B, and $b \in B$. Then the image of the evaluation map ϕ_b is the smallest subring of B that contains both A and b.*

Proof. Since ϕ_b is a ring homomorphism, its image is a subring. For every $a \in A$, $\phi_b(a) = a$, where a is viewed as the constant polynomial, and $\phi_b(x) = b$. Hence $\operatorname{Im} \phi_b$ is a subring of B which contains A and b.

Suppose C is a subring of B which contains A and b. Then for every $a_0, \ldots, a_n \in A$, we have

$$a_0 + a_1 b + \cdots + a_n b^n \in C$$

as C is closed under addition and multiplication. This implies that $\operatorname{Im} \phi_b$ is a subset of C. The claim follows. □

Definition 3.1.2. *Suppose A is a subring of a unital commutative ring B, and $b \in B$. The smallest subring of B which contains A and b is denoted by $A[b]$.*

Warning. The notation $A[b]$ can be confusing because of its similarity with the ring of polynomials $A[x]$. You have to notice that $b \in B$ is not an indeterminant.

By Lemma 3.1.1, we have that $\operatorname{Im} \phi_b = A[b]$.

Exercise 3.1.3. *Earlier you have seen that the image $\mathbb{Q}[i]$ of $\phi_i : \mathbb{Q}[x] \to \mathbb{C}$ and the image $\mathbb{Q}[\sqrt{2}]$ of $\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C}$ are given only using polynomials of degree at most 1. You have also observed that to get the entire $\mathbb{Q}[\sqrt[3]{2}]$, one can only use polynomials of degree at most 3. What do you think is the general rule?*

3.2 Units and fields

As it has been pointed out earlier, Khwarizmi was interested in solving degree 1 equations. Now we try to do same in a ring: suppose R is a ring and $a, b \in R$. Does the equation $ax = b$ have a solution in R? Over real numbers, such an equation has a solution as long as $a \neq 0$. In fact, if $a \neq 0$, then $x = a^{-1}b$ is the unique solution of $ax = b$. So the question is whether or not a has a multiplicative inverse.

Definition 3.2.1. *Suppose R is a unital ring. We say $a \in R$ is a* unit *if there is $a' \in R$ such that $a \cdot a' = a' \cdot a = 1_R$. The set of all units of R is denoted by $R^\times$.*

Lemma 3.2.2. *Suppose R is a unital commutative ring and $a \in R$ is a unit. Then there is a unique $a' \in R$ such that $a \cdot a' = 1_R$. (We call such an a' the* multiplicative inverse *(or simply the* inverse*) of a. The multiplicative inverse of a is denoted by a^{-1}.)*

Proof. Suppose $a \cdot a' = a \cdot a'' = 1_R$. We have to show that $a' = a''$. We have

$$\begin{aligned} a' =& a' \cdot 1_R = a' \cdot (a \cdot a'') \\ =& (a' \cdot a) \cdot a'' && \text{(by the associativity)} \\ =& (a \cdot a') \cdot a'' && \text{(by the commutativity)} \\ =& 1_R \cdot a'' = a''. \end{aligned}$$

□

Lemma 3.2.3. *Suppose R is a unital ring. Then $(R^\times, \cdot)$ is a group.*

Proof. We start by showing that $R^\times$ is closed under multiplication. Suppose $a, b \in R^\times$; then

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = 1_R. \qquad \text{(justify this!)}$$

Hence $a \cdot b \in R^\times$.

Next we show that $(R^\times, \cdot)$ has an identity. Notice since $1_R \cdot 1_R = 1_R$, $1_R \in R^\times$. As $1_R \cdot a = a \cdot 1_R = a$ for every $a \in R^\times$, we deduce that 1_R is the identity of $R^\times$.

Observe that we have the associativity of $\cdot$ for free as R is a ring.

Finally we show that every element of $R^\times$ has an inverse. Suppose $a \in R^\times$. Then $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$. This implies that $a^{-1} \in R^\times$, which completes the proof. □

Example 3.2.4. $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, *and* $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

Example 3.2.5. *Find* $\mathbb{Z}^\times$.

Proof. By the definition, $a \in \mathbb{Z}^\times$ if and only if $aa' = 1$ for some $a' \in \mathbb{Z}$. If $aa' = 1$, then $|a||a'| = 1$ and $|a|$ and $|a'|$ are two positive *integers*. Hence $|a|, |a'| \geq 1$ and $|a||a'| = 1$. This implies that $|a| = |a'| = 1$. Therefore $a = \pm 1$. As $(-1)(-1) = 1$ and $(1)(1) = 1$, we deduce that $\mathbb{Z}^\times = \{1, -1\}$. □

Example 3.2.6. *Find* 2^{-1} *in* $\mathbb{Z}_3$.

Proof. Notice that $[2]_3 \cdot [2]_3 = [1]_3$, and so $2^{-1} = 2$ in $\mathbb{Z}_3$. □

Warning. When we know that we are working with elements of $\mathbb{Z}_n$, we often write a instead of $[a]_n$. When we are asked to find the inverse of an apparently integer number a in $\mathbb{Z}_n$, we should not write $\frac{1}{a}$. We should find an integer a' such that

$$aa' \equiv 1 \pmod{n}.$$

Exercise 3.2.7. *Review your notes from either math 109 or math 100 a where the following property of the greatest common divisor of two integers is discussed. Suppose a and b are two non-zero integers. Then*

the equation $ax + by = c$ has an integer solution if and only if $\gcd(a, b)$ *divides c.*

This fact can be written in a compact form as $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$. (See proposition 2.3.5 of your book.)

Using the above exercise, we can describe the group $\mathbb{Z}_n^\times$ of units of $\mathbb{Z}_n$.

Proposition 3.2.8. *Suppose n is a positive integer. Then*

$$\mathbb{Z}_n^\times = \{[a]_n | \ \gcd(a, n) = 1\}.$$

Proof. Notice that $[a]_n$ is a unit in $\mathbb{Z}_n$ if and only if for some $[x]_n \in \mathbb{Z}_n$ we have $[a]_n[x]_n = [1]_n$. This means the congruence equation $ax \equiv 1 \pmod{n}$ has a solution. This in turn means for some integers x and y we have $ax - 1 = ny$. So we are looking for as such that the following equation has an integer solution:

$$ax - ny = 1.$$

By the above exercise, this happens exactly when $\gcd(a, n) = 1$. The claim follows. □

Euler's phi function $\phi(n)$ is

$$|\{a \in \mathbb{Z} \mid 1 \le a \le n, \gcd(a, n) = 1\}|.$$

Hence by Proposition 3.2.8, we have that

$$|\mathbb{Z}_n^\times| = \phi(n).$$

As a corollary of this equation, we can deduce Euler's theorem.

Theorem 3.2.9 (Euler's theorem)**.** *Suppose n is a positive integer, and* $\gcd(a, n) = 1$. *Then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. In group theory, you have learned that if $(G, \cdot)$ is a finite group, then for every $g \in G$ we have

$$g^{|G|} = 1.$$

We apply this result for the group $\mathbb{Z}_n^\times$. When $\gcd(a,n)=1$, $[a]_n \in \mathbb{Z}_n^\times$. Therefore by the above discussion we have

$$[a]_n^{|\mathbb{Z}_n^\times|} = [a]_n^{\phi(n)} = [1]_n.$$

Hence

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

□

Definition 3.2.10. *A unital commutative ring F is called a* field *if $F^\times = F \setminus \{0\}$.*

Example 3.2.11. *$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields, and $\mathbb{Z}$ is not a field.*

Corollary 3.2.12. *Suppose n is a positive integer. Then $\mathbb{Z}_n$ is a field if and only if n is prime.*

Proof. By Proposition 3.2.8, we have that $\mathbb{Z}_n$ is a field if and only if

$$\mathbb{Z}_n \setminus \{[0]_n\} = \{[a]_n |\ \gcd(a,n)=1\}.$$

This means $1 < n$ and every positive integer less than n is coprime with n. The claim follows. □

3.3 Zero-divisors and integral domains

Let's go back to a special case of linear equations: $ax=0$. We know that over $\mathbb{C}$, 0 is the unique solution of this equation if $a \neq 0$. On the other hand, in $\mathbb{Z}_6$, we have $[2]_6[3]_6 = [0]_6$, which means $2x=0$ has a non-zero solution in $\mathbb{Z}_6$. This brings us to the following definition.

Definition 3.3.1. *Suppose R is a commutative ring. We say $a \in R$ is a* zero-divisor *if $a \neq 0$ and $ab=0$ for some non-zero $b \in R$. The set of zero divisors of R is denoted by $D(R)$.*

Definition 3.3.2. *A unital commutative ring D is called an* integral domain *if D has more than one element (alternatively we can say $0_D \neq 1_D$ (why?)) and D has no zero-divisors.*

Example 3.3.3. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are integral domains, and $\mathbb{Z}_6$ is not an integral domain.*

Lemma 3.3.4. *Suppose R is a unital commutative ring. Then $R^\times \cap D(R) = \varnothing$.*

Proof. Suppose to the contrary that $a \in R^\times \cap D(R)$. Then for some $a' \in R \setminus \{0\}$ we have $a \cdot a' = 0$. Then

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

On the other hand, we have

$$a^{-1} \cdot (a \cdot a') = (a^{-1} \cdot a) \cdot a' = 1_R \cdot a' = a'.$$

Hence $a'=0$, which is a contradiction. □

Corollary 3.3.5. *Every field F is an integral domain.*

Proof. Since F is a field, $1_F \in F^\times = F \setminus \{0_F\}$. Hence $1_F \neq 0_F$. Next we want to show that F has no zero-divisors; that means we want to show $D(F) = \varnothing$. By Lemma 3.3.4, we have that $D(F) \cap F^\times = \varnothing$. Since F is a field, $F^\times = F \setminus \{0\}$. Altogether we deduce that $D(F) = \varnothing$, and the claim follows. □

Notice that the converse of Corollary 3.3.5 is not correct; for instance $\mathbb{Z}$ is an integral domain, but it is not a field. The converse statement, however, holds for finite integral domains. Before proving this result, let's show the *cancellation law* for integral domains.

Lemma 3.3.6 (Cancellation law)**.** *Suppose D is an integral domain. Then for every non-zero $a \in D$ and $b, c \in D$,*

$$ab = ac \quad \textit{implies} \quad b = c.$$

Proof. Since $ab = ac$, we have $a(b - c) = 0$. Since $a \neq 0$ and D does not have a zero-divisor, we deduce that $b - c = 0$, which means $b = c$. This completes the proof. □

Proposition 3.3.7. *Suppose D is a finite integral domain. Then D is a field.*

Proof. Since D is an integral domain, it is a unital commutative ring and $0_D \neq 1_D$. So it is enough to show that every non-zero element $a \in D$ is a unit. This means we have to show that for some $x \in D$ we have $ax = 1$. Let $\ell_a : D \to D, \ell_a(x) := ax$. With this choice of ℓ_a, it is enough to show that 1 is in the image of ℓ_a. We will show that ℓ_a is surjective. Notice that since D is a finite set, $\ell_a : D \to D$ is surjective if and only if it is injective. Therefore it is enough to prove that ℓ_a is injective. Notice that

$$\begin{aligned} \ell_a(b) = \ell_a(c) \Rightarrow & ab = ac && \text{(By the cancellation law)} \\ \Rightarrow & b = c. \end{aligned}$$

Therefore ℓ_a is injective which finishes the proof. □

3.4 Characteristic of a unital ring

Definition 3.4.1. *Suppose R is a ring. Let*

$$N^+(R) := \{n \in \mathbb{Z}^+ \,|\, \textit{for every } a \in R, na = 0\}. \tag{3.1}$$

If $N^+(R)$ is empty, we say that the characteristic *of R is* zero*. If $N^+(R)$ is not empty, the* characteristic *of R is the minimum of $N^+(R)$. The characteristic of R is denoted by* $\operatorname{char}(R)$.

Notice that for every ring R we have that $\operatorname{char}(R)a = 0$ for every $a \in R$.

Let us recall that by Lemma 2.3.1 we have that

$$e : \mathbb{Z} \to R, e(n) := n1_R$$

is a ring homomorphism. The next lemma gives us a clear connection between the ring homomorphism e and the characteristic of R.

Lemma 3.4.2. *Let R be a unital ring and $e : \mathbb{Z} \to R, e(n) := n1_R$. For every unital ring R, we have* $\ker e = \mathrm{char}(R)\mathbb{Z}$.

Proof. From group theory, we know that every subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for some non-negative integer m. Since $\ker e$ is a subgroup of $\mathbb{Z}$, for some non-negative integer n_0 we have that $\ker e = n_0\mathbb{Z}$.

If $n_0 = 0$, then there is no positive integer n such that $n1_R = 0$. Hence $N^+(R)$ is empty where $N^+(R)$ is as in (3.1). Therefore $\mathrm{char}(R) = 0$. Thus in this case we have $\ker e = \mathrm{char}(R)\mathbb{Z}$.

Now suppose $n_0 \neq 0$. For every $n \in N^+(R)$, we have $n1_R = 0$ which implies that n is in $\ker e = n_0\mathbb{Z}$. Therefore

$$n \geq n_0 \qquad \text{if} \qquad n \in N^+(R). \tag{3.2}$$

On the other hand, for every $a \in R$, we have

$$\begin{aligned} n_0 a =& \underbrace{a + \cdots + a}_{n_0\text{-times}} \\ =& \underbrace{(1_R \cdot a) + \cdots + (1_R \cdot a)}_{n_0\text{-times}} \\ =& (\underbrace{1_R + \cdots + 1_R}_{n_0\text{-times}}) \cdot a = (n_0 1_R) \cdot a \qquad \text{(distribution)} \\ =& 0 \cdot a = 0 \end{aligned} \tag{3.3}$$

By (3.3), we deduce that

$$n_0 \in N(R). \tag{3.4}$$

By (3.2) and (3.4), we deduce that $n_0 = \min N^+(R) = \mathrm{char}(R)$, and the claim follows. □

Proposition 3.4.3. *Suppose D is an integral domain. Then $\mathrm{char}(D)$ is either 0 or a prime number.*

Proof. Suppose to the contrary that $\mathrm{char}(D)$ is neither 0 nor prime. Then either $\mathrm{char}(D)$ is either 1 or of the form ab where a and b are two integers more than 1.

If $\mathrm{char}(D) = 1$, then $1_D = 0_D$ which is a contradiction as D is an integral domain.

If $\mathrm{char}(D) = ab$ and a, b are integers more than 1, then by Lemma 3.4.2 we have $\ker e = ab\mathbb{Z}$. Hence $e(ab) = 0$, which implies that

$$e(a) \cdot e(b) = 0. \tag{3.5}$$

As D is an integral domain, by (3.5) we deduce that either $e(a) = 0$ or $e(b) = 0$. Hence either $a \in \ker e$ or $b \in \ker e$. Since $\ker e = ab\mathbb{Z}$ and a and b are integers more than 1, we get a contradiction. □

Chapter 4

Lecture 4

4.1 Defining fractions

In the previous lecture, we showed that *every field is an integral domain*, and we noticed that the converse does not hold in general: for instance $\mathbb{Z}$ is an integral domain but it is not a field. Today we will show every integral domain can be embedded into a field. Let's discuss this from the point of view of solving equations. Notice that in a field every linear equation of the form $ax = b$ has a (unique) solution if a is not zero. This property does not hold in an arbitrary integral domain. Let's say we start with an integral domain D and "add" all the zeros of the equations of the form $bx = a$ with $b \neq 0$ to D. What do we get? Let's look at the ring of integers $\mathbb{Z}$. In this case, we get $\{\frac{a}{b} | \, a, \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\}$, which is the field $\mathbb{Q}$ of rational numbers. We use our understanding of rational numbers as our guide to create fractions for an arbitrary integral integral domain D. Every fraction is of the form $\frac{a}{b}$; so it is given by a pair of elements the *numerator* a and the *denominator* b. The numerator is arbitrary and the denominator is every *non-zero* element. The subtlety is that two different pairs might give us the same fractions. In the field of rational numbers we know that $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$. We use this to *identify* two different pairs together. Formally, we define a relation between the pairs, show that this is an equivalence relation, and use the corresponding equivalence relations to define fractions.

Suppose D is an integral domain. For (a, b) and (c, d) in $D \times (D \setminus \{0\})$, we say $(a, b) \sim (c, d)$ if $ad = bc$. Next we check that $\sim$ is an equivalence relation. Recall that a relation is an equivalence relation if it is *reflexive* (every element is "equal" to itself!), *symmetric* (if x is "equal" to y, then y is "equal" to x), and *transitive* (if x is "equal" to y and y is "equal" to z, then x is "equal" to z). This means we have to check the following:

1. *For every* $(a, b) \in D \times (D \setminus \{0\})$*, we have* $(a, b) \sim (a, b)$. This holds as $ab = ba$.

2. *For every* $(a, b), (c, d) \in D \times (D \setminus \{0\})$*, if* $(a, b) \sim (c, d)$*, then* $(c, d) \sim (a, b)$. This holds as $ad = bc$ implies that $cb = da$.

3. *For every* $(a, b), (c, d), (e, f) \in D \times (D \setminus \{0\})$*, if* $(a, b) \sim (c, d)$ *and* $(c, d) \sim (e, f)$*, then* $(a, b) \sim (e, f)$. The proof of this part is a bit more involved. Since

$(a,b) \sim (c,d)$, we have $ad = bc$, and $(c,d) \sim (e,f)$ implies that $cf = de$. Multiplying both sides of $ad = bc$ by f, and multiplying both sides of $cf = de$ by b, we obtain the following

$$adf = bcf, \text{ and } cfb = deb.$$

Hence $adf = deb$. As $d \neq 0$ and D is an integral domain, by the cancellation law, we have $af = eb$. Therefore

$$(a,b) \sim (e,f).$$

Notice that in the last item, we used the condition that D is an integral domain in a crucial way.

We let $\frac{a}{b}$ be the the *equivalence class* $[(a,b)]$, and let

$$Q(D) := \left\{ \frac{a}{b} \;\middle|\; (a,b) \in D \times (D \setminus \{0\}) \right\}.$$

4.2 Defining addition and multiplication of fractions

Next we will make define two binary operations on $Q(D)$. Again we imitate rational numbers, and we define

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

Whenever we are working with equivalence classes, we have to be extra careful. We need to check whether or not our definitions are independent of the choice of a representative from equivalence classes.

Let's make it more concrete by working with fractions. We are defining addition and multiplication of fractions in terms of their given numerator and denominator. A priori, it is not clear, why we end up getting the same result if we represent the same fractions with different numerators and denominators. That means we have to show that $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ and $\frac{c_1}{d_1} = \frac{c_2}{d_2}$ imply that

$$\frac{a_1d_1 + b_1c_1}{b_1d_1} = \frac{a_2d_2 + b_2c_2}{b_2d_2} \quad \text{and} \quad \frac{a_1c_1}{b_1d_1} = \frac{a_2c_2}{b_2d_2}.$$

We only discuss why the addition is well-defined. The well-definedness of the multiplication is much easier.

We have that $\frac{a_1d_1+b_1c_1}{b_1d_1} = \frac{a_2d_2+b_2c_2}{b_2d_2}$ if and only if

$$(a_1d_1 + b_1c_1)(b_2d_2) = (a_2d_2 + b_2c_2)(b_1d_1) \quad \Leftrightarrow \tag{4.1}$$

$$(a_1b_2)(d_1d_2) + (c_1d_2)(b_1b_2) = (a_2b_1)(d_1d_2) + (c_2d_1)(b_1b_2).$$

The second equality in (4.1) holds as we have $a_1b_2 = a_2b_1$ and $c_2d_1 = c_1d_2$ because of $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ and $\frac{c_1}{d_1} = \frac{c_2}{d_2}$.

4.3 Fractions form a field

I leave it to you to check that $(Q(D), +, \cdot)$ is a ring. Next we show that $Q(D)$ is a field by checking that every non-zero element of $Q(D)$ is a multiplicative inverse. Before showing this, let us show that $\frac{0}{1}$ is the zero of $Q(D)$ and $\frac{1}{1}$ is the identity of $Q(D)$: for every $\frac{a}{b} \in Q(D)$ we have

$$\frac{0}{1} + \frac{a}{b} = \frac{0 \cdot b + 1 \cdot a}{1 \cdot b} = \frac{a}{b}, \quad \text{and} \quad \frac{1}{1} \cdot \frac{a}{b} = \frac{1 \cdot a}{1 \cdot b} = \frac{a}{b}.$$

We also notice that for every non-zero a in D, we have

$$\frac{0}{1} = \frac{0}{a}, \quad \text{and} \quad \frac{1}{1} = \frac{a}{a}.$$

The first one holds as $0 \cdot a = 0 \cdot 1$ and the second one holds as $1 \cdot a = a \cdot 1$.

Suppose $\frac{a}{b}$ is not zero. Then $a \neq 0$. Hence $\frac{b}{a}$ is an element of $Q(D)$. We have that

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

which means that $\frac{a}{b}$ is a unit in $Q(D)$. Therefore $Q(D)$ is a field.

4.4 The universal property of the field of fractions

In this section, we show that $Q(D)$ is *the smallest* field that contains a copy of D. We have formulate this carefully. First we start by showing that $Q(D)$ has a *copy* of D; this means there is an injective ring homomorphism from D to $Q(D)$. This will be done similar to the way we view integers as fractions with denominator 1.

Lemma 4.4.1. *Suppose D is an integral domain. Let $i : D \to Q(D)$, $i(a) := \frac{a}{1}$. Then i is an injective ring homomorphism.*

Remark 4.4.2. *Suppose A and B are rings. We say A can be* embedded *in B or we say B has a* copy *of A if there is an injective ring homomorphism from A to B.*

Proof of Lemma 4.4.1. We have to show that $i(a) + i(b) = i(a+b)$ and $i(a) \cdot i(b) = i(a \cdot b)$ for every $a, b \in D$:

$$i(a) + i(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} = \frac{a+b}{1} = i(a+b),$$

and

$$i(a) \cdot i(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{a \cdot b}{1 \cdot 1} = i(a \cdot b).$$

Next we show that i is injective:

$$i(a) = i(b) \ \Rightarrow \frac{a}{1} = \frac{b}{1} \ \Rightarrow a \cdot 1 = 1 \cdot b \Rightarrow a = b.$$

□

Next we show that if F is a field which contains a copy of D, then F contains a copy of $Q(D)$. In this sense, $Q(D)$ is the smallest field which contains a copy of D.

Theorem 4.4.3. *Suppose D is an integral domain and F is a field. Suppose $f : D \to F$ is an injective ring homomorphism. Then*

$$\widetilde{f} : Q(D) \to F, \quad \widetilde{f}\Big(\frac{a}{b}\Big) := f(a)f(b)^{-1}$$

is a well-defined injective ring homomorphism. Moreover the following is a commuting diagram

$$\begin{tikzcd} D \arrow[r, "i"] \arrow[dr, "f"'] & Q(D) \arrow[d, "\widetilde{f}"] \\ & F \end{tikzcd}$$

that means we have $\widetilde{f} \circ i = f$.

Proof. We start by showing that $\widetilde{f}$ is well-defined. Suppose $\frac{a_1}{b_1} = \frac{a_2}{b_2}$. Then $a_1b_2 = a_2b_1$ which implies that $f(a_1b_2) = f(a_2b_1)$. Since f is a ring homomorphism, we have

$$f(a_1)f(b_2) = f(a_2)f(b_1). \tag{4.2}$$

As f is injective and b_i's are not zero, we deduce that $f(b_i)$'s are not zero. As F is a field, $f(b_i)$'s are units in F. Therefore by (4.2), we have $f(a_1)f(b_1)^{-1} = f(a_2)f(b_2)^{-1}$. This implies that $\widetilde{f}$ is well-defined.

I leave it to you to check that $\widetilde{f}$ is a ring homomorphism. Next we show that $\widetilde{f}$ is injective. Let us recall an important result from group theory:

A group homomorphism is injective if and only if its kernel is trivial.

Based on the above mentioned result, to show that $\widetilde{f}$ is injective, it is enough to prove that the kernel of $\widetilde{f}$ is trivial:

$$0 = \widetilde{f}\Big(\frac{a}{b}\Big) = f(a)f(b)^{-1} \quad \Rightarrow \quad f(a) = 0 \quad \Rightarrow a = 0$$

where the last implication holds because f is injective.

Finally we prove that the given diagram is commutative. This means we have to show for every $a \in D$, we have $\widetilde{f}(i(a)) = f(a)$. By the definition of $\widetilde{f}$, we have to show $f(a)f(1)^{-1} = f(a)$. Hence we need to show that $f(1) = 1$. Notice that $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$. Since f is injective, $f(1) \neq 0$. As F is a field, $f(1)$ is a unit. Therefore $f(1) = f(1) \cdot f(1)$ implies that $f(1) = 1$, which finishes the proof. □

How can we use the *Universal Property of Field of Fractions*?

The universal property can be used to show that $Q(D)$ is isomorphic to a given ring F. We can use the following strategy to show $Q(D) \simeq F$:

1. Prove that F is a field.

2. Find an injective ring homomorphism $f : D \to F$.
3. Use the universal property of field of fractions to get the injective ring homomorphism
$$\widetilde{f} : Q(D) \to F, \quad \widetilde{f}\left(\frac{a}{b}\right) = f(a)f(b)^{-1}.$$
4. Show that every element of F is of the form $f(a)f(b)^{-1}$ for some $a, b \in D$.

The last step implies that $\widetilde{f}$ is surjective. By the third item, we know that $\widetilde{f}$ is injective. Hence $\widetilde{f}$ is a bijective ring homomorphism. This implies that $Q(D) \simeq F$.

In the next lecture, we use this strategy to show that $Q(\mathbb{Z}[i]) \simeq \mathbb{Q}[i]$.

Chapter 5

Lecture 5

5.1 Using the universal property of the field of fractions.

In the previous lecture we defined the field of fractions of an integral domain and proved its universal property. We also discussed a four step strategy of proving that the field of fractions of an integral domain is isomorphic to a given ring.

Example 5.1.1. *Prove that* $Q(\mathbb{Z}[i]) \simeq \mathbb{Q}[i]$.

Solution. **Step 1.** $\mathbb{Q}[i]$ *is a field.*

We have already seen how to show $\mathbb{Q}[i]$ is a subring of $\mathbb{C}$. So to show it is a field, it is enough to prove that every non-zero element of $\mathbb{Q}[i]$ is a unit. Let $a + bi \in \mathbb{Q}[i]$ be a non-zero element. Then we have

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Since $a, b \in \mathbb{Q}$, we have $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \mathbb{Q}$. Hence $(a+bi)^{-1} \in \mathbb{Q}[i]$. Notice that $a+bi \neq 0$, $a-bi \neq 0$ and we are allowed to multiply the numerator and the denominator by $a - bi$.

Step 2. $f : \mathbb{Z}[i] \to \mathbb{Q}[i], f(z) := z$.

Then clearly f is an injective ring homomorphism.

Step 3. By the Universal Property of Field of Fractions,

$$\widetilde{f} : Q(\mathbb{Z}[i]) \to \mathbb{Q}[i], \quad \widetilde{f}\Big(\frac{z_1}{z_2}\Big) = f(z_1)f(z_2)^{-1}$$

is a well-defined injective ring homomorphism.

Step 4. $\widetilde{f}$ is surjective.

Suppose $a + bi \in \mathbb{Q}[i]$. Then by taking a common denominator for a and b we have that there are integers r, s and t such that

$$a + bi = \frac{r+si}{t} = f(r+si)f(t)^{-1}.$$

Therefore $\widetilde{f}$ is surjective.

By Steps 3 and 4, we have that $\widetilde{f}$ is an isomorphism. □

5.2 Ideals

In group theory (and linear algebra), you have seen the importance of kernel of homomorphisms. Next we find out exactly what subsets of a ring A can be the kernel of a ring homomorphism from A to another ring. We have already proved that if $f : A \to B$ is a ring homomorphism, then the kernel of f have the following properties:

1. For every $x, y \in \ker f$, $x - y \in \ker f$, and
2. For every $x \in \ker f$ and $a \in A$, then $ax \in \ker f$ and $xa \in \ker f$.

We will show that these conditions are enough to be the kernel of a ring homomorphism. This brings us to the definition of *ideals*.

It should be pointed out that this is not the historical route to the theory of ideals. The theory of ideals started in order to get the factorization property for more general rings than ring of integers. We will come back to this historical note later when we define prime ideals.

Definition 5.2.1. *Suppose A is a ring, and I is a non-empty subset. We say I is an* ideal *of A if*

1. *For every $x, y \in I$, $x - y \in I$, and*
2. *For every $x \in I$ and $a \in A$, then $ax \in I$ and $xa \in I$.*

When I is an ideal of A, we write $I \trianglelefteq A$ or $I \triangleleft A$.

So we have

Lemma 5.2.2. *For every ring homomorphism $f : A \to B$, we have that* $\ker f$ *is an ideal.*

Next we construct some ideals.

Lemma 5.2.3. *Suppose A is a unital commutative ring, and $x_1, \ldots, x_n \in A$. Then the smallest ideal of A which contains $x_1, \ldots, x_n$ is*

$$\{a_1x_1 + \cdots + a_nx_n \mid a_1, \ldots, a_n \in A\}. \tag{5.1}$$

We denote this ideal by $\langle x_1, \ldots, x_n\rangle$ and we call it the ideal generated by $x_1, \ldots, x_n$.

Proof. We start by showing that the set I given in (5.1) is an ideal and it contains x_i's. Suppose $y, y' \in I$; then

$$y = \sum_{i=1}^{n} a_ix_i \text{ and } y' = \sum_{i=1}^{n} a'_ix_i$$

for some a_i's and a'_i's in A. Hence

$$y - y' = (\sum_{i=1}^{n} a_ix_i) - (\sum_{i=1}^{n} a'_ix_i) = \sum_{i=1}^{n}(a_i - a'_i)x_i \in I.$$

For every $a \in A$, we have

$$ay = a(\sum_{i=1}^{n} a_i x_i) = \sum_{i=1}^{n} (aa_i)x_i \in I.$$

This shows that I is an ideal of A. For every i_0, we have

$$x_{i_0} = 0_A x_1 + \cdots + 0_A x_{i_0 - 1} + 1_A x_{i_0} + 0_A x_{i_0+1} + \cdots + 0_A x_n \in I,$$

which implies that x_i's are in I.

Next suppose J is an ideal of A which contains x_i's. Then for every $a_i \in A$ we have $a_i x_i \in A$, which in turn implies that

$$a_1 x_1 + \cdots + a_n x_n \in J.$$

Therefore $I \subseteq J$. This finishes the proof. □

We say an ideal I is a *principal ideal* if it is generated by one element. By Lemma 5.2.3, we have that in a unital commutative ring A the principal ideal generated by x is

$$\langle x \rangle = \{ax \mid a \in A\}.$$

We sometimes denote $\langle x \rangle$ by xA.

As in group theory, we will prove the isomorphism theorems. To get to that, we start by defining the quotient ring.

5.3 Quotient rings

Suppose I is an ideal of a ring A. Then for every $x, y \in I$, we have $x - y \in I$. Hence by the subgroup criterion, I is a subgroup of A. As A is abelian, I is a normal subgroup of A. Therefore the set A/I of all the cosets of I form an abelian group under the following operation

$$(x + I) + (y + I) := (x + y) + I.$$

Next we define a multiplication on A/I.

Lemma 5.3.1. *Suppose $I \trianglelefteq A$. The following is a well-defined operation on A/I*

$$(x + I) \cdot (y + I) := xy + I$$

for $x + I, y + I \in A/I$.

Proof. Suppose $x_1 + I = x_2 + I$ and $y_1 + I = y_2 + I$. Then $x_1 - x_2 \in I$ and $y_1 - y_2 \in I$. Here we are using a result from group theory which states that for two cosets $a + H$ and $a' + H$ we have

$$a + H = a' + H \text{ if and only if } a - a' \in H. \tag{5.2}$$

By (5.2), to show $x_1y_1 + I = x_2y_2 + I$ it is necessary and sufficient to show that

$$x_1y_1 - x_2y_2 \in I. \tag{5.3}$$

We show this by adding and subtracting a new term (this method is similar to how we find the formula for the derivative of product of two functions):

$$\begin{aligned} x_1y_1 - x_2y_2 =&(x_1y_1 - x_1y_2) + (x_1y_2 - x_2y_2) \\ =&x_1(y_1 - y_2) + (x_1 - x_2)y_2. \end{aligned} \tag{5.4}$$

Since $y_1 - y_2 \in I$ and $x_1 - x_2 \in I$, we have

$$x_1(y_1 - y_2), (x_1 - x_2)y_2 \in I. \tag{5.5}$$

By (5.4), (5.5), and the fact that I is closed under addition we deduce that $x_1y_1 - x_2y_2 \in I$. Hence $x_1y_1 + I = x_2y_2 + I$ which finishes the proof. □

Notice that Lemma 5.3.1 holds for non-commutative rings as well.

Proposition 5.3.2. *Suppose A is a ring and $I \lhd A$. Then*

1. *$(A/I, +, \cdot)$ is a ring where for every $x + I, y + I \in A/I$ we have*

$$(x + I) + (y + I) := (x + y) + I \quad \text{and} \quad (x + I) \cdot (y + I) := xy + I.$$

2. *$p_I : A \to A/I, p_I(x) := x + I$ is a surjective ring homomorphism.*

3. *$\ker p_I = I$.*

Remark 5.3.3. *The ring A/I is called a quotient ring of A and p_I is called the natural quotient map.*

Proof of Proposition 5.3.2. Since all the operations are defined in terms of coset representatives, it is straightforward to check all the properties of rings and show that A/I is a ring. I leave this as an exercise.

Let's prove the second item:

$$p_I(x) + p_I(y) = (x + I) + (y + I) = (x + y) + I = p_I(x + y),$$

and

$$p_I(x) \cdot p_I(y) = (x + I) \cdot (y + I) = xy + I = p_I(xy).$$

Every element of A/I is of the form $x + I = p_I(x)$, which means that p_I is surjective.

Finally notice that

$$x \in \ker p_I \;\Leftrightarrow\; p_I(x) = 0 + I \;\Leftrightarrow\; x + I = 0 + I \;\Leftrightarrow\; x \in I,$$

and the claim follows. □

The following is a consequence of Proposition 5.3.2 and Lemma 5.2.2:

Corollary 5.3.4. *Suppose A is a ring and I is a subset of A. Then I is the kernel of a ring homomorphism from A to another ring if and only if I is an ideal.*

5.4 The first isomorphism theorem for rings

In this section, we prove the first isomorphism theorem for rings. Let's recall the group theoretic version of this theorem:

Theorem 5.4.1 (The 1st Isomorphism Theorem for Groups)**.** *Suppose $f : G \to G'$ is a group homomorphism. Then*

$$\overline{f} : G/\ker f \to \operatorname{Im} f, \ \ \overline{f}(g \ker f) := f(g)$$

is a well-defined group isomorphism.

We use Theorem 5.4.1 to show the following:

Theorem 5.4.2. *Suppose $f : A \to A'$ is a ring homomorphism. Then*

$$\overline{f} : A/\ker f \to \operatorname{Im} f, \ \ \overline{f}(a + \ker f) := f(a)$$

is a ring isomorphism.

Proof. Since f is an additive group homomorphism, by the first isomorphism theorem for groups we have that $\widetilde{f}$ is a well-defined group isomorphism. To finish the proof, it is enough to show that $\overline{f}$ preserves the multiplication:

$$\overline{f}(xy + \ker f) = f(xy) = f(x)f(y) = \overline{f}(x + \ker f)\overline{f}(y + \ker f),$$

for every $x, y \in A$. This finishes the proof. □

Example 5.4.3. *Suppose n is a positive integer. Then $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.*

Proof. Let $c_n : \mathbb{Z} \to \mathbb{Z}_n$ be the residue map $c_n(x) := [x]_n$. Then c_n is surjective and

$$x \in \ker c_n \ \Leftrightarrow \ [x]_n = [0]_n \ \Leftrightarrow \ n|x \ \Leftrightarrow \ x \in n\mathbb{Z}.$$

By the first isomorphism theorem for rings, we have that

$$\overline{c}_n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n, \quad \overline{c}_n(x + n\mathbb{Z}) = c_n(x)$$

is a ring isomorphism. □

A general strategy of using the first isomorphism theorem to show that a quotient ring A/I is isomorphic to a ring B is to start with a ring homomorphism $f : A \to C$ where B is a subring of C, and show that $\operatorname{Im} f = B$ and $\ker f = I$. This is what we did in the previous example and what we will do in the next example as well.

Example 5.4.4. *We have*

$$\mathbb{Q}[x]/\langle x^2 - 2 \rangle \simeq \mathbb{Q}[\sqrt{2}],$$

and

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Proof. Let $\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C}$ be the evaluation map $\phi_{\sqrt{2}}(f(x)) = f(\sqrt{2})$. Then by the first theorem for rings we have

$$\mathbb{Q}[x]/\ker\phi_{\sqrt{2}} \simeq \operatorname{Im}\phi_{\sqrt{2}}.$$

Recall that we have defined $\mathbb{Q}[\sqrt{2}]$ to be the image $\operatorname{Im}\phi_{\sqrt{2}}$ of $\phi_{\sqrt{2}}$.

Next we find the kernel $\ker\phi_{\sqrt{2}}$. Notice that $\sqrt{2}$ is a zero of x^2-2, and so x^2-2 is in $\ker\phi_{\sqrt{2}}$. Suppose $f(x) \in \ker\phi_{\sqrt{2}}$. By the long division, there are $q(x), r(x) \in \mathbb{Q}[x]$ such that

1. $f(x) = q(x)(x^2-2) + r(x)$, and
2. $\deg r < \deg(x^2-2)$.

Since $\deg r < 2$, there are $a, b \in \mathbb{Q}$ such that $r(x) = ax+b$. As $f(\sqrt{2}) = 0$, we deduce that

$$0 = f(\sqrt{2}) = q(\sqrt{2})\underbrace{(\sqrt{2})^2-2)}_{\text{is } 0} + (a\sqrt{2}+b).$$

Hence $a\sqrt{2}+b=0$. If $a \neq 0$, then $\sqrt{2} = -b/a \in \mathbb{Q}$ which is a contradiction as $\sqrt{2}$ is irrational. Thus $a=0$, which in turn implies that $b=0$. This means $r(x)=0$, and so $f(x) = q(x)(x^2-2) \in I$. Therefore $\ker\phi_{\sqrt{2}} = I$.

(We will continue in the next lecture.) □

Chapter 6

Lecture 6

6.1 An application of the first isomorphism theorem.

In the previous lecture, we were in the middle of the proof of the following result. We will be generalizing this result later in the course. We will be using similar techniques to describe the structure of $\mathbb{Q}[\alpha]$ where α is a zero of a polynomial.

Example 6.1.1. *We have*

$$\mathbb{Q}[x]/\langle x^2-2\rangle \simeq \mathbb{Q}[\sqrt{2}],$$

and

$$\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}.$$

Proof. We have already considered the evaluation map $\phi_{\sqrt{2}}$, used the first isomorphism theorem to show that

$$\mathbb{Q}[x]/\ker\phi_{\sqrt{2}} \simeq \operatorname{Im}\phi_{\sqrt{2}}.$$

Next we used the long division and proved that $\ker\phi_{\sqrt{2}} = \langle x^2-2\rangle$.

Next we want to show that $\mathbb{Q}[\sqrt{2}] = \{a_0+a_1\sqrt{2} \mid a_0,a_1 \in \mathbb{Q}\}$. To show this we again use the long division.

Elements of $\mathbb{Q}[\sqrt{2}]$ are of the form $p(\sqrt{2})$ for some $p(x) \in \mathbb{Q}[x]$. By the long division, there are $q(x), r(x) \in \mathbb{Q}[x]$ such that

1. $p(x) = q(x)(x^2-2)+r(x)$, and
2. $\deg r < \deg(x^2-2)$.

Hence there are $a_0, a_1 \in \mathbb{Q}$ such that $r(x) = a_0 + a_1 x$. Therefore

$$p(\sqrt{2}) = q(\sqrt{2})(\sqrt{2}^2-2)+(a_0+a_1\sqrt{2}) = a_0+a_1\sqrt{2}.$$

This implies that $\mathbb{Q}[\sqrt{2}] = \{a_0+a_1\sqrt{2} \mid a_0,a_1 \in \mathbb{Q}\}$, and the claim follows. □

As you can see in this examples, the long division plays an important role in understanding of polynomials. Next we want to see in what generality the long division holds.

6.2 Degree of polynomials

Suppose A is a unital commutative ring and

$$f(x)=a_0+a_1x+\cdots+a_nx^n\in A[x] \quad \text{and} \quad a_n\neq 0.$$

Then we say a_nx^n is the *leading term* of f, and we write $\mathrm{Ld}(f):=a_nx^n$. The leading term contains two information: the *leading coefficient* a_n and the exponent n of x which is called the *degree* of f, and we write $\deg f=n$. We use the following convention for the zero polynomial:

$$\deg 0=-\infty, \quad \text{and} \quad \mathrm{Ld}(0):=0.$$

Example 6.2.1. *Find* $\deg((2x+1)(3x^2+1))$ *in* $\mathbb{Z}_6[x]$.

Solution. By the distribution property we have

$$(2x+1)(3x^2+1)=\underbrace{(2\cdot 3)}_{0\text{ in }\mathbb{Z}_6}x^3+3x^2+2x+1=3x^2+2x+1.$$

Hence $\deg((2x+1)(3x^2+1))=2$. □

Notice that in the above example, $\deg(2x+1)=1$ and $\deg(3x^2+1)=2$. Hence sometimes,

$$\deg f\cdot g\neq \deg f+\deg g.$$

A closer examination of the above example reveals that existence of zero-divisors is responsible for the failure of the degree of the product formula. In fact, if *at least one of the leading coefficients of f or g is not a zero-divisor, then we have*

$$\deg f\cdot g=\deg f+\deg g.$$

Let's see the details.

Lemma 6.2.2. *Suppose A is a unital commutative ring, and $f(x),g(x)\in A[x]$.*

1. *Suppose the leading coefficient of f is a and the leading coefficient of g is b. If $ab\neq 0$, then* $\mathrm{Ld}(fg)=\mathrm{Ld}(f)\,\mathrm{Ld}(g)$ *and* $\deg fg=\deg f+\deg g$.

2. *Suppose that the leading coefficient of f is not a zero-divisor. Then*

$$\mathrm{Ld}(fg)=\mathrm{Ld}(f)\,\mathrm{Ld}(g) \quad \textit{and} \quad \deg fg=\deg f+\deg g; \tag{6.1}$$

in particular, if D is an integral domain, then (6.1) *holds.*

Proof. (1) Suppose

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\ g(x)=b_0+b_1x+\cdots+b_mx^m,$$

$a_n=a$, and $b_m=b$. Then

$$f(x)g(x)=a_nb_mx^{n+m}+\text{ terms of degree less than } m+n.$$

Hence if a_nb_m is not zero, then $\mathrm{Ld}(fg) = a_nb_mx^{n+m}$. Notice that by the assumption we have $a_nb_m = ab \neq 0$. Therefore the claim follows as $\mathrm{Ld}(f) = ax^n$ and $\mathrm{Ld}(g) = bx^m$.

(2) Suppose g is not zero and its leading coefficient is b. Since the leading coefficient a of f is not a zero divisor, $ab \neq 0$. Therefore by part (1), the claim follows. If $g = 0$, then $fg = 0$. Hence $\deg fg = \deg g = -\infty$. As we are using the convention that $-\infty + n = -\infty$ for every $n \in \mathbb{Z}$, the claim follows in this case as well.

When D is an integral domain, the leading coefficient of a non-zero $f(x)$ is not a zero-divisor. Hence we get the claim. If $f = 0$, then $fg = 0$. Thus $\mathrm{Ld}(fg) = 0 = \mathrm{Ld}(f)\,\mathrm{Ld}(g)$ and $\deg fg = -\infty = -\infty + \deg g = \deg f + \deg g$, which finishes the proof. □

6.3 Zero-divisors and units of ring of polynomials

In this section, we use Lemma 6.2.2 to study the ring of polynomials of integral domains.

Lemma 6.3.1. *Suppose D is an integral domain. Then $D[x]$ is an integral domain.*

Proof. Since D is an integral domain, it is a unital commutative ring. Therefore $D[x]$ is a unital commutative ring. Since D is an integral domain, it is a non-trivial ring. As $D[x]$ has a copy of D (constant polynomials), $D[x]$ is a non-trivial ring. So it remains to show that $D[x]$ does not have a zero-divisor. Suppose $f(x)g(x) = 0$ for some $f, g \in D[x]$. Then $\deg fg = -\infty$, and so by Lemma 6.2.2 we have

$$-\infty = \deg f + \deg g.$$

Therefore not both of $\deg f$ and $\deg g$ can be integers, and at least one of them is $-\infty$. This means either $f = 0$ or $g = 0$. This means $D[x]$ does not have a zero-divisors. □

Lemma 6.3.2. *Suppose D is an integral domain. Then*

$$D[x]^\times = D^\times.$$

Proof. Suppose $u \in D^\times$. Therefore $u^{-1} \in D$ exists. Since $D[x]$ has a copy of D as the set of constant polynomials, we deduce that $u^{-1} \in D[x]$ (notice that $D[x]$ and D have the same identity). Hence $u \in D^\times$. This means $D^\times \subseteq D[x]^\times$.

Let's go to the more interesting part where the assumption that D is an integral domain is actually needed.

Suppose $f(x) \in D[x]^\times$. This means there is $g(x) \in D[x]$ such that $f(x)g(x) = 1$. By Lemma 6.2.2, we have that

$$\deg f + \deg g = \deg fg = \deg 1 = 0.$$

This, in particular, implies that f and g are not zero, and so their degrees are at least 0. Therefore $\deg f$ and $\deg g$ are two non-negative integers that add up to 0. Hence both of them are zeros. That means $f(x) = a \in D$, $g(x) = b \in D$, and $f(x)g(x) = ab$ is 1. This implies that $f(x) = a \in D^\times$, which finishes the proof. □

6.4 Long division

In this section, we will show the most general form of the long division for polynomials. Let's start with a quick overview of the long division for polynomials. Say we want to divide

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

by

$$g(x) = b_m x^m + \cdots + b_1 x + b_0.$$

In the long division algorithm, first we look at the degrees. If $\deg f = n$ is smaller than $\deg g = m$, then we are done! In this case, the quotient is 0 and the remainder is $f(x)$. If $\deg f \geq \deg g$, then we look for a monomial cx^k to multiply by $\mathrm{Ld}(g)$ and end up getting $\mathrm{Ld}(f)$; that means $(cx^k)(b_m x^m) = a_n x^n$:

$$\begin{array}{rl} & \quad\ \boxed{cx^k} \\ \cline{2-2} \boxed{b_m x^m} + \cdots + b_0 &) \ \ \boxed{a_n x^n} + \cdots + a_0 \end{array}$$

This means that $k + m = n$ and $b_m a = a_n$. Since we assumed $n \geq m$, $n - m \geq 0$, and we can let $k := n - m$. The equation $b_m c = a_n$, however, does not necessarily have a solution in A. This equation has a solution in A if b_m is a unit. In this case, we see that the desired monomial is $(b_m^{-1} a_n) x^{n-m}$. After finding this monomial, we subtract $(b_m^{-1} a_n x^{n-m}) g(x)$ from $f(x)$, get a smaller degree polynomial and *continue this process*. This leads us to the following theorem.

Theorem 6.4.1 (Long Division For Polynomials)**.** *Suppose A is a unital commutative ring, $f(x), g(x) \in A[x]$ and the leading coefficient of $g(x)$ is a unit in A. Then there are unique $q(x) \in A[x]$ (quotient) and $r(x) \in A[x]$ (remainder) that satisfy the following properties:*

$$f(x) = g(x)q(x) + r(x) \quad \textit{and} \quad \deg r < \deg g. \tag{6.2}$$

(Whenever you see the phrase *and we continue this process*, it means that there is an *induction argument* in the formal proof.)

Proof. (The existence part) We proceed by the strong induction on $\deg f$. If $\deg f < \deg g$, then $q(x) = 0$ and $r(x) = f(x)$ satisfy (6.2). So we prove the strong induction step under the extra condition that $\deg f \geq \deg g$. Suppose $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, $a_n \neq 0$, and $b_m \neq 0$. Then by the assumption b_m is a unit in A. Let

$$\overline{f}(x) := f(x) - (b_m^{-1} a_n) x^{n-m} g(x). \tag{6.3}$$

Then one can see that $\deg \overline{f} < \deg f$. Hence by the strong induction hypothesis, we can divide $\overline{f}$ by g and get a quotient $\overline{q}$ and a remainder r; this means we have

$$\overline{f}(x) = \overline{q}(x) g(x) + r(x) \quad \text{and} \quad \deg r < \deg g. \tag{6.4}$$

By (6.4) and (6.3), we obtain

$$f(x) = ((b_m^{-1} a_n) x^{n-m} + \overline{q}(x)) g(x) + r(x) \quad \text{and} \quad \deg r < \deg g.$$

Hence $q(x) := (b_m^{-1}a_n)x^{n-m} + \overline{q}(x)$ and $r(x)$ satisfy (6.2). This completes the proof of the existence part.

(The uniqueness part) Suppose q_1, r_1 and q_2, r_2 both satisfy (6.2). We have to prove that $q_1 = q_2$ and $r_1 = r_2$. As q_i, r_i satisfy (6.2). This means

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x),$$

$$\deg r_1 < \deg g, \text{ and } \deg r_2 < \deg g.$$

Hence we have

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x) \quad \text{and} \quad \deg(r_2 - r_1) < \deg g. \tag{6.5}$$

Since the leading coefficient of g is a unit, it is not a zero-divisor (see Lemma 3.3.4). Therefore by Lemma 6.2.2 and (6.5), we have

$$\deg(r_1 - r_2) = \deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg g < \deg g.$$

Hence $\deg(q_1 - q_2) < 0$, which implies that $q_1 - q_2 = 0$. Thus by (6.5), we deduce that $r_1 = r_2$. Overall we showed that $q_1 = q_2$ and $r_1 = r_2$, which finishes the proof the uniqueness. □

Chapter 7

Lecture 7

7.1 The factor theorem and the generalized factor theorems

In the previous lecture we proved a general form of the long division for polynomials. We proved that if A is a unital commutative ring, we can divide $f(x)$ by $g(x)$ for $f, g \in A[x]$ and a quotient and a remainder if the leading coefficient of g is a unit in A. In particular, if A is a field, then the leading coefficient of every non-zero polynomial is a unit. Hence we can divide every polynomial by every non-zero polynomial.

The Factor Theorem is an important application of the long division for polynomials.

Theorem 7.1.1. *Suppose A is a unital commutative ring and $f(x) \in A[x]$. Then*

1. *for every $a \in A$, there is a unique $q(x) \in A[x]$ such that*
$$f(x) = (x - a)q(x) + f(a).$$

2. (The Factor Theorem) *We have that a is a zero of $f(x)$ if and only if there is $q(x) \in A[x]$ such that*
$$f(x) = (x - a)q(x).$$

Proof. (1) By the long division for polynomials, there are unique $q(x)$ and $r(x)$ with the following properties:

$$f(x) = (x - a)q(x) + r(x) \quad \text{and} \quad \deg r < \deg(x - a).$$

The second property implies that $r(x)$ is a constant, say $r(x) = c \in A$. Then we have $f(x) = (x - a)q(x) + c$. Evaluating both sides at $x = a$, we deduce that $c = f(a)$. Altogether, we obtain that $f(x) = (x - a)q(x) + f(a)$, which finishes the proof of the first part.

(2) Suppose a is a zero of f; then $f(a) = 0$. Therefore by part (1), we have that $f(x) = (x - a)q(x)$ for some $q(x) \in A[x]$.

To show the converse, we can evaluate both sides of $f(x) = (x - a)q(x)$ at $x = a$, and deduce that $f(a) = 0$. This finishes the proof. □

The factor theorem can be interpreted in terms of the evaluation map: for every $a \in A$ we have

$$\ker \phi_a = \langle x - a \rangle,$$

where $\phi_a : A[x] \to A, \phi_a(f(x)) := f(a)$.

Theorem 7.1.2. *Suppose D is an integral domain, $f(x) \in D[x]$, and $a_1, \dots, a_n$ are distinct elements of D. Then $a_1, \dots, a_n$ are zeros of $f(x)$ if and only if there is $q(x) \in D[x]$ such that*

$$f(x) = (x - a_1) \cdots (x - a_n) q(x).$$

Proof. We proceed by the induction on n. The base of induction $n = 1$ follows from the Factor Theorem. So we focus on the induction step. Suppose $a_1, \dots, a_{n+1}$ are distinct zeros of $f(x)$. Then by the induction hypothesis, there is $\overline{q}(x) \in D[x]$ such that

$$f(x) = (x - a_1) \cdots (x - a_n) \overline{q}(x). \tag{7.1}$$

Since a_{n+1} is a zero of $f(x)$, by (7.1) we deduce that

$$0 = (a_{n+1} - a_1) \cdots (a_{n+1} - a_n) \overline{q}(a_{n+1}). \tag{7.2}$$

Since a_j's are distinct, $a_{n+1} - a_i$'s are not zero. As D is an integral domain, it has no zero-divisor. Therefore by (7.2), we obtain that

$$\overline{q}(a_{n+1}) = 0.$$

Hence by the Factor Theorem, there is $q(x) \in D[x]$ such that

$$\overline{q}(x) = (x - a_{n+1}) q(x). \tag{7.3}$$

By (7.2) and (7.3), we obtain that

$$f(x) = (x - a_1) \cdots (x - a_n)(x - a_{n+1}) q(x).$$

This finishes the claim. □

Remark 7.1.3. *The Factor Theorem holds for every unital commutative ring, but the Generalized Factor Theorem is true only for integral domains.*

Exercise 7.1.4. *Give an example where the Generalized Factor Theorem fails.*

Corollary 7.1.5. *Suppose D is an integral domain and $f(x) \in D[x] \setminus \{0\}$. Then f does not have more than $\deg f$ distinct zeros in D.*

Proof. Suppose $a_1, \dots, a_m$ are distinct zeros of $f(x)$. Then by the generalized factor theorem there is $q(x) \in D[x]$ such that

$$f(x) = (x - a_1) \cdots (x - a_m) q(x). \tag{7.4}$$

Comparing the degrees of both sides of (7.4), we get

$$\deg f = m + \deg q.$$

Notice that since f is not zero, neither is q. Thus $\deg q \geq 0$. Hence $\deg f \geq m$, which finishes the proof. □

7.2 An application of the generalized factor theorem

In this section, we prove an interesting result in congruence arithmetic with the help of the generalized factor theorem. Later, we will prove a generalization of this result for all finite fields.

Theorem 7.2.1. *Suppose p is a prime number. Then*

$$x^p - x = x(x-1)\cdots(x-(p-1))$$

in $\mathbb{Z}_p[x]$.

Proof. By the Fermat's little theorem, for every $a \in \mathbb{Z}_p$, we have $a^p - a = 0$. This means $0, 1, \ldots, p-1$ are distinct zeros of $x^p - x$ in $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is an integral domain, we can employ the generalized factor theorem and deduce that there is $q(x) \in \mathbb{Z}_p[x]$ such that

$$x^p - x = x(x-1)\cdots(x-(p-1))q(x). \tag{7.5}$$

Comparing the degree of the both sides of (7.5), we obtain that $p = p + \deg q$. Hence $q(x) = c$ is a non-zero constant. Therefore

$$x^p - x = cx(x-1)\cdots(x-(p-1)). \tag{7.6}$$

Comparing the leading coefficients of (7.6), we deduce that $c = 1$. This implies that

$$x^p - x = x(x-1)\cdots(x-(p-1)),$$

and the claim follows. □

As a corollary of Theorem 7.2.1, we deduce Wilson's theorem.

Corollary 7.2.2. *Suppose p is prime. Then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. By Theorem 7.2.1, we have

$$x^p - x = x(x-1)\cdots(x-(p-1)) \tag{7.7}$$

in $\mathbb{Z}_p[x]$. This means that all the coefficients of these polynomials are congruent modulo p. Let's compare the coefficients of x. The coefficient of x on the left hand side of (7.7) is -1, and the coefficient of x on the right hand side of (7.7) is $(-1)(-2)\cdots(-(p-1))$. Therefore

$$(-1)^{p-1}(p-1)! \equiv -1 \pmod{p}. \tag{7.8}$$

For $p = 2$, we have $(2-1)! \equiv -1 \pmod{2}$. So we can and will assume that $p \neq 2$. Therefore p is odd, which implies that $(-1)^{p-1} = 1$. By (7.8) and $(-1)^{p-1} = 1$, we obtain that

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

which finishes the proof of Wilson's theorem. □

We can use polynomial equations to deduce many interesting congruence relations. The next exercise is another such example.

Exercise 7.2.3. *Suppose p is an odd prime number. Use $(x-1)^p = x^p - 1$ in $\mathbb{Z}_p[x]$ and the cancellation law in $\mathbb{Z}_p[x]$, to deduce that*

$$\binom{p-1}{i} \equiv (-1)^i \pmod{p}$$

for every $0 \leq i \leq p-1$.

7.3 Ideals of ring of polynomials over a field

Let's go back to the zeros of polynomials. Suppose $\alpha \in \mathbb{C}$ is a zero of a polynomial. We would like to understand the ring structure of $\mathbb{Q}[\alpha]$. By the first isomorphism theorem, we have

$$\mathbb{Q}[x]/\ker \phi_\alpha \simeq \mathbb{Q}[\alpha]$$

where $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at α. To understand the ring structure of $\mathbb{Q}[\alpha]$, we need to study the ideals of $\mathbb{Q}[x]$.

Theorem 7.3.1. *Suppose F is a field. Then every ideal of $F[x]$ is principal.*

Proof. Suppose I is an ideal of $F[x]$. If I is the zero ideal, we are done. Suppose I is not zero, and choose $p_0(x) \in I$ such that

$$\deg p_0 = \min\{\deg p \mid p \in I \setminus \{0\}\};$$

$\deg p_0$ is the smallest among the degrees of non-zero polynomials of I. The next claim finishes the proof.

Claim. $I = \langle p_0 \rangle$.

Proof of Claim. Since p_0 is in I, $\langle p_0 \rangle \subseteq I$. Next we want to show that every element of I is in $\langle p_0 \rangle$. Suppose $f(x) \in I$. We have to show that $f(x)$ is a multiple of $p_0(x)$. Since F is a field every non-zero element of F is a unit. This implies that the leading coefficient of p_0 is a unit in F, and so we can use the long division and divide $f(x)$ by $p_0(x)$. Let $q(x)$ be the quotient and $r(x)$ be the remainder of $f(x)$ divided by $p_0(x)$: this means

$$f(x) = p_0(x)q(x) + r(x) \quad \text{and} \quad \deg r < \deg p_0. \tag{7.9}$$

Since $f(x), p_0(x) \in I$, $r(x) = f(x) - p_0(x)q(x) \in I$. As $r \in I$, $\deg r < \deg p_0$ and $\deg p_0$ is the smallest degree of non-zero polynomials of I, we obtain that $r(x) = 0$. Therefore $f(x) = p_0(x)q(x) \in \langle p_0(x) \rangle$. This completes the proof of the Claim. □

Definition 7.3.2. *Suppose D is an integral domain. We say D is a Principal Ideal Domain (PID) if every ideal of D is principal.*

Example 7.3.3. *The ring $\mathbb{Z}$ of integers and the ring $F[x]$ of polynomials over a field F are PIDs.*

Let's recall that the way we proved $\mathbb{Z}$ is a PID is by using a result from group theory which asserts that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some integer n. This result, in part, was proved using the long division for integers. As we see, there is a common technique of using a long division to prove that $\mathbb{Z}$ and $F[x]$ are PIDs. This brings us to the definition of *Euclidean Domain*.

7.4 Euclidean Domain

In mathematics, we often find a common pattern, extract the essence of various proofs, and introduce a new object that has only the needed properties. The advantage of this process is that for new examples we can focus on only the needed properties.

Definition 7.4.1. *An integral domain D is called a* Euclidean domain *if there is a* norm function $N : D \to \mathbb{Z}^{\geq 0}$ *with the following properties:*

1. $N(d) = 0$ *if and only if* $d = 0$.
2. *For every* $a \in D$ *and* $b \in D \setminus \{0\}$*, there are* $q, r \in D$ *such that*
   - *(i)* $a = bq + r$*, and*
   - *(ii)* $N(r) < N(b)$.

In a Euclidean Domain, we have a form of a long division, and this help us prove that every Euclidean Domain is a PID.

Theorem 7.4.2. *Suppose D is a Euclidean Domain. Then D is a PID.*

Proof. Suppose I is an ideal of D. If I is zero, we are done. Suppose I is not zero. Choose $a_0 \in I$ such that $N(a_0)$ is the smallest among the norm of the non-zero elements of I:

$$N(a_0) = \min\{N(a) \mid a \in I \setminus \{0\}\}.$$

The following Claim finishes the proof.

Claim. $I = \langle a_0 \rangle$.

Proof of Claim. Since $a_0 \in I$, we have $\langle a_0 \rangle \subseteq I$. Next we show that every element of I is a multiple of a_0. For $a \in I$, by the main property of Euclidean Domains, there are $q, r \in D$ such that

$$a = a_0 q + r, \quad \text{and} \quad N(r) < N(a_0). \tag{7.10}$$

Since $a, a_0 \in I$, we have $r = a - a_0 q \in I$. As $r \in I$, $N(r) < N(a_0)$, and $N(a_0)$ is the smallest norm of non-zero elements of I, we obtain that $r = 0$. Therefore $a = a_0 q \in \langle a_0 \rangle$. This completes the proof of the Claim. □

Notice that because of the long division for integers, the function $N : \mathbb{Z} \to \mathbb{Z}^{\geq 0}, N(a) := |a|$ makes $\mathbb{Z}$ a Euclidean domain. Similarly the long division for polynomials and the function $N : F[x] \to \mathbb{Z}^{\geq 0}, N(f(x)) := 2^{\deg f}$ (with the convention that $2^{-\infty} = 0$) makes $F[x]$ a Euclidean domain when F is a field.

Next we use the concept of Euclidean Domain to prove that the Gaussian integers $\mathbb{Z}[i]$ is a PID. In the next lecture, we will prove:

Theorem 7.4.3. *The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain. Therefore $\mathbb{Z}[i]$ is a PID.*

Chapter 8

Lecture 8

8.1 Gaussian integers

In the other lecture, we defined Euclidean Domain and proved that every Euclidean domain is a PID. We have also pointed out that $\mathbb{Z}$ and $F[x]$, where F is a field, are Euclidean domains. Next we want to prove that the ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain, and so it is a PID.

Theorem 8.1.1. $\mathbb{Z}[i]$ *is a Euclidean domain and a PID.*

Proof. To show $\mathbb{Z}[i]$ is a Euclidean domain, we have to find a *norm function* with the desired properties. Let

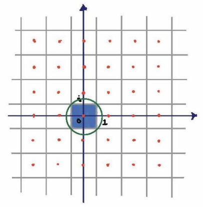
$$N : \mathbb{Z}[i] \to \mathbb{Z}^{\geq 0},\ N(z) := |z|^2,$$

where $|z|$ is the complex norm. Notice that for every integers a and b, we have $N(a + bi) = a^2 + b^2 \in \mathbb{Z}^{\geq 0}$. Next notice that for every complex number z, we have

$$N(z) = 0 \Leftrightarrow |z| = 0 \Leftrightarrow z = 0.$$

It is remained to show a type of division property for $\mathbb{Z}[i]$ with respect to the function N.

We start with the division in $\mathbb{C}$: for every $z \in \mathbb{Z}[i]$ and $w \in \mathbb{Z}[i] \setminus \{0\}$, consider $\frac{z}{w} \in \mathbb{C}$. Notice that the square tiling in the given figure implies that there is $q \in \mathbb{Z}[i]$ such that $\frac{z}{w} - q$ is in the central square. Therefore $\left|\frac{z}{w} - q\right| \leq \frac{\sqrt{2}}{2}$, and so the complex norm of $r := z - wq$ is at most $\frac{\sqrt{2}}{2}|q| < |q|$.



Since z, w, q are in $\mathbb{Z}[i]$, so is r. Altogether we obtain the existence of $q, r \in \mathbb{Z}[i]$ such that

$$z = qw + r, \quad \text{and} \quad N(r) < N(q).$$

This shows that the ring of Gaussian integers is a Euclidean domain. Earlier we have seen that every Euclidean domain is a PID, which finishes the proof. □

Exercise 8.1.2. *Let $\omega := \frac{-1}{2} + \frac{\sqrt{3}}{2}i$, and $\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}$. Use a similar method as in the proof of Theorem 8.1.1 to show that $\mathbb{Z}[\omega]$ is a PID.*

8.2 Algebraic elements and minimal polynomials

Let's go back to zeros of polynomials.

Definition 8.2.1.

1. *We say $\alpha \in \mathbb{C}$ is an* algebraic *number if it is a zero of a polynomial $f(x) \in \mathbb{Q}[x]$.*
2. *More generally, when F is a subfield of another field E*[1]*, we say $\alpha \in E$* is algebraic over *F if α is a zero of a polynomial $f(x) \in F[x]$.*
3. *A complex number α is called* transcendental *if it is not algebraic.*
4. *Assuming E is a field extension of F, we say $\alpha \in E$ is* transcendental *over F if it is not algebraic over F.*

Example 8.2.2. *$\sqrt[3]{2}$ is an algebraic number, and there are interesting and not so easy results that the Euler number e and π are transcendental.*

One can easily see that, for E is a field extension of F, $\alpha \in E$ is algebraic over F if and only if the kernel $\ker \phi_\alpha$ of the evaluation map

$$\phi_\alpha : F[x] \to E, \quad \phi_\alpha(f(x)) := f(\alpha)$$

is non-zero. In this setting, our goal is to understand the structure of the ring $F[\alpha]$. So far we have seen many such examples: $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, etc. In the examples we have discussed, we described the elements of these rings as certain linear combinations, and proved that all of these rings are fields. We want to generalize these results.

Notice that by the first isomorphism theorem we have

$$F[x]/\ker \phi_\alpha \simeq F[\alpha]. \tag{8.1}$$

This means we need to investigate $\ker \phi_\alpha$. For instance we immediately deduce the following:

Corollary 8.2.3. *Suppose E is a field extension of F, and $\alpha \in E$ is transcendental over F. Then $F[\alpha] \simeq F[x]$.*

Proof. Since α is transcendental over F, $\ker \phi_\alpha = 0$. Therefore by (8.1), the claim follows. □

Next we use the fact that $F[x]$ is a PID to describe $\ker \phi_\alpha$ when $\alpha \in E$ is algebraic over F.

Theorem 8.2.4 (The minimal polynomial)**.** *Suppose E is a field extension of F, and $\alpha \in E$ is algebraic over F. Then the following statements hold.*

[1] In this case we say E is a *field extension* of F.

1. *There is a unique non-constant monic polynomial* $m_\alpha(x) \in F[x]$ *such that* $\ker \phi_\alpha = \langle m_\alpha(x) \rangle$. *(*$m_\alpha(x) \in F[x]$ *is called* the minimal polynomial of α over F.
2. *The minimal polynomial* $m_\alpha(x) \in F[x]$ *is a non-constant monic polynomial which cannot be written as a product of smaller degree polynomials in* $F[x]$.

Proof. (1) Since $F[x]$ is a PID, there is $f(x) \in F[x]$ which generates $\ker \phi_\alpha$. Since α is algebraic over F, $f(x)$ is not zero. We also know that non-zero constant functions are not in the kernel of ϕ_α. Hence $f(x)$ is not a constant polynomial. Suppose

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

and $a_n \neq 0$. Then a_n is a unit in F (as F is a field). Let

$$\overline{f}(x) := a_n^{-1} f(x) = x^n + (a_n^{-1} a_{n-1}) x^{n-1} + \cdots + (a_n^{-1} a_0).$$

Since $\overline{f}(x) = a_n^{-1} f(x) \in \langle f(x) \rangle$ and $f(x) = a_n \overline{f}(x) \in \langle \overline{f} \rangle$, we deduce that

$$\langle \overline{f} \rangle = \langle f \rangle = \ker \phi_\alpha.$$

This shows the *existence* of a monic non-constant polynomial which generates $\ker \phi_\alpha$. Next we show the uniqueness of such a polynomial. It is clear that uniqueness is a special case of the following Claim.

Claim. *Suppose* f_1 *and* f_2 *are non-constant monic polynomials in* $F[x]$*, and* $\langle f_1 \rangle = \langle f_2 \rangle$. *Then* $f_1 = f_2$.

Proof of Claim. Since $\langle f_1 \rangle = \langle f_2 \rangle$, there are polynomials $q_1, q_2 \in F[x]$ such that $f_1 q_1 = f_2$ and $f_2 q_2 = f_1$. Comparing the degrees of the sides, we deduce that

$$\deg f_1 + \deg q_1 = \deg f_2 \quad \text{and} \quad \deg f_2 + \deg q_2 = \deg f_1. \tag{8.2}$$

Notice that since $f_i \neq 0$, so are q_i's. Therefore $\deg q_i \geq 0$. Hence by (8.2), we have $\deg f_1 \leq \deg f_2$ and $\deg f_2 \leq \deg f_1$. This implies that $\deg f_1 = \deg f_2$, and so q_i's are non-zero constants. Suppose $q_1(x) = c \in F^\times$. Then we have $cf_1 = f_2$. Comparing the leading coefficients of both sides, we obtain that $c = 1$. Therefore $f_1 = f_2$, and the claim follows. □

(2) Suppose to the contrary that $m_\alpha(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ with $\deg g, \deg h < \deg m_\alpha$. Then

$$\phi_\alpha(g)\phi_\alpha(h) = \phi_\alpha(m_\alpha) = 0$$

implies that either $g \in \ker \phi_\alpha$ or $h \in \ker \phi_\alpha$ (notice that F has no zero-divisors). As $\ker \phi_\alpha$ is generated by $m_\alpha(x)$, either $m_\alpha(x) | g(x)$ or $m_\alpha(x) | h(x)$. Since g and h are not zero, we deduce that either $\deg m_\alpha \leq \deg g$ or $\deg m_\alpha \leq \deg h$. This contradicts that $\deg g, \deg h < \deg m_\alpha$. □

Next we prove the converse of the second part of Theorem 8.2.4. This result will help us to actually find the minimal polynomial $m_\alpha(x)$ for some algebraic elements.

Theorem 8.2.5 (Characterization of minimal polynomials)**.** *Suppose E is a field extension of F, and $\alpha \in E$ is algebraic over F. Then a monic non-constant polynomial $p(x)$ in $F[x]$ is the minimal polynomial of α if and only if $p(\alpha) = 0$ and $p(x)$ cannot be written as a product of smaller degree polynomials in $F[x]$.*

Proof. Part (2) of Theorem 8.2.4 gives us ($\Rightarrow$), and so we focus on ($\Leftarrow$).

Since $p(\alpha) = 0$, $p(x)$ is in $\ker \phi_\alpha$. As $\ker \phi_\alpha$ is generated by the minimal polynomial m_α, we obtain that $p(x) = m_\alpha(x)q(x)$ for some $q(x) \in F[x]$. Since $p(x)$ cannot be written as a product of smaller degree polynomials in $F[x]$, we deduce that $\deg m_\alpha = \deg p$ and $q(x)$ is a non-zero constant polynomial. Suppose $q(x) = c \in F$. Then comparing the leading coefficients of both sides of $cm_\alpha(x) = p(x)$, it follows that $c = 1$. Thus $m_\alpha(x) = p(x)$, and the claim follows. □

It is useful to notice that $m_\alpha(x)$ has the smallest degree among non-zero polynomials in $F[x]$ that have α as a zero.

Proposition 8.2.6. *Suppose E is a field extension of F, and $\alpha \in E$ is algebraic over F. Then the following statements hold.*

1. *For $f(x) \in F[x]$, $f(\alpha) = 0$ if and only if $m_\alpha(x)|f(x)$ in $F[x]$.*
2. *Suppose α is a zero of a non-zero polynomial $p(x) \in F[x]$. If $\deg p \leq \deg m_\alpha$, then there is a non-zero constant c such that $p(x) = cm_\alpha(x)$.*

Proof. (1) We have $f(\alpha) = 0 \Leftrightarrow f \in \ker \phi_\alpha = \langle m_\alpha(x) \rangle \Leftrightarrow m_\alpha(x)|f(x)$.

(2) Since $p(\alpha) = 0$, by the first part we have that $p(x)$ is a (non-zero) multiple of $m_\alpha(x)$; that means there is a non-zero polynomial $q(x) \in F[x]$ such that $p(x) = q(x)m_\alpha(x)$. As $\deg p \leq \deg m_\alpha$, we deduce that

$$\deg m_\alpha \geq \deg p = \deg m_\alpha + \deg q, \text{ which implies that } \deg q = 0.$$

This means q is a non-zero constant, and the claim follows. □

8.3 Elements of quotients of ring of polynomials

Let's recall that one of our goals is to understand the ring structure of $F[\alpha]$ and describe its elements. By the discussions in the previous section, we have $F[\alpha] \simeq F[x]/\langle m_\alpha(x) \rangle$. The next result, which is based on the long division for polynomials, gives us a description of elements of the quotient ring of a ring of polynomials by a monic polynomial.

Proposition 8.3.1. *Suppose A is a unital commutative ring, and $p(x) \in A[x]$ is a monic polynomial of degree $n \geq 1$. Then every element of $A[x]$ can be uniquely written as*

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle p(x) \rangle$$

for some $a_0, \ldots, a_{n-1} \in A$.

Proof. **Existence.** For every $f(x) \in A[x]$, by the long division for polynomials there are unique $q(x) \in A[x]$ (the quotient) and $r(x) \in A[x]$ (the remainder) such that

1. $f(x) = q(x)p(x) + r(x)$, and
2. $\deg r < \deg p$.

The second item means that $r(x) = \sum_{i=0}^{n-1} a_i x^i$ for some $a_i \in A$. The first item implies that $f(x) - r(x) \in \langle p(x) \rangle$. Altogether we have

$$f(x) + \langle p(x) \rangle = \sum_{i=0}^{n-1} a_i x^i + \langle p(x) \rangle.$$

Uniqueness. Suppose $\sum_{i=0}^{n-1} a_i x^i + \langle p(x) \rangle = \sum_{i=0}^{n-1} a_i' x^i + \langle p(x) \rangle$. Then $h(x) := \sum_{i=0}^{n-1} a_i x^i - \sum_{i=0}^{n-1} a_i' x^i$ is a multiple of $p(x)$ and has degree at most $n-1$. As $\deg p = n$ and $p(x)$ is monic, the only multiple of $p(x)$ that has degree less than n is 0. Hence $\sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{n-1} a_i' x^i$, which implies the uniqueness part. □

Chapter 9

Lecture 9

9.1 Elements of $F[\alpha]$

One of our main goals is to understand the ring structure of $\mathbb{Q}[\alpha]$ for an algebraic number α. In the previous lecture we showed that for a field extension E of F and $\alpha \in E$ that is algebraic over F, there is a unique monic non-constant polynomial $m_\alpha(x) \in F[x]$ such that

1. For every $f(x) \in F[x]$, $f(\alpha) = 0$ if and only if $m_\alpha(x) | f(x)$.
2. For a monic polynomial $p(x) \in F[x]$, we have that $p(x) = m_\alpha(x)$ if and only if $p(\alpha) = 0$ and $p(x)$ cannot be written as a product of smaller degree polynomials in $F[x]$.
3. $F[\alpha] \simeq F[x]/\langle m_\alpha(x) \rangle$.

The polynomial $m_\alpha(x) \in F[x]$ is called the minimal polynomial of α over F. [1] Because of the third property, we described elements of the quotient ring $F[x]/\langle p(x) \rangle$ where $p(x)$ is a polynomial of degree $n \geq 1$. Using the long division for polynomials, we proved that every element of this quotient ring can be *uniquely* written as $r(x) + \langle p(x) \rangle$ for some $r(x) \in F[x]$ with $\deg r \leq n - 1$. Base on these results, we immediately get a fairly good description of elements of $F[\alpha]$.

Theorem 9.1.1. *Suppose E is a field extension of F, and $\alpha \in E$ is algebraic over F. Suppose the degree of the minimal polynomial $m_\alpha(x)$ of α over F is n. Then every element of $F[\alpha]$ can be uniquely written as*

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

for some a_i's in F.

[1] A better notation for $m_\alpha(x)$ should include F as well, as the minimal polynomial of α only makes sense after we specify F. That is why in some texts $m_\alpha(x)$ is denoted by $m_{\alpha,F}(x)$. Here we assume that we know what F is from the context in which α is discussed.

Proof. By the first isomorphism theorem for rings, we know that

$$\overline{\phi}_\alpha : F[x]/\langle m_\alpha(x)\rangle \to F[\alpha], \quad \overline{\phi}_\alpha(f(x) + \langle m_\alpha(x)\rangle) := f(\alpha) \tag{9.1}$$

is an isomorphism. By Proposition 8.3.1, every element of $F[x]/\langle m_\alpha(x)\rangle$ can be uniquely written as $(\sum_{i=0}^{n-1} a_i x^i) + \langle m_\alpha(x)\rangle$ for some a_i's in F. Hence by (9.1), we obtain that every element of $F[\alpha]$ can be uniquely written as

$$\overline{\phi}_\alpha\Big(\sum_{i=0}^{n-1} a_i x^i) + \langle m_\alpha(x)\rangle\Big) = \sum_{i=0}^{n-1} a_i \alpha^i.$$

This completes the proof. □

Note that Theorem 9.1.1 is a generalization of many examples that we have discussed so far, e.g.

$$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\} \quad \text{because} \quad m_{i,\mathbb{Q}}(x) = x^2 + 1,$$

and

$$\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \mid a_0, a_1, a_2 \in \mathbb{Q}\} \quad \text{because} \quad m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3 - 2.$$

9.2 Irreducible elements

By now it is clear that in order to understand the ring structure of $F[\alpha]$ for a given α which is algebraic over F, we have to figure out a way to find the minimal polynomial $m_\alpha(x) \in F[x]$. Theorem 8.2.5 gives us a key characterization of $m_\alpha(x)$ which brings us to the definition of irreducible elements.

Definition 9.2.1. *Suppose D is an integral domain. We say $d \in D$ is* irreducible *if*

1. *$d \notin D^\times \cup \{0\}$, and*
2. *If $d = ab$ for some $a, b \in D$, then either $a \in D^\times$ or $b \in D^\times$.*

For instance an integer n is irreducible in $\mathbb{Z}$ if $n = \pm p$ for some prime number p. Let me warn you that later we will define *prime elements* of an integral domain, and irreducible and prime elements do not always coincide!

Lemma 9.2.2. *Suppose F is a field. Then $p(x) \in F[x]$ is irreducible if and only if $p(x)$ is not constant and it cannot be written as a product of smaller degree polynomials in $F[x]$.*

Proof. ($\Rightarrow$) Since $f(x)$ is irreducible, $f(x) \notin F[x]^\times \cup \{0\}$. As $F[x]^\times = F^\times = F \setminus \{0\}$, we obtain that $f(x)$ is not constant. Now suppose to the contrary that $f(x) = g(x)h(x)$ and $\deg g, \deg h < \deg f$. This implies that $g(x)$ and $h(x)$ are not constant polynomials. On the other hand, since $f(x)$ is irreducible, $f(x) = g(x)h(x)$ implies that either $g \in F[x]^\times$ or $h \in F[x]^\times$. As $F[x]^\times = F^\times$, we deduce that either $\deg g = 0$ or $\deg h = 0$, which is a contradiction.

($\Leftarrow$) Suppose $f(x) = g(x)h(x)$. Since f cannot be written as a product of smaller degree polynomials in $F[x]$, we have that either $\deg g \geq \deg f$ or $\deg h \geq \deg f$. As $\deg f = \deg g + \deg h$, we deduce that either $\deg g = 0$ or $\deg h = 0$. That means either $g \in F \setminus \{0\}$ or $h \in F \setminus \{0\}$. Since F is a field, we obtain that either $g \in F^\times = F[x]^\times$ or $h \in F^\times = F[x]^\times$. This completes the proof. □

Now, some of the properties of minimal polynomials can be phrased in a more compact form.

Corollary 9.2.3 (Minimal polynomials and irreducibility)**.** *Suppose E is a field extension of F, $\alpha \in E$ is algebraic over F, and $p(x) \in F[x]$ is a monic polynomial. Then $p(x) = m_\alpha(x)$ if and only if $p(\alpha) = 0$ and $p(x)$ is irreducible.*

Proof. This is an immediate consequence of Theorem 8.2.5 and Lemma 9.2.2. □

This motivates us to answer the following questions:

1. Assuming that D is an integral domain or a PID, what can we say about ideals that are generated by irreducible elements and their quotient rings?

2. Can we come up with certain mechanisms to find out whether a given monic polynomial is irreducible?

We start by answering the first question. We have already pointed out that irreducible elements of the ring of integers are essentially prime numbers. Therefore for an irreducible element p of $\mathbb{Z}$ we have that $\mathbb{Z}/\langle p \rangle$ is a field. We will show that this result holds for every PID.

Let's begin by understanding when exactly two principal ideals are equal.

Lemma 9.2.4. *Suppose D is an integral domain, and $a, b \in D$. Then $\langle a \rangle = \langle b \rangle$ if and only if $a = bu$ for some unit u.*

Proof. We notice that $\langle a \rangle = \langle b \rangle$ if and only if $a \in \langle b \rangle$ and $b \in \langle a \rangle$. This means

$$\langle a \rangle = \langle b \rangle \Leftrightarrow \exists x, y \in D, a = bx \text{ and } b = ay. \tag{9.2}$$

($\Leftarrow$) If $a = bu$ for some unit u, then $b = au^{-1}$. Therefore by (9.2), we have $\langle a \rangle = \langle b \rangle$.

($\Rightarrow$) If $a = 0$, then $b \in \langle a \rangle$ implies that $b = 0$. Therefore $a = 1 \cdot b$ and there is nothing to prove.

Suppose $a \neq 0$, and $x, y \in D$ are as in (9.2). Then

$$a = bx = (ay)x = a(yx).$$

By the cancellation law, we deduce that $yx = 1$ (notice that D is an integral domain and $a \neq 0$, and so we are allowed to use the cancellation law). Hence x is a unit, which finishes the proof. □

Lemma 9.2.4 immediately gives us a description for units in terms of ideals.

Lemma 9.2.5. *Suppose A is a unital commutative ring, and $a \in A$. Then a is a unit if and only if $\langle a \rangle = A$.*

Proof. ($\Rightarrow$) Assuming that a is a unit, we have that $a' = (a'a^{-1})a \in \langle a \rangle$ for every $a' \in A$. This means that $A = \langle a \rangle$.

($\Leftarrow$) If $\langle a \rangle = A$, then $1 \in \langle a \rangle$, which implies that $1 = aa'$ for some $a' \in A$. Therefore a is a unit. □

Lemma 9.2.5 help us to describe fields in terms of their ideals.

Lemma 9.2.6. *Suppose F is a unital commutative ring. Then F is a field if and only if F has exactly two distinct ideals $\{0\}$ and F.*

Proof. ($\Rightarrow$) Since F is a field, F and $\{0\}$ are distinct. Now suppose I is a non-zero ideal of F. Then there is a non-zero element a in I. Since F is a field, a is a unit in F. Hence by Lemma 9.2.5

$$F = \langle a \rangle \subseteq I.$$

This means $I = F$.

($\Leftarrow$) Since F and $\{0\}$ are distinct, $0 \not\in F^{\times}$. So it is enough to show that every non-zero element of F is a unit. Suppose $a \in F \setminus \{0\}$, and consider $\langle a \rangle$. As F is the only non-zero ideal of F, we have $F = \langle a \rangle = aF$. Hence by Lemma 9.2.5, a is a unit in F. This finishes the proof. □

We also notice that in a field F, there is no irreducible element as $F = F^{\times} \cup \{0\}$. So when we are studying irreducible elements, we can and will assume that the given integral domain is not a field.

Lemma 9.2.7. *Suppose D is an integral domain which is not a field. Then $a \in D$ is irreducible if and only if $\langle a \rangle$ is a maximal ideal among proper principal ideals.*

Let's begin by explaining various phrases in the statement of Lemma 9.2.7. Suppose Σ is a collection of subsets of a given set X, Then we say $A \in \Sigma$ is a *maximal* element of Σ if there is no element $B \in \Sigma$ that contains A as a proper subset. In mathematical language, it means

$$A \in \Sigma \text{ is maximal if and only if } \forall B \in \Sigma, A \subseteq B \Rightarrow B = A.$$

In Lemma 9.2.7, the collection Σ is $\{I \trianglelefteq D \mid I \text{ is principal}, I \neq D\}$. Altogether, we can rewrite Lemma 9.2.7 as follows.

Suppose D is an integral domain which is not a field, and $a \in D$. Then a is irreducible in D if and only if $\langle a \rangle \neq D$ and for every $b \in D$,

$$\langle a \rangle \subseteq \langle b \rangle \Rightarrow \textit{ either } \langle a \rangle = \langle b \rangle \textit{ or } \langle b \rangle = D.$$

Proof of Lemma 9.2.7. $(\Leftarrow)$ Suppose a is irreducible in D and $\langle a \rangle \subseteq \langle b \rangle$. As a is irreducible, it is not a unit. Therefore by Lemma 9.2.5, $\langle a \rangle$ is a proper ideal.

As $a \in \langle b \rangle$, $a = bc$ for some $c \in D$. Since a is irreducible, either $b \in D^\times$ or $c \in D^\times$. If $b \in D^\times$, then by Lemma 9.2.5 we have $\langle b \rangle = D$. If $c \in D^\times$, then by Lemma 9.2.4, $\langle a \rangle = \langle b \rangle$.

$(\Leftarrow)$ Since $\langle a \rangle$ is a proper ideal, by Lemma 9.2.5 a is not a unit. Next we argue why $a \neq 0$.

Suppose to the contrary that $a = 0$. Then for every non-zero element $b \in D$, we have $\langle a \rangle \subsetneq \langle b \rangle$. Hence by the assumption $\langle b \rangle = D$. This together with Lemma 9.2.5 implies that b is a unit. This means every non-zero element of D is a unit, which implies that D is a field. This is a contradiction.

Next let's assume that $a = bc$ for some $b, c \in D$. Then $\langle a \rangle \subseteq \langle b \rangle$. By the assumption, we deduce that either $\langle a \rangle = \langle b \rangle$ or $\langle b \rangle = D$. Therefore by Lemma 9.2.4 and Lemma 9.2.5, we deduce that either there is $u \in D^\times$ such that $a = bu$ or $b \in D^\times$. In the former case, by the cancellation law, we have $c = u \in D^\times$ and in the latter case, $b \in D^\times$. This means a is irreducible. □

9.3 Maximal ideals and their quotient rings

Based on Lemma 9.2.7, we know that irreducibility is an information about principal ideals, and so we gain more information when D is a PID. If D is a PID and $a \in D$ is irreducible, then $\langle a \rangle$ is maximal among *all* proper ideals. This brings us to the definition of maximal ideals.

Definition 9.3.1. *Suppose A is a unital commutative ring and $I \trianglelefteq A$. We say I is a* maximal *ideal if it is maximal among* proper *ideals; that means*

$$\forall J \trianglelefteq A, I \subseteq J \Rightarrow \text{ either } J = I \text{ or } J = A.$$

So by Lemma 9.2.7 and Lemma 9.2.6, we immediately obtain the following:

Lemma 9.3.2. *Suppose D is a PID, and $a \in D$. Then*

1. *for $a \neq 0$, we have that $\langle a \rangle$ is a maximal ideal if and only if a is irreducible.*

2. *$\{0\}$ is a maximal ideal if and only if D is a field.*

The next Proposition gives us the key property of maximal ideals.

Proposition 9.3.3. *Suppose A is a unital commutative ring and $I \trianglelefteq A$. Then I is a maximal ideal if and only if A/I is a field.*

We start with the *corresponding* lemma which describes ideals of a quotient ring.

Lemma 9.3.4. *Suppose A is a unital commutative ring and $I \trianglelefteq A$. Then $\bar{J}$ is an ideal of A/I if and only if $\bar{J} = J/I$ for some $J \trianglelefteq A$ which contains I.*

Proof. ($\Rightarrow$) Suppose $\bar{J}$ is an ideal of A/I, and let

$$J := \{a \in A \mid a + I \in \bar{J}\}.$$

Then for every $a \in I$, we have $a + I = 0 + I \in \bar{J}$, and so $a \in J$. Therefore $I \subseteq J$. Next we show that J is an ideal of A. Suppose $a, a' \in J$. Then $a + I, a' + I \in \bar{J}$. As $\bar{J}$ is an ideal, we have $(a + I) - (a' + I) \in \bar{J}$. This implies that $(a - a') + I \in \bar{J}$, and so $a - a' \in J$. For $a \in J$, we have that $a + I \in \bar{J}$. Since $\bar{J}$ is an ideal of A/I, for every $b \in A$, we have that $(b + I)(a + I) \in \bar{J}$. Therefore $ba + I \in \bar{J}$. Hence $ba \in J$. Altogether we have that J is an ideal, it contains I, and

$$\bar{J} = \{a + I \mid a \in J\} = J/I.$$

($\Leftarrow$) From group theory we know that J/I is a subgroup of A/I. Now suppose $a+I \in J/I$ and $b+I \in A/I$. Since J is an ideal of A and $a \in J$, we have that $ab \in J$. Hence $(a + I)(b + I) \in J/I$. Thus J/I is an ideal of A/I. □

Proof of Proposition 9.3.3. By Lemma 9.2.6, A/I is a field if and only if it has exactly two ideals I/I and A/I. By Lemma 9.3.4, every ideal of A/I is of the form J/I where J is an ideal of A which contains I. Hence A/I has exactly two ideals if and only if I and A are the only ideals of A which contain I and $I \neq A$. The latter happens exactly when I is a maximal ideal. This completes the proof. □

We immediately get the following corollary for PIDs.

Corollary 9.3.5. *Suppose that D is a PID and not a field, and $a \in D$. Then $D/\langle a\rangle$ is a field if and only if a is irreducible in D.*

Proof. By Proposition 9.3.3, $D/\langle a\rangle$ is a field if and only if $\langle a\rangle$ is a maximal ideal. By Lemma 9.3.2 and the assumption that D is not a field, $\langle a\rangle$ is a maximal ideal if and only if a is irreducible. This completes the proof. □

9.4 $F[\alpha]$ is a field!

Now we are well-prepared to prove the following:

Theorem 9.4.1. *Suppose E is a field extension of F, and $\alpha \in E$ is algebraic over F. Then $F[\alpha]$ is a field.*

Proof. We have already proved that $F[\alpha] \simeq F[x]/\langle m_{\alpha,F}(x)\rangle$ where $m_{\alpha,F}(x)$ is the minimal polynomial of α over F (see (9.1) and Theorem 8.2.4). We further showed that $m_{\alpha,F}(x)$ is irreducible in $F[x]$ (see Corollary 9.2.3), and $F[x]$ is a PID (see Theorem 7.3.1) which is not a field (see Lemma 6.3.2). Then by Corollary 9.3.5, we deduce that $F[x]/\langle m_{\alpha,F}(x)\rangle$ is a field. Thus $F[\alpha]$ is a field. □

As you can see in this proof, we do not show the existence of the multiplicative inverse of an element in a direct way. So for a given algebraic number α sometimes it is tricky to express the inverse of $p(\alpha)$ in terms of a linear combination of $1, \alpha, \alpha^2, \cdots$.

Exercise 9.4.2. *Suppose $\alpha \in \mathbb{C}$ is a zero of $x^3 - x + 1$. Express α^{-1}, $(\alpha + 1)^{-1}$, and $(\alpha^2 + 1)^{-1}$ in the form $a_0 + a_1\alpha + a_2\alpha^2$ for some $a_0, a_1, a_2 \in \mathbb{Q}$.*

Chapter 10

Lecture 10

We have seen that many properties of $F[\alpha]$ where α is algebraic over F depends on the minimal polynomial $m_{\alpha,F}(x)$ of α over F. So it is crucial to have a method of finding $m_{\alpha,F}(x)$. Let's recall that the key property of the minimal polynomial is the following:

$p(x) = m_{\alpha,F}(x)$ if and only if $p(\alpha) = 0$, $p(x)$ is monic and irreducible in $F[x]$.

We will prove a series of *irreducibility criteria* which help us find minimal polynomials of certain algebraic elements.

10.1 Irreducibility and zeros of polynomials

We start with pointing out a consequence of the factor theorem.

Lemma 10.1.1. *Suppose F is a field, and $f(x) \in F[x]$.*

1. *If $\deg f = 1$, then f is irreducible.*
2. *If $\deg f \geq 2$ and f has a zero in F, then f is not irreducible.*
3. *Suppose $\deg f = 2$ or 3. Then f is irreducible in $F[x]$ if and only if f does not have a zero in F.*

Proof. (1) Suppose $\deg f = 1$. Then clearly it is not constant. If $f = gh$, then $1 = \deg g + \deg h$, which implies that we cannot have $\deg g, \deg h < 1$. Therefore f is irreducible.

(2) Suppose $\deg f \geq 2$ and $f(a) = 0$ for some $a \in F$. Then by the factor theorem, there is $g(x) \in F[x]$ such that $f(x) = (x-a)g(x)$. Hence $\deg g = \deg f - 1 < \deg f$ and $\deg(x-a) < \deg f$. Therefore $f(x)$ is not irreducible in $F[x]$.

(3) Suppose $\deg f = 2$ or 3 and $f(x)$ is not irreducible. Then there are $g, h \in F[x]$ such that $f(x) = g(x)h(x)$ and $\deg g, \deg h < \deg f \leq 3$. These imply that $\deg g, \deg h \geq 1$ and $\deg f = \deg g + \deg h \leq 3$. Hence either $\deg g = 1$ or $\deg h = 1$. Without loss of generality, we can and will assume that $\deg g = 1$. Thus $g(x) = a_0 + a_1 x$ for some $a_0, a_1 \in F$ and $a_1 \neq 0$. Then $-a_0 a_1^{-1} \in F$ is a zero of $g(x)$, which implies that $f(x)$ has a zero in F. □

Example 10.1.2. *1.* $f(x) := x^3 - x + 1$ *is irreducible in* $\mathbb{Z}_3[x]$.

2. $\mathbb{Z}_3[x]/\langle f(x)\rangle$ *is a field of order* 27.

Proof. (1) Since $\deg f = 3$, f is irreducible in $\mathbb{Z}_3[x]$ if and only if it does not have a zero in $\mathbb{Z}_3$. As we have seen earlier, by the Fermat's little theorem, $x^3 - x + 1$ does not have a zero in $\mathbb{Z}_3$, which finishes the proof of part one.

(2) Since $f(x)$ is irreducible and $\mathbb{Z}_3[x]$ is a PID, $\langle f(x)\rangle$ is a maximal ideal of $\mathbb{Z}_3[x]$ (see Lemma 9.3.2). Therefore $\mathbb{Z}_3[x]/\langle f(x)\rangle$ is a field (see Proposition 9.3.3). We have proved that every element of $\mathbb{Z}_3[x]/\langle f(x)\rangle$ can be uniquely written as $r(x)+\langle f(x)\rangle$ for a polynomial $r(x) \in \mathbb{Z}_3[x]$ with degree at most 2. Notice that there are 27 polynomials of degree at most 2 in $\mathbb{Z}_3[x]$. (see Proposition 8.3.1). □

Exercise 10.1.3. *Every odd degree polynomial in* $\mathbb{R}[x]$ *is not irreducible.*

10.2 Rational root criterion

Next we give an effective criterion for finding out whether or not a polynomial in $\mathbb{Z}[x]$ has a zero in $\mathbb{Q}$.

Proposition 10.2.1 (Rational root criterion)**.** *Suppose*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

$a_0 \neq 0$, *and* $a_n \neq 0$. *If* $f(\frac{b}{c}) = 0$ *for some* $b, c \in \mathbb{Z}$ *with* $c \neq 0$ *and* $\gcd(b,c) = 1$, *then*

$$b|a_0 \quad \textit{and} \quad c|a_n.$$

(The denominator divides the leading coefficient and the numerator divides the constant term.)

Proof. Since $f(\frac{b}{c}) = 0$, multiplying both sides by c^n, we have

$$a_n b^n + a_{n-1}b^{n-1}c + \cdots + a_1 bc^{n-1} + a_0 c^n = 0. \tag{10.1}$$

This implies that

$$a_n b^n = -c(a_{n-1}b^{n-1} + \cdots + a_1 bc^{n-2} + a_0 c^{n-1}) \text{ is a multiple of } c.$$

Since $\gcd(b,c) = 1$ and $c|a_n b^n$, by Euclid's lemma, $c|a_n$. Similarly (10.1) implies that

$$a_0 c^n = -b(a_n b^{n-1} + a_{n-1}b^{n-2}c + \cdots + a_1 c^{n-1}) \text{ is a multiple of } b.$$

Therefore again by Euclid's lemma we deduce $b|a_0$. This finishes the proof. □

The rational root criterion has many implications. Here is one of them:

Corollary 10.2.2. *Suppose* $f(x) \in \mathbb{Z}[x]$ *is a monic polynomial. Then every rational zero of* f *is an integer which is the divisor of the constant term* $f(0)$.

Proof. Suppose $\frac{b}{c}$ is a zero of f and $\gcd(b,c)=1$. Then by the rational root criterion, c divides the leading coefficient which is 1. Hence $c=\pm 1$. This implies that $\frac{b}{c}=\pm b\in\mathbb{Z}$. Another application of the rational root criterion implies that b divides the constant term. This completes the proof. □

Example 10.2.3. *Suppose $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+1\in\mathbb{Z}[x]$. Prove that f has a rational zero if and only if either $f(1)=0$ or $f(-1)=0$.*

Proof. By Corollary 10.2.2, since f is a monic integer polynomial, every rational zero of f is integer and it is a divisor of the constant term which is 1. Hence a rational zero of f is either 1 or -1. This finishes the proof. □

10.3 Mod criterion: zeros

Though Corollary 10.2.2 theoretically gives us a relatively good algorithm for finding out the rational zeros of a monic integer polynomial, but from computational point of view it might be a daunting task to evaluate a polynomial of degree 20 at 2. On the other hand, finding what 2^n modulo 5 is actually easy! This means from computational point of view it is better to work with integers modulo a *small* positive integer. The following lemma shows us how we can employ this technique.

Lemma 10.3.1. *Suppose A and B are unital commutative rings, and $c:A\to B$ is a ring homomorphism. Then*

1. *$c:A[x]\to B[x], c\Big(\sum_{i=0}^n a_ix^i\Big):=\sum_{i=0}c(a_i)x^i$ is a ring homomorphism.*
2. *For $a\in A$ and $b\in B$, let*

$$\phi_a:A[x]\to A,\phi_a(f(x)):=f(a)\quad\textit{and}\quad\phi_b:B[x]\to B,\phi_b(g(x)):=g(b)$$

be the corresponding evaluation maps. Then for every $a\in A$ we have

$$c(\phi_a(f(x)))=\phi_{c(a)}(c(f(x))).$$

Proof. Both parts are easy to check and I leave the task of writing the details as an exercise. □

Lemma 10.3.1 immediately implies that if $f(x)\in A[x]$ has a zero in A, then $c(f)$ has a zero in B. The contrapositive of this statement is often used.

Suppose $c:A\to B$ is a ring homomorphism, and $f(x)\in A[x]$. If $c(f(x))$ does not have a zero in B, then $f(x)$ does not have a zero in A.

Here is one important example.

Lemma 10.3.2. *Suppose $f(x)\in\mathbb{Z}[x]$ is a monic polynomial. If $f(x)$ does not have a zero in $\mathbb{Z}_n$ for some positive integer n, then $f(x)$ does not have a zero in $\mathbb{Q}$.*

The common steps for proving statements of this type where we want to show certain property $\mathscr{P}$ passes from $\mathbb{Z}_n$ to $\mathbb{Q}$ are:

0. Look at the contrapositive, and start with $\mathbb{Q}$.

1. Show that we can pass to $\mathbb{Z}$.

2. Use the residue maps and pass to $\mathbb{Z}_n$.

Usually Step 1 is the hard step where we want to go from $\mathbb{Q}$ to $\mathbb{Z}$.

Proof of Lemma 10.3.2. Suppose $f(x)$ has a zero in $\mathbb{Q}$. Since $f(x) \in \mathbb{Z}[x]$ is monic, by Corollary 10.2.2 $f(x)$ has a zero $a \in \mathbb{Z}$. Then by Lemma 10.3.1, $c_n(a) := [a]_n$ is a zero of $c_n(f)$ where $c_n : \mathbb{Z} \to \mathbb{Z}_n$. (We simply say that a is a zero of $f(x)$ in $\mathbb{Z}_n$). This shows that the contrapositive of the claim holds, which finishes the proof. □

Lemma 10.3.2 in conjunction with Fermat's little theorem can become a very strong tool. Let's recall that Fermat's little theorem states

$$a^p = a \quad \text{for every } a \in \mathbb{Z}_p.$$

Hence $a^{p^2} = (a^p)^p = a^p = a$ for every $a \in \mathbb{Z}_p$. Therefore inductively we can show that the following holds:

For every positive integer n, prime p, and $a \in \mathbb{Z}_p$,

$$a^{p^n} = a. \tag{10.2}$$

By (10.2), we have that for non-negative integers $c_0, \ldots, c_n$, prime p, and $a \in \mathbb{Z}_p$ the following holds:

$$a^{c_n p^n + c_{n-1}p^{n-1} + \cdots + c_0} = a^{c_n + \cdots + c_0}.$$

This gives us a fast algorithm for finding large powers of elements in $\mathbb{Z}_p$. This makes it easier to evaluate (large degree) polynomials in $\mathbb{Z}_p$.

Example 10.3.3. *Suppose p is prime. Prove that $f(x) := x^{p^2} + px^{p^2-p} - x + (2p+1)$ does not have a rational zero.*

Proof. We will show that $f(x)$ does not have a zero in $\mathbb{Z}_p$. Notice that $f(x)$ modulo p is $x^{p^2} - x + 1$. Hence for every $a \in \mathbb{Z}_p$, we have

$$f(a) = a^{p^2} - a + 1 = 1, \tag{10.3}$$

where the last equality holds because of (10.2). By (10.3), $f(x)$ does not have a zero in $\mathbb{Z}_p$. By Lemma 10.3.2, we deduce that $f(x)$ does not have a zero in $\mathbb{Q}$. This finishes the proof. □

Chapter 11

Lecture 11

In the previous lecture, we showed that if F is a field, $f(x) \in F[x]$ is a polynomial with degree at least 2, and $f(x)$ has a zero in F, then f is not irreducible. We further showed that the converse holds if the degree of f is either 2 or 3. Then we proved the rational root criterion and use it to show that if $f(x) \in \mathbb{Z}[x]$ is a monic polynomial which does not have a zero in $\mathbb{Z}_n$ for some positive integer n, then f does not have a zero in $\mathbb{Q}$. We proved the the contrapositive by first passing from $\mathbb{Q}$ to $\mathbb{Z}$, and then from $\mathbb{Z}$ to $\mathbb{Z}_n$.

We can use the residue maps to find out if a polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible or not.

Theorem 11.0.1 (mod-p criterion)**.** *Suppose $f(x) \in \mathbb{Z}[x]$ is a monic polynomial and p is a prime number. If $f(x)$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

The proof of this theorem has many steps. The general strategy is the same as the one explained in Section 10.3. We prove the contrapositive statement, and it will be done by (1) going from $\mathbb{Q}$ to $\mathbb{Z}$ and (2) going from $\mathbb{Z}$ to $\mathbb{Z}_p$. The main difficulty is in the first step, where we need Gauss's Lemma.

11.1 Content of a polynomial with rational coefficients.

Before we go to the proof, we point out an important difference between being irreducible in $\mathbb{Q}[x]$ and being irreducible in $\mathbb{Z}[x]$.

Example 11.1.1. *$2x$ is irreducible in $\mathbb{Q}[x]$, but it is not irreducible in $\mathbb{Z}[x]$.*

Proof. By Lemma 10.1.1, we know that every degree 1 polynomial with coefficients in a field is irreducible. Therefore $2x$ is irreducible in $\mathbb{Q}[x]$. On the other hand, $2x$ is 2 times x and neither 2 nor x is a unit in $\mathbb{Z}[x]$ as $\mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{1, -1\}$. □

In fact in general if the greatest common divisor of the coefficients of a non-constant integer polynomial $f(x)$ is not 1, then $f(x)$ cannot be irreducible in $\mathbb{Z}[x]$. This is the case as we can simply factor out the greatest common divisor of the coefficients of f

and write $f(x)$ as a product of two non-unit elements of $\mathbb{Z}[x]$. This brings us to the definition of the *content* of an integer polynomial.

Definition 11.1.2. *Suppose $f(x) := a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ is a non-zero polynomial. The* content *of f is the greatest common divisor of the coefficients $a_0, \ldots, a_n$, and we denote it by $\alpha(f)$.* [1]

Example 11.1.3. *1. $\alpha(2x^2 - 6) = 2$ and $\alpha(2x^3 - 6x + 3) = 1$.*

2. The content of a monic integer polynomial is 1.

Using properties of the greatest common divisors, one can prove the following basic properties of content of polynomials.

Lemma 11.1.4. *Let n be a positive integer, $c_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ be the modulo n residue map, $a \in \mathbb{Z} \setminus \{0\}$, and suppose $f(x), g(x) \in \mathbb{Z}[x]$ are two non-zero polynomials. Then*

1. *$\alpha(af(x)) = |a|\alpha(f)$.*
2. *If $\alpha(f) = d$, then $\frac{1}{d}f(x) \in \mathbb{Z}[x]$ and $\alpha(\frac{1}{d}f(x)) = 1$.*
3. *$n|\alpha(f)$ if and only if $f \in \ker c_n$.*

Proof. Part one follows from the fact that

$$\gcd(aa_0, \ldots, aa_m) = |a| \gcd(a_0, \ldots, a_m).$$

The second part is equivalent to the following property of the greatest common divisor:

$$\gcd(a_0, \ldots, a_m) = d \quad \text{implies} \quad \gcd\left(\frac{a_0}{d}, \ldots, \frac{a_m}{d}\right) = 1.$$

The last part is a consequence of the following statement:

$$n|a_0, \ldots, n|a_m \quad \text{if and only if} \quad n| \gcd(a_0, \ldots, a_m).$$

□

Definition 11.1.5. *We say $f(x) \in \mathbb{Z}[x]$ is a* primitive *polynomial if $\alpha(f) = 1$.*

Lemma 11.1.6. *For every $f \in \mathbb{Z}[x]$, there is a primitive polynomial $\overline{f}$ such that*

$$f(x) = \alpha(f)\overline{f}(x).$$

Proof. This is equivalent to part (2) of Lemma 11.1.4. □

Next, we extend the definition of *content* to polynomials in $\mathbb{Q}[x]$.

Lemma 11.1.7. *For every non-zero polynomial $f(x) \in \mathbb{Q}[x]$, there are unique positive rational number q and primitive polynomial $\overline{f}$ such that $f(x) = q\overline{f}(x)$. Moreover for $f(x) \in \mathbb{Z}[x]$, $q = \alpha(f)$.*

[1] The content of f is often denoted by $c(f)$, but we use the notation c_n for the residue map modulo n. So to avoid the possible confusion, we write $\alpha(f)$ for the content of f.

Proof. (Existence) After multiplying by the common denominator n of the coefficients of f, we get an integer polynomial $\widetilde{f}(x)$; that means $\widetilde{f}(x) := nf(x) \in \mathbb{Z}[x]$. By Lemma 11.1.6, there is a primitive polynomial $\overline{f}(x)$ such that $\widetilde{f}(x) = \alpha(\widetilde{f})\overline{f}(x)$. Overall we get

$$\alpha(\widetilde{f})\overline{f}(x) = nf(x) \quad \text{which implies that} \quad f(x) = \frac{\alpha(\widetilde{f})}{n}\overline{f}(x).$$

This completes proof of existence.

Lemma 11.1.6 implies that for $f(x) \in \mathbb{Z}[x]$, we have that $q = \alpha(x)$ satisfies the desired result.

(Uniqueness) Suppose $q_1, q_2 \in \mathbb{Q}$ are positive and $q_1\overline{f}_1(x) = q_2\overline{f}_2(x)$ for some primitive polynomials $\overline{f}_1(x)$ and $\overline{f}_2(x)$. Suppose $q_i = \frac{m_i}{n}$ for some positive integers m_1, m_2 and n. Then $m_1\overline{f}_1 = m_2\overline{f}_2$, which implies that

$$m_1 = \alpha(m_1\overline{f}_1) = \alpha(m_2\overline{f}_2) = m_2.$$

Hence $q_1 = q_2$. This in turn implies that $\overline{f}_1(x) = \overline{f}_2(x)$. The existence follows. □

Definition 11.1.8. *The unique rational number given in Lemma 11.1.7 is called the* content *of f, and it is denoted by $\alpha(f)$.*

Let's point out the Part (1) of Lemma 11.1.4 holds for polynomials in $\mathbb{Q}[x]$.

Lemma 11.1.9. *For every non-zero $f(x) \in \mathbb{Q}[x]$ and $a \in \mathbb{Q} \setminus \{0\}$, we have*

$$\alpha(af(x)) = |a|\alpha(f(x)).$$

Proof. By the definition of the content, there is a primitive polynomial $\overline{f}(x)$ such that $f(x) = \alpha(f)\overline{f}(x)$. Hence $af(x) = (a\alpha(f))\overline{f(x)}$. As $\pm\overline{f}(x)$ are primitive, we deduce that $\alpha(af(x)) = |a|\alpha(f)$, which finishes the proof. □

11.2 Gauss's lemma

Gauss's lemma is the critical result that help us pass from $\mathbb{Q}$ to $\mathbb{Z}$.

Lemma 11.2.1 (Gauss's lemma, version 1)**.** *If f and g are two primitive polynomials, then fg is also primitive.*

Proof. Suppose to the contrary that $\alpha(fg) \neq 1$. Then there is a prime p which divides $\alpha(fg)$. Hence $c_p(fg) = 0$ (by Part (3) of Lemma 11.1.4). Therefore $c_p(f)c_p(g) = 0$. Notice that as $\mathbb{Z}_p$ is an integral domain, so is $\mathbb{Z}_p[x]$. Therefore $c_p(f)c_p(g) = 0$ implies that either $c_p(f) = 0$ or $c_p(g) = 0$. Another application of Part (3) of Lemma 11.1.4 gives us that either $p|\alpha(f)$ or $p|\alpha(g)$. This contradicts the assumption that both f and g are primitive. □

Lemma 11.2.2 (Gauss's lemma, version 2)**.** *Suppose f and g are two non-zero polynomials in $\mathbb{Q}[x]$. Then*

$$\alpha(fg) = \alpha(f)\alpha(g).$$

Proof. By Lemma 11.1.7, there are primitive polynomials $\overline{f}$ and $\overline{g}$ such that

$$f(x) = \alpha(f)\overline{f}(x) \quad \text{and} \quad g(x) = \alpha(g)\overline{g}(x). \tag{11.1}$$

By (11.1), we have that

$$f(x)g(x) = \alpha(f)\alpha(g)\overline{f}\overline{g}. \tag{11.2}$$

Lemma 11.1.9 implies that

$$\begin{aligned} \alpha(f(x)g(x)) =&\alpha(\alpha(f)\alpha(g)\overline{f}(x)\overline{g}(x)) \\ =&\alpha(f)\alpha(g)\alpha(\overline{f}(x)\overline{g}(x)). \end{aligned} \tag{11.3}$$

By the first version of Gauss's lemma, $\alpha(\overline{f}(x)\overline{g}(x)) = 1$. Hence (11.3) implies that

$$\alpha(fg) = \alpha(f)\alpha(g).$$

This completes the proof. □

11.3 Factorization: going from rationals to integers.

The following is the main result of this section, which gives us Step 1 of proof of Theorem 11.0.1. This result says that having a non-trivial decomposition in over $\mathbb{Q}$, we can get a non-trivial decomposition over $\mathbb{Z}$.

Theorem 11.3.1. *Suppose $f(x)$ is a primitive polynomial and $f(x) = \prod_{i=1}^{n} g_i(x)$ for some $g_i \in \mathbb{Q}[x]$. Then there are primitive polynomials $\overline{g}_i(x)$ such that*

$$g_i(x) = \alpha(g_i)\overline{g}_i(x), \quad \prod_{i=1}^{n} \alpha(g_i) = 1, \quad \textit{and} \quad f(x) = \prod_{i=1}^{n} \overline{g}_i(x).$$

Proof. By the second version of Gauss's lemma, we have

$$\alpha(f) = \alpha\Big(\prod_{i=1}^{n} g_i\Big) = \prod_{i=1}^{n} \alpha(g_i) \quad \text{which implies that} \quad \prod_{i=1}^{n} \alpha(g_i) = 1. \tag{11.4}$$

The last implication holds as $\alpha(f) = 1$. Next notice that by the definition of the content, there are primitive polynomials $\overline{g}_i(x)$ such that $g_i(x) = \alpha(g_i)\overline{g}_i(x)$, and so

$$\prod_{i=1}^{n} \overline{g}_i(x) = \prod_{i=1}^{n} \Big(\alpha(g_i)^{-1} g_i(x)\Big) = \Big(\prod_{i=1}^{n} \alpha(g_i)\Big)^{-1} \prod_{i=1}^{n} g_i(x) = f(x).$$

This finishes the proof. □

We have already pointed out that a subtle difference between being irreducible in $\mathbb{Q}[x]$ and being irreducible in $\mathbb{Z}[x]$ is having a non-trivial content. By Theorem 11.3.1, we can show that this is the only thing that one needs to be worried about:

Corollary 11.3.2. *Suppose $f(x)$ is primitive and* $\deg f \geq 1$. *Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.*

Proof. We prove the contrapositive of this statement. Suppose $f(x)$ is not irreducible in $\mathbb{Q}[x]$. As $\deg f \geq 1$, not being irreducible implies that $f(x) = g_1(x)g_2(x)$ for some smaller degree polynomials $g_1, g_2 \in \mathbb{Q}[x]$. By Theorem 11.3.1, there are primitive polynomials $\overline{g}_i$ such that

$$f(x) = \overline{g}_1(x)\overline{g}_2(x) \quad \text{and} \quad \deg \overline{g}_i = \deg g_i \geq 1. \tag{11.5}$$

By (11.5), we deduce that $f(x)$ is not irreducible in $\mathbb{Z}[x]$.

Now let's assume that $f(x)$ is not irreducible in $\mathbb{Z}[x]$. Since $\deg f \geq 1$, it is not a unit. Hence not being irreducible implies that there are non-unit polynomials $h_1, h_2 \in \mathbb{Z}[x]$ such that $f(x) = h_1(x)h_2(x)$. We claim that $\deg h_i \geq 1$. Suppose to the contrary that $\deg h_i = 0$. This means that $h_i(x) = c \in \mathbb{Z}$ and $c \neq \pm 1$ (as h_i is not a unit). This implies that $c|\alpha(f)$ which contradicts the assumption that f is primitive. Hence $\deg h_i \geq 1$, and so $f(x)$ is not irreducible in $\mathbb{Q}[x]$. □

11.4 Mod criterion: irreducibility

Now we are ready to prove the mod-p irreducibility criterion (Theorem 11.0.1). We show the following slightly stronger result.

Theorem 11.4.1. *Suppose $f(x) \in \mathbb{Q}[x]$ is primitive, p is prime which does not divide the leading coefficient of $f(x)$, and $c_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is the modulo p residue map. If $c_p(f(x))$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. As it has been mentioned earlier, we show the contrapositive of this statement. So suppose $f(x)$ is not irreducible in $\mathbb{Q}[x]$. Hence $f(x)$ is either a constant polynomial or it can be written as product of two smaller degree polynomials. Since $c_p(f)$ is irreducible in $\mathbb{Z}_p[x]$, $c_p(f)$ is not constant. Hence $f(x)$ cannot be constant either. Therefore there are non-constant polynomials $g_i(x) \in \mathbb{Q}[x]$ such that $f(x) = g_1(x)g_2(x)$. As $f(x)$ is primitive, by Theorem 11.3.1 there are non-constant primitive polynomials $\overline{g}_i$ such that

$$f(x) = \overline{g}_1(x)\overline{g}_2(x). \tag{11.6}$$

This equality implies that the leading coefficient of f is the product of the leading coefficients of $\overline{g}_i$'s. Since p does not divide the leading coefficient of f, we obtain that p does not divide the leading coefficient of $\overline{g}_i$'s. Hence

$$\deg c_p(\overline{g}_i) = \deg \overline{g}_i = \deg g_i \geq 1.$$

Another application of (11.6) implies that

$$c_p(f) = c_p(\overline{g}_1)c_p(\overline{g}_2),$$

which means that $c_p(f)$ can be written as a product of two smaller degree polynomials. As $\mathbb{Z}_p$ is a field, we deduce that $c_p(f)$ is not irreducible in $\mathbb{Z}_p[x]$. This completes the proof of the contrapositive statement. □

Chapter 12

Lecture 12

In the previous lecture, we proved many important results on irreducibility of integer polynomials in $\mathbb{Q}[x]$. We proved Gauss's lemma and used to show that a monic non-constant integer polynomial can be written as a product of two non-constant primitive polynomials if and only if it is not irreducible in $\mathbb{Q}[x]$. We used this result to show the mod-p irreducibility criterion.

12.1 An example on the mod irreducibility criterion.

Later we will show that for every prime p and $a \in \mathbb{Z}_p^\times$, $x^p - x + a$ is irreducible in $\mathbb{Z}_p$. This result in combination with the mod p irreducibility criteria can be quit helpful.

Example 12.1.1. *Prove that* $f(x) := x^7 - 7x^5 + 21x^3 + 14x^2 - 8x + 11$ *is irreducible in* $\mathbb{Q}[x]$.

Proof. Notice that $f(x)$ modulo 7 is $x^7 - x + 4$. By the mentioned result, this polynomial is irreducible in $\mathbb{Z}_7[x]$. We also notice that $f(x)$ is monic, it is primitive, and the leading coefficient is not a multiple of 7. Therefore by the mod-p irreducibility criteria, $f(x)$ is irreducible in $\mathbb{Q}[x]$. □

For small degree and small primes p, one can go over all the polynomials and *cross out* all the multiples of smaller degree polynomials. This way we can get the list of all the irreducible polynomials of *small* degree in $\mathbb{Z}_p[x]$. Based on the mod-p irreducibility criteria and using the list of *small* degree irreducible polynomials of $\mathbb{Z}_p[x]$, we can find lots of irreducible polynomials in $\mathbb{Q}[x]$.

Example 12.1.2. *1. Prove that* $x^4 + x + 1$ *is irreducible in* $\mathbb{Z}_2[x]$.

2. Prove that $f(x) := 5x^4 + 2x^3 - 2020x^2 + 2021x + 1$ *is irreducible in* $\mathbb{Q}[x]$.

Proof. (1) For every $a \in \mathbb{Z}_2$ and every positive integer n, we have that $a^n = a$. Hence $a^4 + a + 1 = 1$ for every $a \in \mathbb{Z}_2$. This means this polynomial does not have a degree one factor. Hence it is enough to show that it does not have a degree 2 factor. There are exactly 2^2 degree 2 polynomials in $\mathbb{Z}_2[x]$. Let's the list of them:

$x^2, x^2+1, x^2+x, x^2+x+1$. Notice that the first three have zeros in $\mathbb{Z}_2$, and so they cannot possibly be a factor of x^4+x+1. Next we use the long division and divide x^4+x+1 by x^2+x+1. We deduce that $x^4+x+1=(x^2+x+1)(x^2+x)+1$, and so the remainder is $1 \neq 0$. Hence x^4+x+1 does not have degree 1 or 2 factors. If x^4+x+1 is not irreducible in $\mathbb{Z}_2[x]$, then it can be written as a product of two non-constant polynomials. Since the degree of these factors should add up to 4, we get deduce that one of the factors should be of degree 1 or 2. This is a contradiction. Hence x^4+x+1 is irreducible in $\mathbb{Z}_2[x]$.

(2) Notice that $f(x)$ is primitive, the leading coefficient is odd, and $f(x)$ modulo 2 is x^4+x+1 which is irreducible in $\mathbb{Z}_2[x]$. Hence by the mod-p irreducibility criterion, $f(x)$ is irreducible in $\mathbb{Q}[x]$. □

12.2 Eisenstein's irreducibility criterion

One of the most elegant irreducibility criteria is due to Eisenstein.

Theorem 12.2.1. *Let $f(x)=a_nx^n+\cdots+a_1x+a_0 \in \mathbb{Z}[x]$ and p be prime. Suppose*

$$p \nmid a_n,\ p|a_{n-1}, \ldots,\ p|a_0,\ \textit{and}\ \ p^2 \nmid a_0.$$

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Here we start our proof in a systematic manner, but we finish it by showing an ad-hoc result. One gets a better understanding of the final stage using the Unique Factorization property of the ring of polynomials with coefficients in a field. The Unique Factorization property will be proved later in the course.

Proof of Theorem 12.2.1. Suppose to the contrary that there are non-constant polynomials $g_1, g_2 \in \mathbb{Q}[x]$ such that $f(x)=g_1(x)g_2(x)$. Then there are primitive polynomials $\overline{g}_i(x)$ such that $g_i(x)=\alpha(g_i)\overline{g}_i(x)$ (see Lemma 11.1.7), and by the second version of Gauss's lemma $\alpha(f)=\alpha(g_1g_2)=\alpha(g_1)\alpha(g_2)$. Altogether we obtain that

$$f(x)=\alpha(f)\,\overline{g}_1(x)\overline{g}_2(x). \tag{12.1}$$

Notice that $\mathrm{ld}(f)=\alpha(f)\,\mathrm{ld}(\overline{g}_1)\,\mathrm{ld}(\overline{g}_2)$ together with the assumption that p does not divide the leading coefficient a_n imply the p does not divide $\mathrm{ld}(\overline{g}_1)$ and $\mathrm{ld}(\overline{g}_2)$. Next we look at the equation 12.1 modulo p to obtain that $c_p(f)=c_p(\alpha(f))c_p(\overline{g}_1)c_p(\overline{g}_2)$. By the assumption on the divisibility of all the non-leading coefficients by p, we deduce that

$$c_p(a_n)x^n=c_p(\alpha(f))\;c_p(\overline{g}_1)c_p(\overline{g}_2). \tag{12.2}$$

Since p does not divide $\mathrm{ld}(\overline{g}_i)$, we have that $\deg(c_p(\overline{g}_i))=\deg(\overline{g}_i)>0$. Equation 12.2 takes us to the following lemma:

Lemma 12.2.2. *Suppose F is a field and $\overline{g}_1, \overline{g}_2 \in F[x]$ are two non-constant polynomials such that $\overline{g}_1(x)\overline{g}_2(x)=cx^n$ for some $c \in F^\times$. Then $\overline{g}_1(0)=\overline{g}_2(0)=0$.*

Proof. Suppose to the contrary that $\overline{g}_1(0) \neq 0$. Set

$$\overline{g}_1(x) = b_r x^r + \cdots + b_1 x + b_0 \quad \text{and} \quad \overline{g}_2(x) = c_s x^s + \cdots + c_1 x + c_0,$$

where $b_i, c_j \in F$, $b_r, c_s \in F^\times$. The contrary assumption $\overline{g}_1(0) \neq 0$ implies that $b_0 \in F^\times$. Suppose s' is the smallest non-negative integer such that $c_{s'} \neq 0$. This means

$$c_{s'} \in F^\times \quad \text{and} \quad \overline{g}_2(x) = c_s x^s + \cdots + c_{s'} x^{s'}.$$

Consider the coefficient of $x^{s'}$ in $\overline{g}_1(x)\overline{g}_2(x)$. Since every term of $\overline{g}_2(x)$ is of degree at least s', we deduce that the coefficient of $x^{s'}$ in $\overline{g}_1(x)\overline{g}_2(x)$ is $b_0 c_{s'} \neq 0$. We also notice that $s' \leq s < s + r = n$; this implies that $\overline{g}_1(x)\overline{g}_2(x)$ has at least two non-zero terms and it cannot be equal cx^n. This is a contradiction. By symmetry, we obtain that $\overline{g}_2(0) = 0$, which completes proof of Lemma. □

By Lemma 12.2.2 and (12.2), we deduce that

$$c_p(\overline{g}_1)(0) = c_p(\overline{g}_2)(0) = 0.$$

This means $p|\overline{g}_1(0)$ and $p|\overline{g}_2(0)$. Hence

$$p^2|\overline{g}_1(0)\overline{g}_2(0).$$

On the other hand, $a_0 = f(0) = \alpha(f)\overline{g}_1(0)\overline{g}_2(0)$ is a multiple of $\overline{g}_1(0)\overline{g}_2(0)$. Hence $p^2|a_0$, which is a contradiction. This completes proof of Eisenstein's irreducibility criterion. □

Example 12.2.3. *Prove that* $f(x) := \frac{5}{2}x^6 - \frac{4}{3}x^3 + 7x - \frac{3}{11}$ *is irreducible in* $\mathbb{Q}[x]$.

Proof. First we find the content $\alpha(f)$ and the primitive form $\overline{f}$ of f. To find the content of a polynomial first we factor out a common denominator of the coefficients, and take the greatest common divisor of the numerators of the coefficients:

$$\frac{5}{2}x^6 - \frac{4}{3}x^3 + 7x - \frac{3}{11} = \frac{1}{66}((33 \times 5)x^6 - (22 \times 4)x^3 + (66 \times 7)x - (6 \times 3))$$

So the primitive form of $f(x)$ is

$$\overline{f}(x) = (33 \times 5)x^6 - (22 \times 4)x^3 + (66 \times 7)x - (6 \times 3)$$

Notice that since $\alpha(f)$ is a unit in $\mathbb{Q}$, $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $\overline{f}(x)$ is irreducible in $\mathbb{Q}[x]$. Next we check that we can apply Eisenstein's irreduciblity criterion for $p = 2$, and deduce that $\overline{f}$ is irreducible in $\mathbb{Q}[x]$:

$$2 \nmid (33 \times 5),\ 2|(22 \times 4),\ 2|(66 \times 7),\ 2|(6 \times 3), \text{and } 2^2 \nmid (6 \times 3),$$

and the claim follows. □

Next we discuss a *tricky* application of Eisenstein's irreducibility criterion. As you will see, the polynomial given in the next example at the first glance has nothing to do with Eisenstein's irreducibility criterion. After applying a useful trick, however, we will get a polynomial where the hypothesis of Eisenstein's criterion clearly hold.

Example 12.2.4. *Suppose p is prime. Then $f(x) := x^{p-1}+x^{p-2}+\cdots+1$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Notice that

$$f(x)(x-1) = (x^p + x^{p-1} + \cdots + x) - (x^{p-1} + x^{p-2} + \cdots + 1) = x^p - 1,$$

and so $f(x) = \frac{x^p-1}{x-1}$. Let $g(y) := f(y+1)$. Then

$$g(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{p-1} y^{p-2} + \cdots + \binom{p}{1}.$$

Notice that $p \nmid 1,\ p | \binom{p}{i}$ for every integer $i \in [1, p-1],$ and $p^2 \nmid \binom{p}{1}$. Hence by Eisenstein's irreducibility criterion, we have that $g(y)$ is irreducible in $\mathbb{Q}[y]$. Finally notice that if $f(x) = f_1(x) f_2(x)$ for two non-constant polynomials f_1 and f_2 in $\mathbb{Q}[x]$, then $f(y+1) = f_1(y+1) f_2(y+1)$, which implies that $g(y)$ can be written as a product of two non-constant polynomials in $\mathbb{Q}[y]$. This contradicts the irreducibility of $g(y)$ in $\mathbb{Q}[y]$. □

12.3 Factorization: existence, and a chain condition

Let's go back to Lemma 12.2.2, and see what really we can say about the factors of x^n. Notice that x is an irreducible element of $F[x]$, and so all the irreducible factors of x^n are x. If $F[x]$ has the *Unique Factorization* property, then all the irreducible factors of $\overline{g}_i(x)$'s are x as well. This means $\overline{g}_i = c_i x^{n_i}$ for some $c_i \in F^{\times}$ and positive integer n_i.

Definition 12.3.1. *An integral domain D is called a* Unique Factorization Domain *(UFD) if every non-zero non-unit element of D can be written as a product of irreducible elements* (the existence part)*, and the irreducible factors are unique up to reordering and multiplying by a unit* (the uniqueness part).

Example 12.3.2. *The ring of integers is a UFD. Let's understand that the flexibility given in the uniqueness part are needed. In $\mathbb{Z}$, $2, 3, -2,$ and -3 are irreducible and $2 \times 3 = (-3) \times (-2)$. Hence for the uniqueness we have to allow a reordering of the factors and a possible multiplication by units.*

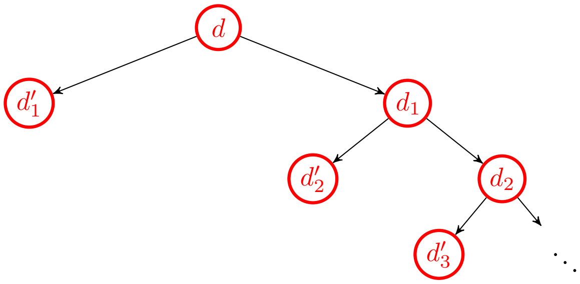
We start with investigating the *existence part* for an arbitrary integral domain D. Suppose $d \in D$ is a non-zero non-unit element. We would like to write d as a product of irreducible elements. We go through the following *pseudo-algorithm*:

1. If d is irreducible, we are done.

2. If d is not irreducible, then there are non-zero non-unit elements $d_1, d'_1 \in D$ such that $d = d_1 d'_1$.

3. Repeat this process for each one of the factors.

If this process *terminates*, we end up writing d as a product of irreducible elements. Let's see what it means for this process to not terminate. We can visualize this process with a binary rooted tree, where all the vertices are labeled by non-zero non-units and label of each vertex is the product of its *children*.



Let's translate this to the language of ideals. Saying that d is a multiple of d_1 is equivalent to $\langle d\rangle \subseteq \langle d_1\rangle$. Recall that $\langle d\rangle = \langle d_1\rangle$ if and only if $d = ud_1$ for some $u \in D^\times$ (see Lemma 9.2.4). Hence $\langle d\rangle = \langle d_1\rangle$ if and only if $d_1 u = d_1 d'_1$. By the cancellation law and d'_1 not being a unit, we deduce that we have an infinite *ascending chain* of (principal) ideals:

$$\langle d\rangle \subsetneq \langle d_1\rangle \subsetneq \langle d_2\rangle \cdots .$$

This takes us to the definition of Noetherian rings.

Definition 12.3.3. *A ring A is called* Noetherian *if there is no infinite ascending chain of ideals. That means if $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals of A, then for some positive integer n_0 we have $I_{n_0} = I_{n_0+1} = \cdots$.*

The above discussion on the existence of a factorization into irreducible elements immediately gives us the following result.

Proposition 12.3.4. *Suppose D is a Noetherian integral domain. Then every non-zero non-unit element of D can be written as a product of irreducible elements of D.*

Proposition 12.3.4 would not be a satisfactory result unless we have an effect way of determining whether or not an integral domain is Noetherian.

Lemma 12.3.5. *Suppose A is a unital commutative ring. Then A is Noetherian ring if and only if every ideal of A is finitely generated.*

(An ideal I is called *finitely generated* if there is a finite set $\{a_1, \ldots, a_n\}$ such that $I = \langle a_1, \ldots, a_n\rangle$ (see Lemma 5.2.3).)

Proof. ($\Rightarrow$) Suppose to the contrary that there is an ideal I which is not finitely generated. Inductively we define a sequence of elements $\{a_i\}_{i=1}^{\infty}$ of I such that

$$\langle a_1\rangle \subsetneq \langle a_1, a_2\rangle \subsetneq \cdots ,$$

which contradicts the assumption that A is Noetherian. Let a_1 be an element of I. Since I is not finitely generated, $\langle a_1\rangle$ is a proper subset of I. Hence there is $a_2 \in I \setminus \langle a_1\rangle$. Again, as I is not finitely generate, $\langle a_1, a_2\rangle$ is a proper ideal of I. Therefore there is $a_3 \in I \setminus \langle a_1, a_2\rangle$. We continue this process inductively, and the proof can be completed as it is explained above.

($\Leftarrow$) Suppose $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals of A. Consider $I := \bigcup_{i=1}^{\infty} I_i$. Next we prove that I is an ideal of A.

For every $a, a' \in I$, there are positive integers i and i' such that $a \in I_i$ and $a' \in I_{i'}$. Without loss of generality we can and will assume that $i \le i'$, and so $I_i \subseteq I_{i'}$. Therefore $a, a' \in I_{i'}$. Hence $a - a' \in I_{i'}$, which implies that $a - a' \in I$.

For every $a \in I$, there is a positive integer i such that $a \in I_i$. Hence for every $r \in A$, we have that $ra \in I_i$, which implies that $ra \in I$. This completes the proof of the claim that I is an ideal.

Since I is an ideal, it is finitely generated. Hence there are $a_1, \ldots, a_n \in I$ such that $I = \langle a_1, \ldots, a_n\rangle$. Notice that $a_i \in I$ implies that $a_i \in I_{k_i}$ for some positive integer n_i. Suppose $m := \max\{k_1, \ldots, k_n\}$. Then I_m contains I_{k_i} for every i. Therefore $a_1, \ldots, a_n \in I_m$. This implies that

$$\langle a_1, \ldots, a_n\rangle \subseteq I_m.$$

Hence for every $j \ge m$, we have

$$I_j \subseteq \bigcup_{i=1}^{\infty} I_i = \langle a_1, \ldots, a_n\rangle \subseteq I_m \subseteq I_j. \tag{12.3}$$

By (12.3), we obtain that $I_m = I_j$ for every $j \ge m$. This means that A is Noetherian. □

We immediately deduce that a PID is Noetherian, and so every non-zero non-unit element can be factored into irreducible elements.

Corollary 12.3.6. *Suppose D is a PID. Then D is Noetherian and every non-zero non-unit element of D can be written as a product of irreducible elements.*

Proof. Since D is a PID, every ideal is principal. Hence every ideal is finitely generated. Therefore by Lemma 12.3.5, D is Noetherian. By Proposition 12.3.4, we obtain that every non-zero non-unit element of D can be written as a product of irreducible elements. □

Chapter 13

Lecture 13

In the previous lecture we said an integral domain is called a unique factorization domain if every non-zero non-unit element can written as a product of irreducible elements (the existence part) and the irreducible factors are unique up to reordering and multiplying by units (the uniqueness part). We showed that the existence part holds in a Noetherian integral domain (see Proposition 12.3.4 together with Lemma 12.3.5). Today we will investigate the uniqueness part.

13.1 Factorization: uniqueness, and prime elements.

Let's first formulate what the *uniqueness* precisely means: suppose $p_1, \ldots, p_m$ and $q_1, \ldots, q_n$ are irreducible elements of D. If

$$p_1 \cdots p_m = q_1 \cdots q_n, \tag{13.1}$$

then $p_1 = u_1 q_{i_1}$, $p_2 = u_2 q_{i_2}$, and so on, for some $u_i \in D^\times$ and a permutation $1 \mapsto i_1, \ldots, m \mapsto i_m$ of $1, 2, \ldots, n$; in particular $m = n$. This means we need to show if an irreducible element p divides a product of irreducible elements q_i's, then $p = uq_j$ for some unit u and some index j. This takes us to the definition of *prime* elements.

Definition 13.1.1. *Suppose D is an integral domain.*

1. *For $a, b \in D$, we say a divides b and write $a|b$ if there is $d \in D$ such that $b = ad$*

2. *A non-zero non-unit element p of D is called* prime *when for every $a, b \in D$, if $p|ab$, then either $p|a$ or $p|b$.*

Base on the above discussion, for uniqueness to hold, we need to have that every irreducible element is prime. Next we show this statement and its converse hold.

Proposition 13.1.2. *Let D be an integral domain. Suppose every non-zero non-unit element of D can be written as a product of irreducible elements. Then D is a UFD if and only if every irreducible element is prime.*

The formal proof has many little details that make the proof a bit hard to digest. The idea of proof, however, is rather simple. For that reason first I write an outline of the proof:

Outline of proof. ($\Rightarrow$) Suppose p is irreducible and $p|ab$. Then $ab = pd$ for some $d \in D$. We decompose a, b, and d into irreducible factors. We notice that p is an irreducible factor of the left hand side, and so by the uniqueness of irreducible factors, it should be an irreducible factor of either a or b. This means that either $p|a$ or $p|b$.

($\Leftarrow$) The existence part is given as an assumption. So we focus on the uniqueness part. Starting with $p_1 \cdots p_m = q_1 \cdots q_n$, using the assumption that p_1 is prime, we can find an index i_1 such that $p_1|q_{i_1}$. As q_{i_1} is irreducible, we can deduce that p_1 is q_{i_1} upto multiplying by a unit. Now we cancel out p_1 and continue by induction on the number of involved irreducible factors.

Proof. ($\Rightarrow$) Suppose p is an irreducible element. We have to show that p is prime. Since p is irreducible, it is not either zero or unit. Now suppose for $a, b \in D$, $p|ab$. Notice that if either $a = 0$ or $b = 0$, we are done as $p|0$. So without loss of generality we can and will assume that a and b are non-zero. By the assumption either a is a unit or it can be written as product of irreducible elements. A similar statement holds for b. Suppose $a = uq_1 \cdots q_m$ and $b = u'q_{m+1} \cdots q_n$ for irreducible elements $q_1, \ldots, q_n$ and units u, u'. Then $p|(uu' \prod_{i=1}^n q_i)$. This means there is $d \in D$ such that $pd = uu' \prod_{i=1}^n q_i$. Notice that the right hand side of this equation cannot be zero, and so $d \neq 0$. Therefore $d = u''\ell_1 \cdots \ell_k$ for some irreducible elements $\ell_1, \ldots, \ell_k$ and a unit u''. Hence

$$u''p\ell_1 \cdots \ell_k = uu'q_1 \cdots q_n. \tag{13.2}$$

Since p is not a unit, the right hand side of Equation 13.2 cannot be a unit. Therefore $n \geq 1$. As p and q_1 are irreducible, so are $u''p$ and $uu'q_1$. By the assumption the irreducible elements $u''p, \ell_1, \cdots, \ell_k$ are the same as $uu'q_1, \ldots, q_n$ upto reordering and multiplying by units. Hence there is a unit $\overline{u}$ and an index j such that

$$p = \overline{u}q_j. \tag{13.3}$$

Notice that, if $j \leq m$, then $\overline{u}q_j|a$, and if $j > m$, then $\overline{u}q_j|b$. Therefore by (13.3), we obtain that either $p|a$ or $p|b$. This shows that p is prime.

($\Leftarrow$) By the assumption every non-zero non-unit element can be written as a product of irreducible elements. So we focus on the uniqueness part. Suppose $p_1, \ldots, p_m$ and $q_1, \ldots, q_n$ are irreducible elements and

$$p_1 \cdots p_m = q_1 \cdots q_n. \tag{13.4}$$

We have to show that $m = n$, there is a reordering $i_1, \ldots, i_m$ of $1, \ldots, m$, and units u_j such that $p_j = u_j q_{i_j}$ for every j.

We proceed by induction on n. By (13.4), we have that p_1 divides $q_1 \cdots q_n$. Since every irreducible element is prime, p_1 is prime. Whenever a prime element divides product of certain elements, it should divide one of them. Hence there is an index i_1 such that $p_1|q_{i_1}$. This means $q_{i_1} = p_1 u_1$ for some $u_1 \in D$. Since q_{i_1} is irreducible, either p_1 is a unit or u_1 is a unit. As p_1 is irreducible, it is not a unit. Hence u_1 is a unit. Overall we showed that there are an index i_1 and a unit u_1 such that $q_{i_1} = u_1 p_1$. This implies that

$$p_1 \cdots p_m = u_1 p_1 q_1 \cdots q_{i_1-1} q_{i_1+1} \cdots q_n,$$

and so by the cancellation law, we obtain

$$p_2 \cdots p_m = u_1 q_1 \cdots q_{i_1-1} q_{i_1+1} \cdots q_n. \tag{13.5}$$

If $m = 1$, the left hand side is 1. Hence all the terms in the right hand side are units. This means $n = 1$, and we are done. For $m \geq 2$, the left hand side is not a unit, and so $n \neq 1$. Hence there is q_{j_0} factor in the right hand side of (13.5). Then $u_1 q_{j_0}$ is also irreducible. By the induction hypothesis, we deduce that $m - 1 = n - 1$, and there are a reordering $i_2, \ldots, i_m$ of $1, \ldots, i_1 - 1, i_1 + 1, \ldots, m$, and units u_j for every index $j \in [2, m]$ such that $q_{i_j} = u_j p_j$. This finishes the proof. □

13.2 Prime elements and prime ideals

In this section we investigate prime elements. We have seen that in an integral domain an element p is irreducible if and only if the ideal generated by p is maximal among proper principal ideals (see Lemma 9.2.7). As we want to understand the connection between prime and irreducible elements, we study properties of the principal ideals that generated by prime elements. By the definition, p is a prime element of an integral domain D if (1) p is not either zero or unit, and (2) for every $a, b \in D$, if $p|ab$, then either $p|a$ or $p|b$. We start with translating the concept of divisibility to the language of ideals.

Lemma 13.2.1. *Suppose D is an integral domain, and $a, b \in D$.*

1. *$a|b$ if and only if $b \in \langle a \rangle$ if and only if $\langle b \rangle \subseteq \langle a \rangle$.*
2. *$a|b$ and $b|a$ if and only if $a = bu$ for some unit u.*

Proof. We have that $a|b$ if and only if $b = ac$ for some $c \in D$. Since

$$\langle a \rangle = \{ar \mid r \in D\}$$

(see Lemma 5.2.3), the claim follows.

By the first part, we have $a|b$ and $b|a$ if and only if $\langle a \rangle = \langle b \rangle$. The latter happens if and only if $a = bu$ for some unit u (see Lemma 9.2.4). □

By Lemma 13.2.1, we have that $p \in D$ is prime if and only if (1) $\langle p \rangle$ is a non-zero proper ideal (see Lemma 9.2.5) and (2) if $ab \in \langle p \rangle$, then either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. This takes us to the definition of prime ideals.

Definition 13.2.2. *Suppose A is a unital commutative ring and I is an ideal of A. we say I is a prime ideal if (1) I is proper (that means $I \neq A$), and (2) if $ab \in I$ for some $a, b \in D$, then either $a \in I$ or $b \in I$.*

Hence we immediately deduce the following interpretation of prime elements in the language of principal ideals:

Lemma 13.2.3. *Suppose D is an integral domain and $p \in D$. Then p is a prime element if and only if $p \neq 0$ and $\langle p \rangle$ is a prime ideal.*

We have seen that an ideal I in a unital commutative ring is maximal if and only if the quotient ring A/I is a field (see Proposition9.3.3). Next we understand when an ideal is prime in terms of the corresponding quotient ring.

Lemma 13.2.4. *Suppose A is a unital commutative ring and I is an ideal of A. Then I is a prime ideal if and only if A/I is an integral domain.*

Proof. ($\Rightarrow$) Since I is a proper ideal, A/I is a non-trivial ring. Next we show that A/I does not have a zero-divisor. Suppose $(a+I)(b+I) = 0+I$ for some $a, b \in A$. This means that $ab \in I$. As I is a prime ideal, either $a \in I$ or $b \in I$. From this we deduce that either $a+I = 0+I$ or $b+I = 0+I$. Hence A/I is an integral domain.

($\Leftarrow$) Since A/I is an integral domain, A/I is a non-trivial ring. Therefore I is a proper ideal. Now suppose $ab \in I$. Then $(a+I)(b+I) = 0+I$. Since A/I is an integral domain, we have that either $a+I = 0+I$ or $b+I = 0+I$. Hence either $a \in I$ or $b \in I$. Altogether, we deduce that I is a prime ideal. □

We immediately obtain that every maximal ideal is prime.

Corollary 13.2.5. *Suppose A is a unital commutative ring and I is an ideal of A. If I is a maximal ideal, then I is a prime ideal.*

Proof. Suppose I is a maximal ideal. Then A/I is a field (see Proposition 9.3.3). Hence A/I is an integral domain, which implies that I is a prime ideal (by Lemma 13.2.4). □

13.3 Prime vs irreducible

Next we investigate the connections between prime and irreducible elements. In view of Proposition 13.1.2, such a connection can help us prove that certain integral domains are UFD.

Lemma 13.3.1. *Suppose D is a PID. Then every irreducible element of D is prime.*

Proof. Suppose p is irreducible in D. Then by Lemma 9.3.2, $\langle p \rangle$ is a maximal ideal of D. Therefore by Corollary 13.2.5, $\langle p \rangle$ is a prime ideal. Since $p \neq 0$ (as p is irreducible) and $\langle p \rangle$ is a prime ideal, by Lemma 13.2.3 we deduce that p is a prime element. □

The converse of Lemma 13.3.1 is true in every integral domain.

Lemma 13.3.2. *Suppose D is an integral domain and $p \in D$. If p is a prime element, then p is irreducible.*

Proof. Since p is prime, it is not either zero or unit. Hence to show it is irreducible, we have to argue why $p = ab$ implies that either a is a unit or b is a unit.

For $a, b \in D$ suppose $p = ab$. Since p is prime and $p|ab$, we deduce that either $p|a$ or $p|b$. This means that either $a = pa'$ for some $a' \in D$ or $b = pb'$ for some $b' \in D$. In the former case, we have

$$a = pa' = aba' \text{ which implies that } ba' = 1. \tag{13.6}$$

(Notice that since p is prime, it is not zero. Hence a and b are not zero, and so we are allowed to use the cancellation law.) By (13.6), we obtain that b is a unit. Similarly we can show that $b = pb'$ implies that a is a unit. Altogether we have that $p = ab$ implies that either a is a unit or b is unit. This completes this proof. □

An immediate consequence of the above lemmas is the following theorem.

Theorem 13.3.3. *Suppose D is a PID. Then*

1. *An element $d \in D$ is irreducible if and only if it is prime.*

2. *D is a UFD.*

Proof. Since D is an integral domain, by Lemma 13.3.2 every prime is irreducible. Since D is a PID, by Lemma 13.3.1 every irreducible is prime.

The existence part of being a UFD follows from Corollary 12.3.6. The Uniqueness part of being a UFD follows from the first part and Proposition 13.1.2. □

As a corollary we deduce the following:

Theorem 13.3.4. *The following rings are UFD: $\mathbb{Z}$, $F[x]$ where F is a field, $\mathbb{Z}[i]$, and $\mathbb{Z}[\omega]$ where $\omega := \frac{-1+\sqrt{-3}}{2}$.*

Proof. We have proved that all of these rings are Euclidean domains. This implies that they are PIDs. Hence they are UFDs. □

13.4 Some integral domains that are not UFD.

We have seen some interesting examples that are UFDs. Now we want to see that there are many interesting integral domains that are not UFDs.

Example 13.4.1. *The ring $\mathbb{Z}[\sqrt{-6}] := \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$ is not a UFD.*

Proof. By Proposition 13.1.2, it is enough to find an irreducible element which is not a prime element. To show an element is irreducible, first we have to prove it is not a unit. Therefore we have to describe units of this ring. Let

$$N : \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}, \quad N(z) := |z|^2.$$

Notice that $N(z_1 z_2) = N(z_1)N(z_2)$ for every $z_1, z_2 \in \mathbb{Z}[\sqrt{-6}]$.

Claim 1. $z \in \mathbb{Z}[\sqrt{-6}]$ *is a unit if and only if* $N(z) = 1$.

Proof of Claim 1. ($\Rightarrow$) Since $z \in \mathbb{Z}[\sqrt{-6}]^\times$, there is $z' \in \mathbb{Z}[\sqrt{-6}]$ such that $zz' = 1$. Hence

$$N(zz') = 1 \text{ which implies that } N(z)N(z') = 1.$$

Therefore $N(z) \in \mathbb{Z}^\times = \{\pm 1\}$. Since $N(z)$ is non-negative, we deduce that $N(z) = 1$.

($\Leftarrow$) Suppose $N(z) = 1$. and $x = a + b\sqrt{-6}$. Then

$$(a + b\sqrt{6})(a - b\sqrt{6}) = 1,$$

which implies that $x = a + b\sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]^\times$ as $a - b\sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$. This completes the proof of Claim 1.

Claim 2. *$\sqrt{-6}$ is irreducible in $\mathbb{Z}[\sqrt{-6}]$.*

Proof of Claim 2. Since $N(\sqrt{-6}) = 6 \neq 1$, by Claim 1, $\sqrt{-6}$ is not a unit. Now suppose $\sqrt{-6} = xy$ for some $x, y \in \mathbb{Z}[\sqrt{-6}]$. Then

$$N(\sqrt{-6}) = N(xy) \text{ which implies that } 6 = N(x)N(y). \tag{13.7}$$

If neither x nor y are units, by Claim 1 and (13.7) we have that either $N(x) = 2$ or $N(y) = 2$. This means the next claim completes the proof of Claim 2.

Claim 3. *There is no $x \in \mathbb{Z}[\sqrt{-6}]$ such that $N(x) = 2$.*

Proof of Claim 3. Suppose $N(a + b\sqrt{-6}) = 2$ for some $a, b \in \mathbb{Z}$. Then

$$a^2 + 6b^2 = 2. \tag{13.8}$$

If $b \neq 0$, then $6b^2 \geq 6$. This implies that $a^2 + 6b^2 \geq 6$, which means (13.8) cannot hold. Hence $b = 0$, in which case (13.8) implies that $b^2 = 2$, which is not possible as $\sqrt{2}$ is irrational.

Claim 4. *$\sqrt{-6}$ is not prime in $\mathbb{Z}[\sqrt{-6}]$.*

Proof of Claim 4. Suppose to the contrary that $\sqrt{-6}$ is prime. Then $\sqrt{-6}|2 \times 3$ implies that either $\sqrt{-6}|2$ or $\sqrt{-6}|3$. This means there is $z \in \mathbb{Z}[\sqrt{-6}]$ such that either $z\sqrt{-6} = 2$ or $z\sqrt{-6} = 3$. Comparing the norms of both sides, we obtain that either $6N(z) = 4$ or $6N(z) = 9$. This is a contradiction as $6 \nmid 4$ and $6 \nmid 9$.

Altogether, we found an irreducible element which is not prime, and so $\mathbb{Z}[\sqrt{-6}]$ is not a UFD. □

Chapter 14

Lecture 14

We have proved that

$$\text{Euclidean Domain} \quad \Rightarrow \quad \text{PID} \quad \Rightarrow \quad \text{UFD.}$$

We have also showed a method to works with rings of the form $\mathbb{Z}[\alpha]$ where α is a zero of a monic integer quadratic polynomial. We argued how using a norm function sometimes we can find elements that are irreducible but not prime, and deduce that the given integral domain is not a UFD.

14.1 Ring of integer polynomials is a UFD.

Next we show that $\mathbb{Z}[x]$ is a UFD. Remember that this is not a PID as the ideal $\langle 2, x\rangle$ is not a principal ideal of $\mathbb{Z}[x]$.

Theorem 14.1.1. *The ring $\mathbb{Z}[x]$ is a UFD.*

There are three main ingredients in the proof:

1. $\mathbb{Z}$ is a UFD,
2. $\mathbb{Q}[x]$ is a UFD, and
3. Irreducibility of a polynomial in $\mathbb{Q}[x]$ is equivalent to the irreducibility of the primitive form the polynomial in $\mathbb{Z}[x]$ (Gauss's lemma).

Lemma 14.1.2. *Suppose $c \in \mathbb{Z}$. Then we have that*

1. *c is irreducible in $\mathbb{Z}$ if and only if it is irreducible in $\mathbb{Z}[x]$.*
2. *c is prime in $\mathbb{Z}$ if and only if it is prime in $\mathbb{Z}[x]$.*

Proof. (1) ($\Rightarrow$) Since c is irreducible in $\mathbb{Z}$, it is not 0 or ± 1. As $\mathbb{Z}[x]^{\times} = \{\pm 1\}$, we deduce that c is not zero or a unit in $\mathbb{Z}[x]$. Now suppose $c = f(x)g(x)$. Comparing the degrees of both sides, we deduce that $f(x) = a \in \mathbb{Z}$ and $g(x) = b \in \mathbb{Z}$. As c is irreducible in $\mathbb{Z}$, $c = ab$ implies that either $a = \pm 1$ or $b = \pm 1$. Therefore either $f(x)$ is a unit or $g(x)$ is a unit. This means c is irreducible in $\mathbb{Z}[x]$.

($\Leftarrow$) As c is irreducible in $\mathbb{Z}[x]$, c is not zero or ± 1. Hence c is a non-zero non-unit element of $\mathbb{Z}$. Suppose $c = ab$ for some $a, b \in \mathbb{Z}$. Then either $a \in \mathbb{Z}[x]^\times$ or $b \in \mathbb{Z}[x]^\times$. Since $\mathbb{Z}[x]^\times = \mathbb{Z}^\times$, we deduce that either $a \in \mathbb{Z}^\times$ or $b \in \mathbb{Z}^\times$. Hence c is irreducible in $\mathbb{Z}$.

(2) ($\Rightarrow$) Suppose $c|f(x)g(x)$ for some $f, g \in \mathbb{Z}[x]$. Then there is $q(x) \in \mathbb{Z}[x]$ such that $cq(x) = f(x)g(x)$. Hence $|c|\alpha(q) = \alpha(f)\alpha(g)$, which implies that $c|\alpha(f)\alpha(g)$. Since c is prime in $\mathbb{Z}$, we have that either $c|\alpha(f)$ or $c|\alpha(g)$. As $\alpha(f)|f(x)$ and $\alpha(g)|g(x)$ in $\mathbb{Z}[x]$, we deduce that either $c|f(x)$ or $c|g(x)$.

($\Leftarrow$) Suppose $c|ab$ for some integers a and b. Viewing a and b as constant polynomials, as c is prime in $\mathbb{Z}[x]$, we deduce that either $c|a$ or $c|b$ in $\mathbb{Z}[x]$. This means for some $f(x) \in \mathbb{Z}[x]$ we have that either $cf(x) = a$ or $cf(x) = b$. Comparing the degrees, we deduce that $f(x) \in \mathbb{Z}$. Hence $c|a$ or $c|b$ in $\mathbb{Z}$. This means c is prime in $\mathbb{Z}$. □

Next we show that the primitive form $\overline{f}(x)$ of a polynomial $f(x)$ in $\mathbb{Q}[x]$ captures the divisibility properties of $f(x)$ in $\mathbb{Q}[x]$.

Let's recall that for every non-zero polynomial $f(x) \in \mathbb{Q}[x]$, there is a unique primitive polynomial $\overline{f}(x) \in \mathbb{Z}[x]$ such that $f(x) = \alpha(f)\overline{f}(x)$ where $\alpha(f) \in \mathbb{Q}^\times$ is the content of f.

Proposition 14.1.3. *Suppose $f, g \in \mathbb{Q}[x]$ are two non-zero polynomials, and $\overline{f}(x), \overline{g}(x) \in \mathbb{Z}[x]$ are their primitive forms, respectively.*

1. *We have that $f \in \mathbb{Q}[x]^\times$ if and only if $\overline{f}(x) \in \mathbb{Z}[x]^\times$.*
2. *We have that $f|g$ in $\mathbb{Q}[x]$ if and only if $\overline{f}|\overline{g}$ in $\mathbb{Z}[x]$.*
3. *We have that f is irreducible in $\mathbb{Q}[x]$ if and only if $\overline{f}$ is irreducible in $\mathbb{Z}[x]$.*
4. *We have that f is prime in $\mathbb{Q}[x]$ if and only if $\overline{f}$ is prime in $\mathbb{Z}[x]$.*

Proof. (1) $f(x) \in \mathbb{Q}[x]^\times$ if and only if $f(x) = c \in \mathbb{Q}^\times$. The latter occurs if and only if $f(x) = \pm\alpha(f)$. Notice that $f(x) = \pm\alpha(f)$ precisely when $\overline{f}(x) = \pm 1$. Altogether we have that $f(x) \in \mathbb{Q}[x]^\times$ if and only if $\overline{f}(x) \in \mathbb{Z}[x]^\times$.

(2) ($\Rightarrow$) Since $f(x)|g(x)$ in $\mathbb{Q}[x]$, there is a polynomial $q(x) \in \mathbb{Q}[x]$ such that $g(x) = f(x)q(x)$. Let $\overline{q}(x)$ be the primitive form of $q(x)$. Then

$$\alpha(g)\overline{g}(x) = \alpha(f)\overline{f}(x)\alpha(q)\overline{q}(x). \tag{14.1}$$

By Gauss's lemma, we have

$$\alpha(g) = \alpha(f)\alpha(q) = \alpha(q). \tag{14.2}$$

By (14.1) and (14.2), we deduce that $\overline{g}(x) = \overline{f}(x)\overline{q}(x)$, which implies that $\overline{f}|\overline{g}$ in $\mathbb{Z}[x]$.

($\Leftarrow$) Since $\overline{f}|\overline{g}$ in $\mathbb{Z}[x]$, there is a polynomial $h(x) \in \mathbb{Z}[x]$ such that $\overline{g}(x) = \overline{f}(x)h(x)$. Hence

$$g(x) = \alpha(g)\overline{g}(x) = \alpha(g)\overline{f}(x)h(x) = \underbrace{(\alpha(g)\alpha(f)^{-1}h(x))}_{\text{is in } \mathbb{Q}[x]} f(x),$$

which implies that $f(x)|g(x)$ in $\mathbb{Q}[x]$.

(3) Since $f(x) = \alpha(f)\overline{f}(x)$ and $\alpha(f) \in \mathbb{Q}[x]^\times$, $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $\overline{f}(x)$ is irreducible in $\mathbb{Q}[x]$. By part (1) we can assume that $\deg f \geq 1$. By Corollary 11.3.2, we have that $\overline{f}(x)$ is irreducible in $\mathbb{Q}[x]$ precisely when it is irreducible in $\mathbb{Z}[x]$. This finishes the proof.

(4) ($\Rightarrow$) Suppose $\overline{f}|h_1(x)h_2(x)$ for some $h_1, h_2 \in \mathbb{Z}[x]$. This means that there is $q(x) \in \mathbb{Z}[x]$ such that $h_1(x)h_2(x) = \overline{f}(x)q(x) = (\alpha(f)^{-1}q(x))f(x)$. Hence $f(x)|h_1(x)h_2(x)$ in $\mathbb{Q}[x]$. Since f is prime in $\mathbb{Q}[x]$, we deduce that either $f(x)|h_1(x)$ in $\mathbb{Q}[x]$ or $f(x)|h_2(x)$ in $\mathbb{Q}[x]$. By part (2), we have that either $\overline{f}|\overline{h}_1$ in $\mathbb{Z}[x]$ or $\overline{f}|\overline{h}_2$ in $\mathbb{Z}[x]$. Notice that $\overline{h}_i|h_i$ in $\mathbb{Z}[x]$. Altogether we obtain that either $\overline{f}|h_1$ in $\mathbb{Z}[x]$ or $\overline{f}|h_2$. This means that $\overline{f}$ is prime in $\mathbb{Z}[x]$.

($\Leftarrow$) Suppose $f|g_1g_2$ for some $g_1, g_2 \in \mathbb{Q}[x]$. By part (2), we deduce that $\overline{f}$ divides the primitive form of g_1g_2 in $\mathbb{Z}[x]$. By Gauss's lemma, we have that the primitive form of g_1g_2 is the product of the primitive forms of g_1 and g_2. Hence $\overline{f}|\overline{g}_1\overline{g}_2$ in $\mathbb{Z}[x]$. Since $\overline{f}$ is prime in $\mathbb{Z}[x]$, either $\overline{f}|\overline{g}_1$ in $\mathbb{Z}[x]$ or $\overline{f}|\overline{g}_2$ in $\mathbb{Z}[x]$. Another application of part (2) implies that either $f|g_1$ in $\mathbb{Q}[x]$ or $f|g_2$ in $\mathbb{Q}[x]$. This means that f is prime in $\mathbb{Q}[x]$. □

Proof of Theorem 14.1.1. **Existence part.** Suppose $f(x) \in \mathbb{Z}[x]$ is a non-zero non-unit polynomial. We have to show that we can write $f(x)$ as a product of irreducible elements. If $f(x)$ is a constant function, then $f(x) = a \in \mathbb{Z}$. As $\mathbb{Z}$ is a UFD, a can be written as a product of irreducible elements of $\mathbb{Z}$. By Lemma 14.1.2, irreducible elements of $\mathbb{Z}$ are also irreducible in $\mathbb{Z}[x]$. Hence $f(x)$ can be written as a product of irreducible elements of $\mathbb{Z}[x]$.

Next we assume that $f(x)$ is not a constant polynomial and consider its primitive form $\overline{f}(x)$. Hence $f(x) = \alpha(f)\overline{f}(x)$, where $\alpha(f)$ is the content of f. Notice that $\alpha(f) \in \mathbb{Z}$ can be viewed as a constant polynomial, and so it can be written as a product of irreducible elements of $\mathbb{Z}[x]$ (unless it is 1). Next we view $\overline{f}(x)$ as a non-constant polynomial in $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a UFD, $\overline{f}(x)$ can be written as a product of irreducible elements of $\mathbb{Q}[x]$. Say $p_i(x) \in \mathbb{Q}[x]$ are irreducible and $\overline{f}(x) = \prod_{i=1}^n p_i(x)$. Suppose $\overline{p}_i(x)$ is the primitive form of $p_i(x)$. By Theorem 11.3.1, we have

$$\overline{f}(x) = \prod_{i=1}^{n} \overline{p}_i(x). \tag{14.3}$$

By Proposition 14.1.3, part (3), we have that $\overline{p}_i$'s are irreducible in $\mathbb{Z}[x]$.

Altogether we end up getting a factorization of $f(x)$ into irreducible elements of $\mathbb{Z}[x]$.

Uniqueness part. By Proposition 13.1.2, it is sufficient to show that every irreducible element of $\mathbb{Z}[x]$ is prime. Suppose $f(x) \in \mathbb{Z}[x]$ is irreducible. The decomposition $f(x) = \alpha(f)\overline{f}(x)$ implies that either $f(x)$ is a constant polynomial or it is primitive and $f(x) = \overline{f}(x)$.

Case 1. *$f(x) = a$ is constant.*

By Lemma 14.1.2, part (1), a is irreducible in $\mathbb{Z}$. Since $\mathbb{Z}$ is a UFD, a is prime in $\mathbb{Z}$. Hence by Lemma 14.1.2, part (2), $f(x) = a$ is prime in $\mathbb{Z}[x]$.

Case 2. *$f(x) = \overline{f}(x)$ is primitive.*

Since $\overline{f}(x)$ is irreducible in $\mathbb{Z}[x]$, by Proposition 14.1.3 part (3), $f(x)$ is irreducible in $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a UFD and $f(x)$ is irreducible in $\mathbb{Q}[x]$, $f(x)$ is prime in $\mathbb{Q}[x]$. By Proposition 14.1.3 part (4), $\overline{f}$ is prime in $\mathbb{Z}[x]$. This means $f(x) = \overline{f}(x)$ is prime in $\mathbb{Z}[x]$, which finishes the proof. □

Theorem 14.1.1 is a special case of the following theorem:

Theorem 14.1.4. *Suppose D is a UFD. Then $D[x]$ is a UFD.*

Going through the main ingredients of the above proof, we notice that we have to use the field of fractions $F := Q(D)$ of D. As $F[x]$ is a PID, we know that it is a UFD. So if we manage to define a *primitive* form of a non-zero polynomial $Q(D)[x]$ with properties as in Proposition 14.1.3, we can go through the above proof and show that Theorem 14.1.4 holds.

To define a primitive form of polynomials in $Q(D)[x]$, following the case of integer polynomials, we need to define *the greatest common divisor* of finitely many elements of a UFD D.

Proposition 14.1.5. *Suppose D is a UFD. Then for non-zero elements $a_1, \ldots, a_n$ there is $d \in D$ with the following properties:*

1. *$d|a_1, \ldots, d|a_n$.*
2. *If $d'|a_1, \ldots, d'|a_n$, then $d'|d$.*

If d_1 and d_2 satisfy the above properties, then $d_1 = ud_2$ for some $u \in D^\times$.

An element $d \in D$ which satisfies the above properties is called a greatest common divisor *of $a_1, \ldots, a_n$.*

Chapter 15

Lecture 15

In the previous lecture we proved that $\mathbb{Z}[x]$ is a UFD, and mentioned that in general $D[x]$ is a UFD if D is a UFD. We pointed out the missing ingredient in proving this general statement is a generalization of Gauss's lemma in the context of UFDs. In order to formulate this general form, we need to know what *greatest common divisor* mean in a UFD.

15.1 Valuations and greatest common divisors in a UFD

We prove the following result and use it to define a greatest common divisor of finitely many elements of a UFD.

Proposition 15.1.1. *Suppose D is a UFD. Then for non-zero elements $a_1, \ldots, a_n$ there is $d \in D$ with the following properties:*

1. $d|a_1, \ldots, d|a_n$.

2. *If $d'|a_1, \ldots, d'|a_n$, then $d'|d$.*

If d_1 and d_2 satisfy the above properties, then $d_1 = ud_2$ for some $u \in D^{\times}$.

An element $d \in D$ which satisfies the above properties is called a greatest common divisor *of $a_1, \ldots, a_n$.*

We start by recalling that in a UFD every non-zero non-unit element can be written as a product of irreducible factors and these irreducible factors are unique up to a *multiplication by a unit*. In order to avoid the need for multiplication by a unit, we fix a subset $\mathscr{P}_D$ of irreducible elements of D with the following properties:

1. Every element of $\mathscr{P}_D$ is irreducible.

2. For every irreducible element p of D, there is a unique element $\overline{p} \in \mathscr{P}_D$ such that $p = u\overline{p}$ for some unit u.

Let's recall that $p = u\overline{p}$ for some unit u precisely when $\langle p \rangle = \langle \overline{p} \rangle$. We also notice that in a UFD and element p is irreducible if and only if it is prime. The latter holds exactly when p is prime. An element p is prime if and only if $\langle p\rangle$ is a prime ideal. Altogether, we obtain that there is a bijection between $\mathscr{P}_D$ and the set of non-zero principal prime ideals of D. Notice that there are many choices for such a set. Here we fix one such set and many of the functions that will be defined later depend on this choice.

Since D is a UFD, for every $a \in D \setminus \{0\}$, there are unique $u_a \in D^\times$ and non-negative integers n_p such that

$$a = u_a \prod_{p\in\mathscr{P}_D} p^{n_p}.$$

We use the following functions to refer these values. Let $\sigma : D \setminus \{0\} \to D^\times$ and $v_p : D \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ be such that for every $a \in D \setminus \{0\}$ the following holds

$$a = \sigma(a) \prod_{p\in\mathscr{P}_D} p^{v_p(a)}.$$

This means $v_p(a)$ is the power of p in the factorization of a with respect to the prime factors $\mathscr{P}_D$. Notice that every $a \in D \setminus \{0\}$ has only finitely many irreducible factors. This means only finitely many $v_p(a)$'s are non-zero for $p \in \mathscr{P}_D$. Therefore this product has finitely many terms (the rest are 1).

To understand the function σ better, let's go over the case of ring of integers. The classical convention in the definition of a prime number is slightly different from the way we have defined prime elements of $\mathbb{Z}$. The subtle difference is that in the classical setting a prime number must be *positive*, but in the modern language, say, -2 is also considered a prime element of the ring of integers. In a sense the classical convention factors integers with respect to

$$\mathscr{P}_{\mathbb{Z}} = \{p \in \mathbb{Z} \mid p \text{ is a positive prime element of the ring } \mathbb{Z}\}.$$

With this choice, $\sigma(a)$ is precisely the sign of a; that means it is 1 when a is positive, and it is -1 when a is negative. Because of this, even for an arbitrary UFD, we call $\sigma(a)$ the *sign* of a. Inspired with the case of $D = \mathbb{Z}$, we let

$$|a| := \sigma(a)^{-1}a = \prod_{p\in\mathscr{P}_D} p^{v_p(a)}.$$

For every $a \in D \setminus \{0\}$, $v_p(a)$ is called the *p-valuation* of a. Here are basic properties of these functions.

Proposition 15.1.2. *Suppose D is a UFD, $a, b \in D \setminus \{0\}$. Then*

1. *a) $\sigma(ab) = \sigma(a)\sigma(b)$.*

   b) $|ab| = |a||b|$.

   c) $v_p(ab) = v_p(a) + v_p(b)$ for every $p \in \mathscr{P}_D$.

2. *$a|b$ if and only if $v_p(a) \leq v_p(b)$ for every $p \in \mathscr{P}_D$.*

3. *There is $u \in D^\times$ such that $a = ub$ if and only if $v_p(a) = v_p(b)$ for every $p \in \mathscr{P}_D$.*

Proof. (1) By the factorization of a and b with respect to $\mathscr{P}_D$, we have

$$a = \sigma(a) \prod_{p \in \mathscr{P}_D} p^{v_p(a)}, \quad \text{and} \quad b = \sigma(b) \prod_{p \in \mathscr{P}_D} p^{v_p(b)}. \tag{15.1}$$

Multiplying equations given in (15.1), we deduce that

$$ab = (\sigma(a)\sigma(b)) \prod_{p \in \mathscr{P}_D} p^{v_p(a)+v_p(b)}.$$

Notice that since $\sigma(a)$ and $\sigma(b)$ are units, so is $\sigma(a)\sigma(b)$. Hence by the uniqueness of this factorization, we obtain that

$$\sigma(ab) = \sigma(a)\sigma(b) \quad \text{and} \quad v_p(ab) = v_p(a) + v_p(b) \tag{15.2}$$

for every $p \in \mathscr{P}_D$. Hence

$$|ab| = \sigma(ab)^{-1}(ab) = (\sigma(a)^{-1}a)(\sigma(b)^{-1}b) = |a||b|.$$

(2) ($\Rightarrow$) Suppose $a|b$. Then for $d \in D$, we have $b = ad$. Hence for every $p \in \mathscr{P}_D$ we have

$$v_p(b) = v_p(ad) = v_p(a) + v_p(d) \geq v_p(a).$$

($\Leftarrow$) We start with the prime factorizations of a and b (with respect to $\mathscr{P}_D$) $a = \sigma(a) \prod_{p \in \mathscr{P}_D} p^{v_p(a)}$ and $b = \sigma(b) \prod_{p \in \mathscr{P}_D} p^{v_p(b)}$. We want to write b as a multiple of a. This makes us to consider

$$d := \prod_{p \in \mathscr{P}_D} p^{v_p(b)-v_p(a)},$$

and notice that $d \in D$ as $v_p(b) \geq v_p(a)$ and $v_p(b) = v_p(a) = 0$ except for finitely many p's. Hence

$$\begin{aligned} b =& \sigma(b) \prod_{p \in \mathscr{P}_D} p^{v_p(b)} \\ =& \sigma(b) \prod_{p \in \mathscr{P}_D} p^{v_p(b)-v_p(a)} \prod_{p \in \mathscr{P}_D} p^{v_p(a)} \\ =& (\sigma(b) d \sigma(a)^{-1}) a. \end{aligned}$$

This implies that $a|b$ as $\sigma(a)$ is a unit.

(3) By part (2) we have that $v_p(a) = v_p(b)$ for every $p \in \mathscr{P}_D$ exactly when $a|b$ and $b|a$. By Lemma 13.2.1, we have that $a|b$ and $b|a$ holds if and only if $a = bu$ for some unit u. This completes the proof. □

Next we extend these functions to the group $Q(D)^{\times}$ of units of the field of fractions of D. This is needed as we have to work with the ring of polynomials $Q(D)[x]$ in order to show that $D[x]$ is a UFD.

Proposition 15.1.3 (Basic properties of valuations and the sign function)**.** *Suppose D is a UFD and $Q(D)$ is the field of fractions of D. Then*

1. *The following functions are well-defined group homomorphisms:*

$$\begin{aligned}\sigma :&Q(D)^\times \to D^\times, \quad \sigma\Big(\frac{a}{b}\Big) := \sigma(a)\sigma(b)^{-1}.\\ v_p :&F^\times \to \mathbb{Z}, \quad v_p\Big(\frac{a}{b}\Big) := v_p(a) - v_p(b).\\ |\cdot| :&Q(D)^\times \to Q(D)^\times, \quad \Big|\frac{a}{b}\Big| := \frac{|a|}{|b|}.\end{aligned}$$

2. $\ker|\cdot| = D^\times$ *and* $||q|| = |q|$ *for every* $q \in Q(D)^\times$.

3. *Let* $G(D)$ *be the image of* $|\cdot|$. *Then* $m : D^\times \times G(D) \to Q(D)^\times,\ m(u,q) := uq$ *is a group isomorphism.*

Proof. (1) Here we just check why these functions are well-defined. I leave to you to check why these maps are group homomorphisms.

Suppose $\frac{a}{b} = \frac{c}{d}$ for some $a, b, c, d \in D \setminus \{0\}$. Then $ad = bc$. Applying the functions σ, v_p and σ to the both sides of this equality, by Proposition **??**, we obtain that

$$\sigma(a)\sigma(d) = \sigma(b)\sigma(c), \quad v_p(a) + v_p(d) = v_p(b) + v_p(c), \text{ and } \quad |a||d| = |b||c|$$

Therefore

$$\sigma(a)\sigma(b)^{-1} = \sigma(c)\sigma(d)^{-1}, \quad v_p(a) - v_p(b) = v_p(c) - v_p(d), \text{ and } \quad \frac{|a|}{|b|} = \frac{|b|}{|c|}.$$

This shows that the given functions are well-defined.

(2) $\frac{a}{b}$ is in the kernel of $|\cdot|$ if and only if $|\frac{a}{b}| = 1$. By part (1), the latter holds exactly when $\frac{|a|}{|b|} = 1$. This is equivalent to having $|a| = |b|$. By Proposition **??**, $|a| = |b|$ holds if and only if $a = bu$ for some unit u. Altogether we have that

$$\frac{a}{b} \in \ker|\cdot| \Leftrightarrow \frac{a}{b} = \frac{u}{1}$$

for some $u \in D^\times$. Hence $\ker|\cdot| = D^\times$.

The other claim of Part (2) follows from the definition of $|\cdot|$.

(3) Since $Q(D)^\times$ is abelian, m is a group homomorphism. For every $q \in Q(D)^\times$, we have

$$q = \sigma(q)|q| = m(\sigma(q), |q|)$$

which implies that m is surjective.

Now suppose $(u, q) \in \ker m$. Then $q = u^{-1} \in D^\times \cap G(D)$. Then by Part (2), we have $q = |q| = |u^{-1}| = 1$. This means that $\ker m$ is trivial, and so m is injective. This finishes the proof. □

15.2 Greatest common divisor for UFDs

Using valuations, we can study common divisors of a finite set of non-zero elements of a UFD and prove Proposition 15.1.1.

Proof of Proposition 15.1.1. Suppose $a_1, \ldots, a_n$ are non-zero elements of a UFD D. By Proposition **??**, $b \in D\backslash\{0\}$ is a common divisor of a_i's exactly when $v_p(b) \le v_p(a_i)$ for every index i and every $p \in \mathscr{P}_D$. Hence we have

$$b|a_1, \ldots, b|a_n \Leftrightarrow v_p(b) \le \min\{v_p(a_1), \ldots, v_p(a_n)\} \text{ for every } p \in \mathscr{P}_D. \tag{15.3}$$

Notice that $\min\{v_p(a_1), \ldots, v_p(a_n)\} = 0$ except for finitely many p's, and so

$$d := \prod_{p \in \mathscr{P}_D} p^{\min\{v_p(a_1), \ldots, v_p(a_n)\}}$$

is an element of $G(D) \cap D$. By (15.3), we deduce that

$$b|a_1, \ldots, b|a_n \Leftrightarrow b|d.$$

This shows the existence part of Proposition 15.1.1.

Now suppose d_1 and d_2 satisfy the mentioned properties in Proposition 15.1.1. This means d_i's are common divisors of $a_1, \ldots, a_n$, and every common divisor of $a_1, \ldots, a_n$ is a divisor of d_i's. Therefore $d_1|d_2$ and $d_2|d_1$. Hence by Lemma 13.2.1, there is a unit u such that $d_2 = ud_1$. As d_i's are in $G(D)$, we obtain that $m(1, d_2) = m(u, d_1)$ where m is the group isomorphism given in Part (3) of Proposition 15.1.2. Thus $d_1 = d_2$. This completes the proof. □

The greatest common divisor of $a_1, \ldots, a_n \in D \setminus \{0\}$ is the unique $d \in G(D)$ which is given by Proposition 15.1.1, and from the proof it is clear that

$$\gcd(a_1, \ldots, a_n) := \prod_{p \in \mathscr{P}_D} p^{\min(v_p(a_1), \ldots, v_p(a_n))}. \tag{15.4}$$

Notice that $\gcd$ depends on the choice of $\mathscr{P}_D$, but its value up to a multiplication by a unit is independent of the choice of $\mathscr{P}_D$. Now it is easy to get the following basic properties of the $\gcd$ function, and we leave it as an exercise.

Proposition 15.2.1. *In the above setting, suppose $a_1, \ldots, a_n \in D \setminus \{0\}$. Then*

1. *For every $c \in D \setminus \{0\}$, $\gcd(ca_1, \ldots, ca_n) = |c| \gcd(a_1, \ldots, a_n)$.*
2. *If $\gcd(a_1, \ldots, a_n) = d$, then $\frac{a_i}{d} \in D$ and $\gcd(\frac{a_1}{d}, \ldots, \frac{a_n}{d}) = 1$.*

15.3 Content of polynomials: UFD case

Now we are ready to define the content of $f(x) \in D[x]$ where D is a UFD.

Definition 15.3.1. *Suppose D is a UFD and $f(x) := a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ is a non-zero polynomial. The content of f is*

$$\alpha(f) := \gcd(a_n, a_{n-1}, \ldots, a_0),$$

where gcd *is defined as in* (15.4)*. We say $f(x) \in D[x]$ is* primitive *if $\alpha(f) = 1$.*

By Proposition 15.2.1, we deduce the following properties of the content function.

Lemma 15.3.2. *Suppose D is a UFD, $f, g \in D[x]$ are non-zero polynomials, and $a \in D \setminus \{0\}$. Then*

1. *$\alpha(af) = |a|\alpha(f)$.*
2. *If $\alpha(f) = d$, then $\frac{1}{d} f(x) \in D[x]$ and $\alpha(\frac{1}{d} f(x)) = 1$.*
3. *For $d \in D \setminus \{0\}$, $d|\alpha(f)$ if and only if $c_d(f) = 0$ where $c_d : D[x] \to (D/\langle d \rangle)[x]$ is the natural quotient map.*

By Part (2) of Lemma 15.3.2, every $f(x) \in D[x] \setminus \{0\}$ can be written as $\alpha(f)\overline{f}(x)$ and $\overline{f}(x)$ is a primitive polynomial.

Next we define the content of a non-zero polynomial $f(x) \in Q(D)[x]$ where $Q(D)$ is the field of fractions of D.

Lemma 15.3.3. *Suppose D is a UFD and $Q(D)$ is the field of fractions D. Then for every non-zero polynomial $f \in Q(D)[x]$ there are unique $q \in G(D)$ and primitive polynomial $\overline{f} \in D[x]$ such that $f(x) = q\overline{f}(x)$.*

Proof. (Existence) Suppose $f(x) = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i$ for some $a_i, b_i \in D$. Let $d := \prod_{i=0}^{n} |b_i|$. Then $\widetilde{f}(x) := d\, f(x) \in D[x]$. Then by Lemma 15.3.2, $\widetilde{f}(x) = \alpha(\widetilde{f})\overline{f}(x)$ and $\overline{f}(x)$ is primitive. Hence we have that

$$f(x) = \frac{1}{d}\widetilde{f}(x) = \frac{\alpha(\widetilde{f})}{d}\overline{f}(x).$$

Notice that since $\alpha(\widetilde{f})$ and d are in the image of $|\cdot|$, $\frac{\alpha(\widetilde{f})}{d} \in G(D)$. This shows the existence part.

(Uniqueness) Suppose $q_1, q_2 \in G(D)$, $\overline{f}_1, \overline{f}_2 \in D[x]$ are primitive polynomials, and $q_1\overline{f}_1(x) = q_2\overline{f}_2(x)$. Suppose $q_i := \frac{c_i}{d_i}$ for $i = 1, 2$. Let $d := |d_1||d_2|$; then $dq_i \in D$. Hence $(dq_1)\overline{f}_1(x) = (dq_2)\overline{f}_2(x)$, which implies that

$$\alpha((dq_1)\overline{f}_1(x)) = \alpha((dq_2)\overline{f}_2(x)).$$

Therefore by Part (1) of Lemma 15.3.2, we have $|dq_1| = |dq_2|$. Since $d, q_i \in G(D)$, by Part (2) of Proposition 15.1.2 we have that $|dq_i| = dq_i$. Thus $dq_1 = dq_2$, which implies that $q_1 = q_2$. This in turn gives us that $\overline{f}_1 = \overline{f}_2$, and the uniqueness follows. □

The unique element $q \in G(D)$ given in Lemma 15.3.3 is called the *content* of $f(x)$ and it is denoted by $\alpha(f)$, and the primitive polynomial $\overline{f}(x)$ given in Lemma 15.3.3 is called the *primitive form* of $f(x)$.

15.4 Gauss's lemma for UFDs.

Having the definition of the content of a polynomial in $Q(D)[x]$, we can formulate and prove Gauss's lemma for UFDs.

Lemma 15.4.1. *Suppose D is a UFD, and $f, g \in D[x]$ are primitive. Then fg is primitive.*

Proof. Suppose to the contrary that fg is not primitive. Then there is $p \in \mathscr{P}_D$ which divides $\alpha(fg)$. This means all the coefficients of fg are in $\langle p \rangle$. Therefore $c_p(fg) = 0$ where $c_p : D[x] \to (D/\langle p \rangle)[x]$ is the natural quotient map. Notice that since D is a UFD and p is irreducible, p is a prime element of D. Hence $\langle p \rangle$ is a prime ideal. This implies that $D/\langle p \rangle$ is an integral domain. Thus $(D/\langle p \rangle)[x]$ is also an integral domain. Knowing that $c_p(f)c_p(g) = 0$ and $(D/\langle p \rangle)[x]$ is an integral domain, we obtain that either $c_p(f) = 0$ or $c_p(g) = 0$. This means either $p|\alpha(f)$ or $p|\alpha(g)$, which is a contradiction as $\alpha(f) = \alpha(g) = 1$. □

Lemma 15.4.2. *Suppose D is a UFD. Then for every $f, g \in Q(D)[x] \setminus \{0\}$ we have $\alpha(fg) = \alpha(f)\alpha(g)$.*

Proof. By the definition of the content, we have

$$f(x) = \alpha(f)\overline{f}(x) \quad \text{and} \quad g(x) = \alpha(g)\overline{g}(x) \tag{15.5}$$

and $\overline{f}(x)$ and $\overline{g}(x)$ are primitive polynomials. By (15.5), we obtain that

$$f(x)g(x) = (\alpha(f)\alpha(g))\overline{f}(x)\overline{g}(x). \tag{15.6}$$

By the first version of Gauss's lemma for UFDs, we have that $\overline{f}(x)\overline{g}(x)$ is primitive. Since $\alpha(f), \alpha(g) \in G(D)$, we have $\alpha(f)\alpha(g) \in G(D)$. By (15.6), $\alpha(f)\alpha(g) \in G(D)$, $\overline{f}(x)\overline{g}(x)$ being a primitive polynomial, and the definition of content of a polynomial, we have that $\alpha(fg) = \alpha(f)\alpha(g)$. This completes the proof. □

The following is an immediate consequence of the second version of Gauss's lemma for UFDs.

Corollary 15.4.3. *Let* $\operatorname{prim} : Q(D)[x] \setminus \{0\} \to D[x] \setminus \{0\}, \operatorname{prim}(f)$ *be the primitive form of f. Then*

$$\operatorname{prim}(fg) = \operatorname{prim}(f)\operatorname{prim}(g)$$

for every $f, g \in Q(D)[x] \setminus \{0\}$.

Proof. We have $f = \alpha(f)\operatorname{prim}(f)$, $g = \alpha(g)\operatorname{prim}(g)$, and $fg = \alpha(fg)\operatorname{prim}(fg)$. Hence by the second version of Gauss's lemma for UFDs, we obtain that

$$\operatorname{prim}(fg) = \operatorname{prim}(f)\operatorname{prim}(g).$$

This completes the proof. □

Now we have all the needed tools to redo the proof of why $\mathbb{Z}[x]$ is a UFD and obtain its generalization. I leave it to you to go over the proof and make sure all the arguments go through to prove the following theorem.

Theorem 15.4.4. *If D is a UFD, then $D[x]$ is a UFD.*

By induction, one can easily show the following.

Corollary 15.4.5. *If D is a UFD, then $D[x_1, \dots, x_n]$ is a UFD.*

In particular, we have that $\mathbb{Z}[x_1, \dots, x_n]$ and $F[x_1, \dots, x_n]$ where F is a field, are UFDs.

Chapter 16

Lecture 16

We have used the central problem of understanding zeros of polynomials as our point of reference in exploring algebra. So far we have worked under the assumption that we are given a field extension E of F that contains a zero α of $f(x) \in F[x]$ and among other things proved:

1. There is a unique polynomial $m_{\alpha,F}(x) \in F[x]$ with the following properties:

   a) α is a zero of $g(x) \in F[x]$ if and only if $m_{\alpha,F}(x)|g(x)$.

   b) $p(x) = m_{\alpha,F}(x)$ if and only if $p(x)$ is a monic irreducible element of $F[x]$ and $p(\alpha) = 0$.

2. $F[\alpha] \simeq F[x]/\langle m_{\alpha,F}(x)\rangle$.

3. $F[\alpha]$ is a field.

4. Every element of $F[\alpha]$ can be uniquely written as an F-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ where $n := \deg m_{\alpha,F}(x)$.

Next we want to answer the following questions:

1. For $f(x) \in F[x]$, can we find a field extension E of F that contains a zero of f? Is there a field extension that contains all the zeros of f?

2. Do we have a *canonical choice* for such a field extension? Can we talk about *the smallest* field extension that contains all the zeros of f?

16.1 Existence of a splitting field.

In this section we prove that every polynomial $f(x) \in F[x]$ can be decomposed to linear factors over a field extension.

Proposition 16.1.1. *Suppose F is a field and $f(x) \in F[x]$ is a non-constant polynomial. Then there are a field extension E of F and $\alpha_1, \ldots, \alpha_n$ such that*

1. *$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$, where $a = \mathrm{ld}(f)$ is the leading coefficient of f, and*
2. *$E = F[\alpha_1, \ldots, \alpha_n]$.*

Here $F[\alpha_1, \ldots, \alpha_n]$ is the subring of E that is generated by F and α_i's. By adding α_i's one-by-one, we see that

$$F[\alpha_1, \ldots, \alpha_n] = (F[\alpha_1, \ldots, \alpha_{n-1}])[\alpha_n],$$

and so

$$F[\alpha_1, \ldots, \alpha_n] = \Big\{ \sum_{\mathbf{i}} c_{\mathbf{i}} \alpha_1^{i_1} \cdots \alpha_n^{i_n} \mid c_{\mathbf{i}} \in F, \mathbf{i} = (i_1, \ldots, i_n) \Big\}.$$

A field extension E of F which satisfies the properties of Proposition 16.1.1 is called a *splitting field of $f(x)$ over F.*

To prove this result, we start with finding a single linear factor in a field extension when f is irreducible.

Lemma 16.1.2. *Suppose F is a field and $f(x) \in F[x]$ is an irreducible polynomial. Then there are a field extension E of F and $\alpha \in E$ such that $f(\alpha) = 0$ and $E = F[\alpha]$.*

To find such a field extension, we make a backward argument. If $E = F[\alpha]$, then we have that

$$\theta : F[x]/\langle m_{\alpha,F}(x)\rangle \to E, \theta(g(x) + \langle m_{\alpha,F}(x)\rangle) := g(\alpha)$$

is an isomorphism. Notice that since $f(\alpha) = 0$, $m_{\alpha,F}(x)|f(x)$. As $f(x)$ is irreducible in $F[x]$ and $m_{\alpha,F}(x)|f(x)$, there is $c \in F^{\times}$ such that $f(x) = cm_{\alpha,F}(x)$. This implies that $\langle m_{\alpha,F}(x)\rangle = \langle f(x)\rangle$. Hence there is an isomorphism from $F[x]/\langle f(x)\rangle$ to E which sends $x + \langle f(x)\rangle$ to α. This shows us what we should choose for E and α.

Proof. Let $E := F[x]/\langle f\rangle$. Since F is a field, $F[x]$ is a PID. As $F[x]$ is a PID and $f \in F[x]$ is irreducible, $\langle f\rangle$ is a maximal ideal of $F[x]$. Therefore $F[x]/\langle f\rangle$ is a field.

Next we show that E is a field extension of F. Let $I := \langle f\rangle$, and $i : F \to E, i(c) := c + I$. It is easy to see that i is a ring homomorphism which sends 1_F to 1_E. Thus $\ker i$ is a proper ideal of F. Since 0 is the only proper ideal of a field, we obtain that $\ker i = 0$. This implies that i is injective. Hence E is a field extension of F.

Now we show that $\alpha := x + I \in E$ is a zero of f. In order to evaluate f at α, we have to view the coefficients of F as elements of E. This means we have to work with the copy of F in E. Suppose

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

Then

$$\begin{aligned} f(\alpha) =& i(a_n)\alpha^n + \cdots + i(a_0) \\ =& (a_n + I)(x+I)^n + \cdots + (a_0 + I) \\ =& (a_n x^n + \cdots + a_0) + I \\ =& f(x) + I = 0 + I. \end{aligned}$$

The last equality holds because $f(x) \in I$. Notice that $0 + I$ is the zero of E. Hence $f(\alpha) = 0$.

Finally every element of E is of the form

$$\left(\sum_{j=0}^{m} b_j x^j\right) + I = \sum_{j=0}^{m} i(b_j)\alpha^j \in F[\alpha].$$

Hence $E = F[\alpha]$. This completes the proof. □

Proof of Proposition 16.1.1. We proceed by the strong induction on $\deg f$. We start with the base of induction. Suppose $\deg f = 1$. Then $f(x) = ax + b = a(x + b/a)$. Then $\alpha := -b/a \in F$ is a zero of $f(x)$. Then $E := F$ and $\alpha \in E$ satisfy the properties mentioned in the statement of Proposition 16.1.1. This completes the proof of the base case.

To prove the strong induction step, we consider two cases.

Case 1. f is not irreducible in $F[x]$.

In this case, there are non-constant $g, h \in F[x]$ such that $f(x) = g(x)h(x)$. So $\deg g, \deg h < \deg f$. By the strong induction hypothesis, there are a field extension E_1 of F and $\alpha_1, \ldots, \alpha_m \in E_1$ such that

$$g(x) = b(x - \alpha_1) \cdots (x - \alpha_m) \tag{16.1}$$

where $b = \mathrm{ld}(g)$ and

$$E_1 = F[\alpha_1, \ldots, \alpha_m]. \tag{16.2}$$

Another application of the strong induction hypothesis implies that there are a field extension E of E_1 and $\beta_1, \ldots, \beta_k \in E$ such that

$$h(x) = c(x - \beta_1) \cdots (x - \beta_k) \tag{16.3}$$

where $c = \mathrm{ld}(h)$ and

$$E = E_1[\beta_1, \ldots, \beta_k]. \tag{16.4}$$

Altogether we obtain that

$$f(x) = g(x)h(x) = (bc)(x - \alpha_1) \cdots (x - \alpha_m)(x - \beta_1) \cdots (x - \beta_k),$$

and

$$E = (F[\alpha_1, \ldots, \alpha_m])[\beta_1, \ldots, \beta_k] = F[\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_k].$$

And the claim follows in this case.

Case 2. $f(x) \in F[x]$ is irreducible.

In this case, by Lemma 16.1.2, there are a field extension E_1 of F and $\alpha \in E_1$ such that

$$f(\alpha) = 0 \quad \text{and} \quad E_1 = F[\alpha].$$

By the factor theorem, there is $g(x) \in E_1[x]$ such that

$$f(x) = (x - \alpha)g(x).$$

Notice that $\deg g < \deg f$, and so by the strong induction hypothesis, there are a field extension E of E_1 and $\alpha_1, \ldots, \alpha_n \in E$ such that

$$g(x) = b(x-\alpha_1)\cdots(x-\alpha_n) \tag{16.5}$$

where $b = \mathrm{ld}(g)$ and

$$E_1 = F[\alpha_1, \ldots, \alpha_n]. \tag{16.6}$$

Altogether we have that

$$f(x) = (x-\alpha)g(x) = b(x-\alpha)(a-\alpha_1)\cdots(x-\alpha_n),$$

and

$$E = (F[\alpha])[\alpha_1, \ldots, \alpha_n] = F[\alpha, \alpha_1, \ldots, \alpha_n].$$

This completes the proof. □

16.2 Towards uniqueness of a splitting field.

In this section among other things we show that two splitting fields of $f(x)$ over F are isomorphic. The results of this section play an important role in Galois theory.

Similar to the proof of the existence part, we start with adding one zero of an irreducible factor. We formulate a result which is essentially proved in the discussion prior to the proof of Lemma 16.1.2.

Lemma 16.2.1. *Suppose F is a field and $f(x) \in F[x]$ is irreducible. Assume E is a field extension of E and $\alpha \in E$ such that*

$$f(\alpha) = 0 \quad \textit{and} \quad E = F[\alpha].$$

Then

$$\overline{\phi}_\alpha : F[x]/\langle f \rangle \to E,\ \overline{\phi}_\alpha(g(x) + \langle f \rangle) := g(\alpha)$$

is an isomorphism.

Proof. we have that

$$\overline{\phi}_\alpha : F[x]/\langle m_{\alpha,F}(x) \rangle \to E,\ \ \overline{\phi}_\alpha(g(x) + \langle m_{\alpha,F}(x) \rangle) := g(\alpha) \tag{16.7}$$

is an isomorphism. Notice that since $f(\alpha) = 0$, $m_{\alpha,F}(x) | f(x)$. As $f(x)$ is irreducible in $F[x]$ and $m_{\alpha,F}(x)|f(x)$, there is $c \in F^\times$ such that $f(x) = cm_{\alpha,F}(x)$. This implies that $\langle m_{\alpha,F}(x) \rangle = \langle f(x) \rangle$. Therefore the claim follows form (16.7). □

Lemma 16.2.1 can be viewed as a type of *uniqueness* result for such a field. In the next lemma, we strengthen this uniqueness result in a way which makes it more suitable for a later use in an inductive argument.

Roughly the next lemma says that if we have two copies of a field, let's call them F_1 and F_2, and an irreducible polynomial $f_1 \in F_1[x]$, then the copy of f_1 in $F_2[x]$, let's call it f_2, is irreducible, and after adding a zero α_1 of f_1 to F_1 and adding a zero α_2 of f_2 to F_2, we end up getting isomorphic fields.

Lemma 16.2.2. *Suppose F and F' are fields and $\theta : F \to F'$ is an isomorphism. Let $f(x) \in F[x]$ be an irreducible polynomial. Suppose E is a field extension of F, $\alpha \in E$, E' is a field extension of F', and $\alpha' \in E$ satisfy the following properties:*

1. *$f(\alpha) = 0$ and $E = F[\alpha]$.*
2. *$\theta(f)(\alpha') = 0$ and $E' = F'[\alpha']$.*

Then there is a unique isomorphism $\widehat{\theta} : E \to E'$ such that for every $a \in F$, $\widehat{\theta}(a) = \theta(a)$ and $\widehat{\theta}(\alpha) = \alpha'$.

Notice that the ring isomorphism $\theta : F \to F'$ can be extended to a ring isomorphism from $F[x]$ to $F'[x]$ that is also denoted by θ:

$$\theta\Big(\sum_{i=0}^{n} a_i x^i\Big) := \sum_{i=0}^{n} \theta(a_i) x^i.$$

Roughly for $f \in F[x]$, $\theta(f)$ is the copy of f in $F'[x]$.

The conclusion of Lemma 16.2.2 is often captured in the following diagram as it is often better to *see* what we can prove. We say the following is a *commutative diagram*:

$$\begin{tikzcd}
E \arrow[r, dashed, "\widehat{\theta}"] & E' \\
F \arrow[u, hook] \arrow[r, "\theta"] & F' \arrow[u, hook]
\end{tikzcd}$$

This means all directed paths in the diagram with the same start and endpoints lead to the same result.

Our proof can be summarized in the following diagram:

$$\begin{tikzcd}
E \arrow[r, "\overline{\phi}_{\alpha}{}^{-1}"'] \arrow[rrr, bend left, "\widehat{\theta}"] & F[x]/\langle f\rangle \arrow[r, "\overline{\theta}"] & F'[x]/\langle \theta(f)\rangle \arrow[r, "\overline{\phi}_{\alpha'}"'] & E' \\
F \arrow[u, hook] \arrow[r] \arrow[rrr, bend right, "\theta"'] & F \arrow[u, hook] \arrow[r, "\theta"] & F' \arrow[u, hook] \arrow[r] & F' \arrow[u, hook]
\end{tikzcd} \tag{16.8}$$

Going though the above diagram, we give the details of the proof.

Proof of Lemma 16.2.2. Lemma 16.2.1 gives us the first block in the diagram in (16.8). To understand the second block, we start with a ring homomorphism from the numerator of the left hand side to the right hand side. Let

$$\widetilde{\theta} : F[x] \to F'[x]/\langle\theta(f)\rangle, \quad \widetilde{\theta}(g) := \theta(g) + \langle\theta(f)\rangle.$$

Notice that $\widetilde{\theta}$ is the composite of θ with the quotient map

$$p : F'[x] \to F'[x]/\langle\theta(f)\rangle,$$

and so $\widetilde{\theta}$ is a surjective ring homomorphism. By the first ring isomorphism we have that

$$\overline{\theta} : F[x]/\ker\widetilde{\theta} \to F'[x]/\langle\theta(f)\rangle, \;\; \overline{\theta}(g + \ker\widetilde{\theta}) := \theta(g) + \langle\theta(f)\rangle \tag{16.9}$$

is a ring isomorphism. We also have that $g \in \ker\widetilde{\theta}$ if and only if

$$\theta(g) \in \langle\theta(f)\rangle = \theta(\langle f\rangle),$$

and the latter holds precisely when $g \in \langle f\rangle$. This implies that $\ker\widetilde{\theta} = \langle f\rangle$. Hence by (16.9), we have that $\overline{\theta}$ is an isomorphism from $F[x]/\langle f\rangle$ to $F'[x]/\langle\theta(f)\rangle$. This gives us the middle block in the diagram given in (16.8). We also notice that since θ is an isomorphism and $f \in F[x]$ is irreducible, $\theta(f)$ is irreducible in $F'[x]$. As $\alpha' \in E'$ is a zero of $\theta(f)$, another application of Lemma 16.2.1 gives us the last block in the diagram given in (16.8). The composite of the ring isomorphisms in the first row give us an isomorphism $\widehat{\theta} : E \to E'$ and because the diagram in (16.8) is a commutative diagram, the claim follows. □

Lemma 16.2.2 will be used to show that splitting fields of $f(x) \in F[x]$ are isomorphic.

Chapter 17

Lecture 17

In the previous lecture we proved the *existence of a splitting field* (see Proposition 16.1.1), and to work towards the uniqueness of splitting fields, we proved that adding zeros of an irreducible polynomial and its twin in another copy of the base field give us isomorphic fields (see Lemma 16.2.1).

From Lemma 16.2.1, we immediately obtain that adding two zeros of an irreducible polynomial to the base field give us two isomorphic fields.

Corollary 17.0.1. *Suppose F is a field and $f(x) \in F[x]$ is irreducible. Suppose E and E' are field extensions of F, $\alpha \in E$ and $\alpha' \in E'$ are zeros of $f(x)$. Then there is a ring isomorphism $\widehat{\theta} : F[\alpha] \to F'[\alpha']$ such that*

$$\widehat{\theta}(g(\alpha)) := g(\alpha')$$

for every $g(x) \in F[x]$.

Proof. By Lemma 16.2.2, there is a ring isomorphism $\widehat{\theta} : F[\alpha] \to F[\alpha']$ such that $\widehat{\theta}(c) = c$ for every $c \in F$, and $\theta(\alpha) = \alpha'$. Then, for every $g(x) = \sum_{i=0}^{n} c_i x^i \in F[x]$ we have

$$\widehat{\theta}(g(\alpha)) = \widehat{\theta}(\sum_{i=0}^{n} c_i\alpha^i) = \sum_{i=0}^{n} \widehat{\theta}(c_i)\widehat{\theta}(\alpha)^i = \sum_{i=0}^{n} c_i\alpha'^i = g(\alpha').$$

This completes the proof. □

Exercise 17.0.2. *Suppose E is a field extension of F and $\alpha, \alpha' \in E$ are algebraic over F. Suppose $g(\alpha) \mapsto g(\alpha')$ for every $g(x) \in F[x]$ is a well-defined map. Then $m_{\alpha,F}(x) = m_{\alpha',F}(x)$, and so they are zeros of a single irreducible polynomial in $F[x]$.*

17.1 Extension of isomorphisms to splitting fields.

Now we are ready to prove the uniqueness of splitting fields. The following theorem plays an important role in Galois theory and understanding *symmetries* of splitting fields.

Theorem 17.1.1. *Suppose F and F' are fields, and $\theta : F \to F'$ is a ring isomorphism. Let $f(x) \in F[x] \setminus F$. Suppose E is a splitting field of f over F, and E' is a splitting field of $\theta(f)$ over F'. Then θ can be extended to an isomorphism $\widehat{\theta} : E \to E'$. This means that for every $c \in F$, we have $\widehat{\theta}(c) = \theta(c)$.*

The conclusion of Theorem 17.1.1 can be captured in the following commutative diagram.

$$\begin{tikzcd}
E \arrow[r, dashed, "\widehat{\theta}"] & E' \\
F \arrow[u, hook] \arrow[r, "\theta"] & F' \arrow[u, hook]
\end{tikzcd}$$

A *dashed arrow* means that this function was not initially given, and having other functions, we can find this one in a way that results in obtaining a commutative diagram, and *a hooked arrow* means that it is a natural inclusion map.

Proof. We proceed by induction on $\deg f$. If $\deg f = 1$, then f has a zero in F, and $\theta(f)$ has a zero in F'. Therefore $E = F$ and $E' = F'$. Hence we can choose $\widehat{\theta} = \theta$.

To prove the induction step, we start by recalling what it means that E and E' are splitting fields. Since E is a splitting field of f over F, there are $\alpha_1, \ldots, \alpha_n \in E$ such that

$$E = F[\alpha_1, \ldots, \alpha_n] \quad \text{and} \quad f(x) = a(x - \alpha_1) \cdots (x - \alpha_n), \tag{17.1}$$

where $a = \mathrm{ld}(f)$. Similarly we have that there are $\alpha'_1, \ldots, \alpha'_n \in E'$ such that

$$E' = F'[\alpha'_1, \ldots, \alpha'_n] \quad \text{and} \quad \theta(f(x)) = a'(x - \alpha'_1) \cdots (x - \alpha'_n), \tag{17.2}$$

where $a' = \mathrm{ld}(\theta(f))$. Since α_1 is a zero of f, we have that $m_{\alpha_1,F}$ is an irreducible factor of f in $F[x]$. Therefore $\theta(m_{\alpha_1,F})$ is an irreducible factor of $\theta(f)$ in $F'[x]$. Since $x - \alpha'_i$'s are irreducible factors of $\theta(f)$ in $E'[x]$, $\theta(m_{\alpha_1,F})$ divides $\theta(f)$ in $E'[x]$ and $E'[x]$ is a UFD, we deduce that

$$\theta(m_{\alpha_1,F}) = (x - \alpha'_{i_1}) \cdots (x - \alpha'_{i_k}) \tag{17.3}$$

for some $i_1, \ldots, i_k$. After the rearranging the indexes, if needed, we can and will assume that $x - \alpha'_1$ is a factor of $\theta(m_{\alpha_1,F})$ which means α'_1 is a zero of $\theta(m_{\alpha_1,F})$.

Since $m_{\alpha_1,F}$ is irreducible in $F[x]$ and α'_1 is a zero of $\theta(m_{\alpha_1,F})$, by Lemma 16.2.2 there is ring isomorphism $\widehat{\theta}_1 : F[\alpha_1] \to F'[\alpha'_1]$ which is an extension of θ (this means the diagram in (17.4) is a commutative diagram), and $\widehat{\theta}_1(\alpha_1) = \alpha'_1$.

$$\begin{tikzcd}
F[\alpha_1] \arrow[r, dashed, "\widehat{\theta}_1"] & F'[\alpha'_1] \\
F \arrow[u, hook] \arrow[r, "\theta"] & F' \arrow[u, hook]
\end{tikzcd} \tag{17.4}$$

Notice that by the factor theorem, there is $g \in (F[\alpha_1])[x]$ such that

$$f(x) = (x - \alpha_1)g(x). \tag{17.5}$$

By (17.5) and (17.1), we deduce that

$$g(x) = a(x-\alpha_2)\cdots(x-\alpha_n). \tag{17.6}$$

Applying $\widehat{\theta}_1$ to the both sides of (17.5), we obtain that

$$\widehat{\theta}_1(f) = (x-\widehat{\theta}_1(\alpha_1))\widehat{\theta}_1(g). \tag{17.7}$$

Since $\widehat{\theta}_1(\alpha_1) = \alpha'_1$, by (17.2), it follows that

$$\widehat{\theta}_1(g) = a'(x-\alpha'_2)\cdots(x-\alpha'_n). \tag{17.8}$$

By (17.6), after adding zeros of g to $F[\alpha_1]$

$$(F[\alpha_1])[\alpha_2,\ldots,\alpha_n] = F[\alpha_1,\ldots,\alpha_n]$$

we get E. Hence E is a splitting field of g over $F[\alpha_1]$. Similarly, by (17.8), after adding zeros of $\widehat{\theta}_1(g)$ to $F'[\alpha'_1]$ we get E'. Therefore E' is a splitting field of $\widehat{\theta}_1(g)$ over $F'[\alpha'_1]$. Since $\deg g < \deg f$, we can and will apply the induction hypothesis. By the induction hypothesis, we obtain a ring isomorphism $\widehat{\theta} : E \to E'$ which is an extension of $\widehat{\theta}_1$ (see the commutative diagram given in (17.9)).

$$\begin{tikzcd}
E \arrow[r, dashed, "\widehat{\theta}"] & E' \\
F[\alpha_1] \arrow[u, hook] \arrow[r, "\widehat{\theta}_1"] & F'[\alpha'_1] \arrow[u, hook]
\end{tikzcd} \tag{17.9}$$

By (17.4) and (17.9) (see the diagram in (17.10)),

$$\begin{tikzcd}
E \arrow[r, "\widehat{\theta}"] & E' \\
F[\alpha_1] \arrow[u, hook] \arrow[r, "\widehat{\theta}_1"] & F'[\alpha'_1] \arrow[u, hook] \\
F \arrow[u, hook] \arrow[r, "\theta"] & F' \arrow[u, hook]
\end{tikzcd} \tag{17.10}$$

we deduce that $\widehat{\theta}$ is an extension of θ, which completes the proof. □

The idea of the above proof is easy:

1. Find an *irreducible* factor of f in $F[x]$, say $h(x)$.

2. Add a zero of h to F and a zero of $\theta(h)$ to F', and find $\widehat{\theta}_1 : F[\alpha_1] \to F'[\alpha'_1]$.

3. View E as a splitting field of g and E' as a splitting field of $\widehat{\theta}_1(g)$. Use *induction hypothesis*.

Based on Theorem 17.1.1, we can prove the uniqueness of splitting fields up to an isomorphism.

Theorem 17.1.2. *Suppose F is a field, $f(x) \in F[x] \setminus F$, and E, E' are splitting fields of $f(x)$ over F. Then there is a ring isomorphism $\widehat{\theta} : E \to E'$ such that $\widehat{\theta}|_F = \mathrm{id}_F$; that means for every $c \in F$ we have that $\widehat{\theta}(c) = c$.*

Proof. Notice that $\mathrm{id}_F : F \to F$ is an isomorphism, and so by Theorem 17.1.1, there is a ring isomorphism $\widehat{\theta} : E \to E'$ which is an extension of id_F. This completes the proof. □

17.2 Two examples

In general giving a precise description of a splitting field of a polynomial is a very hard task. In this section, we learn two examples where to some extend we can describe a splitting of the given polynomial.

Example 17.2.1. *Let $\zeta_n := e^{2\pi i/n}$. Then $\mathbb{Q}[\zeta_n]$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$.*

Proof. Notice that the multiplicative order of ζ_n is n. Hence $(\zeta_n^j)^n = 1$ for every integer j in $[0, n)$, and $1, \zeta_n, \ldots, \zeta_n^{n-1}$ are distinct. Therefore these are distinct zeros of $x^n - 1$. Thus by the generalized factor theorem, comparing the degrees and the leading coefficients, we obtain that

$$x^n - 1 = (x - 1)(x - \zeta_n) \cdots (x - \zeta_n^{n-1}).$$

Hence $E := \mathbb{Q}[1, \zeta_n, \ldots, \zeta_n^{n-1}]$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$. Notice that $\mathbb{Q}[\zeta_n] \subseteq E$. Since $\zeta_n^j \in \mathbb{Q}[\zeta_n]$ for every integer j, we have that $E \subseteq \mathbb{Q}[\zeta_n]$. The claim follows. □

Example 17.2.2. *Let $\zeta_n := e^{2\pi i/n}$. Then $\mathbb{Q}[\zeta_n, \sqrt[n]{2}]$ is a splitting field of $x^n - 2$ over $\mathbb{Q}$.*

Proof. Notice that $(\zeta_n^j \sqrt[n]{2})^n = 2$ for every integer j. Hence $\sqrt[n]{2}, \zeta_n \sqrt[n]{2}, \ldots, \zeta_n^{n-1} \sqrt[n]{2}$ are distinct zeros of $x^n - 2$. Therefore by the generalized factor theorem, comparing degrees and leading coefficients, we obtain that

$$x^n - 2 = (x - \sqrt[n]{2})(x - \zeta_n \sqrt[n]{2}) \cdots (x - \zeta_n \sqrt[n]{2}^{n-1}).$$

Therefore $E := \mathbb{Q}[\sqrt[n]{2}, \zeta_n \sqrt[n]{2}, \ldots, \zeta_n^{n-1} \sqrt[n]{2}]$ is a splitting field of $x^n - 2$ over $\mathbb{Q}$. Notice that $\zeta_n := (\zeta_n \sqrt[n]{2})(\sqrt[n]{2})^{-1} \in E$. Hence $\mathbb{Q}[\sqrt[n]{2}, \zeta_n] \subseteq E$. We also have that $\zeta_n^j \sqrt[n]{2} \in \mathbb{Q}[\zeta_n, \sqrt[n]{2}]$ for every integer j. This implies that $E \subseteq \mathbb{Q}[\sqrt[n]{2}, \zeta_n]$, and the claim follows. □

Next we use splitting fields to study finite fields.

Chapter 18

Lecture 18

In the previous couple of lectures we proved the following results about splitting fields.

Theorem (Existence (See Proposition 16.1.1))**.** *Suppose F is a field and $f \in F[x] \setminus F$. Then there is a s splitting field E of f over F.*

Let's recall that E is called a *splitting field* of f over F if there are $\alpha_1, \ldots, \alpha_n \in E$ such that $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$, for some $a \in F$, and $E = F[\alpha_1, \ldots, \alpha_n]$.

Theorem (Uniqueness (See Theorem 17.1.2))**.** *Suppose F is a field and $f \in F[x] \setminus F$, E, E' are splitting fields of f over F. Then there is $\widehat{\theta} : E \to E'$ such that for every $c \in F$, $\widehat{\theta}(c) = c$.*

For field extensions E and E' of F, we say a ring isomorphism $\widehat{\theta} : E \to E'$ is an *F-isomorphism* if $\widehat{\theta}(c) = c$ for every $c \in F$.

The Uniqueness result was proved using the following isomorphism extension theorem.

Theorem (Isomorphism extension (See Theorem 17.1.1))**.** *Suppose F and F' are fields, $\theta : F \to F'$ is an isomorphism, and $f(x) \in F[x] \setminus F$. Suppose E is a splitting field of f over F, and E' is a splitting field of $\theta(f)$ over F'. Then there is an isomorphism $\widehat{\theta} : E \to E'$ which is an extension of θ.*

Prove of Isomorphism Extension Theorem is based on the following result on sending a zero of an irreducible polynomial to another zero.

Theorem (Sending a zero to another (See Lemma 16.2.2))**.** *Suppose F and F' are fields, f is irreducible in $F[x]$. Suppose E is a field extension of which contains a zero α of f, and E' is a field extension of F' which contains a zero of $\theta(f)$. Then there is $\widehat{\theta} : F[\alpha] \to F'[\alpha']$ which is an extension of θ and $\widehat{\theta}(\alpha) = \alpha'$.*

Now we use these results to study finite fields.

18.1 Finite fields: uniqueness

Suppose F is a finite field. Then its characteristic is a prime number p.

Lemma 18.1.1 (Order of a finite field)**.** *Suppose F is a finite of characteristic p. Then $|F| = p^n$ for some positive integer n.*

Proof. Since F is a finite integral domain, p is prime. Suppose ℓ is a prime factor of $|F|$. Then by Cauchy's theorem from group theory, there is $a \in F$ such that the additive order of a is ℓ. Since $\mathrm{char}(F) = p$, $pa = 0$. This implies that the additive order ℓ of a divides p. As ℓ and p primes, we deduce that $\ell = p$. Hence the only prime factor of $|F|$ is p, which implies that $|F|$ is a power of p. This completes the proof. □

We have seen that $x^p - x = \prod_{a \in \mathbb{Z}_p}(x - a)$. Next we generalize this to any finite field. We start with the following lemma, which can be viewed as a generalization of Fermat's little theorem.

Lemma 18.1.2. *Suppose F is a finite field of order q. Then $a^q = a$ for every $a \in F$.*

Proof. If $a = 0$, then clearly we have that $a^q = a$. If $a \neq 0$, then a is a unit. Hence $a^{|F^\times|} = 1$ as we know that in every (multiplicative) group G we have $g^{|G|} = e$. Since F is a field, we have $|F^\times| = |F| - 1 = q - 1$. Therefore $a^{q-1} = 1$, which implies that $a^q = a$. This completes the proof. □

Theorem 18.1.3. *Suppose F is finite field of order q. Then*

$$x^q - x = \prod_{\alpha \in F}(x - \alpha)$$

in $F[x]$.

Proof. By Lemma 18.1.2, every $\alpha \in F$ is a zero of $x^q - x$. Hence by the generalized factor theorem, there is $g(x) \in F[x]$ such that

$$x^q - x = g(x) \prod_{\alpha \in F}(x - \alpha). \tag{18.1}$$

Comparing the degrees of both sides, we deduce that g is a non-zero constant. Subsequently comparing the leading coefficients of both sides of (18.1), we obtain that $g = 1$. The claim follows. □

Theorem 18.1.4 (Uniqueness)**.** *Suppose F is a finite field of order $q = p^n$ where p is a prime number. Then F is a splitting field of $x^q - x$ over $\mathbb{Z}_p$. In particular, if F and F' are two fields of order q, then they are isomorphic.*

Proof. By Lemma 18.1.1, we obtain that the characteristic of F is p. Hence $\mathbb{Z}_p$ can be viewed as a subfield of F. By Theorem 18.1.3, we have that $x^q - x$ can be factored as a product of degree one polynomials over F, and adding zeros of $x^q - x$ to $\mathbb{Z}_p$, we get the entire F. Hence F is a splitting field of $x^q - x$ over $\mathbb{Z}_p$.

If F and F' are fields of order q, then both of them are splitting fields of $x^q - x$ over $\mathbb{Z}_p$. Hence by Theorem 17.1.2, F and F' are isomorphic. This completes the proof. □

18.2 Finite fields: towards existence

We want to show the existence of a finite field of order $q = p^n$ where p is prime and n is a positive integer. By Theorem 18.1.4, we have to consider a splitting field E of $x^q - x$ over $\mathbb{Z}_p$ and show that it has q elements. So in this section, we let E be a splitting field of $x^q - x$ over $\mathbb{Z}_p$ and

$$F := \{\alpha \in E \mid \alpha^q = \alpha\}.$$

Lemma 18.2.1. *In the above setting, F is a field.*

Proof. To show F is a field, we prove that is closed under addition, multiplication, negation, and inversion.

Notice that since the characteristic of F is a prime number p, the Frobenius map $\sigma : E \to E, \sigma(a) := a^p$ is a ring homomorphism (see Problem 4 in Week 1 assignment). Therefore

$$\sigma^{(n)} : E \to E, \quad \sigma^{(n)}(a) = a^{p^n}$$

is also a ring homomorphism. Notice that F is the set of *fixed points* of $\sigma^{(n)}$; that means that

$$F = \{a \in E \mid \sigma^{(n)}(a) = a\}.$$

For every $\alpha, \beta \in F$, we have

$$\sigma^{(n)}(\alpha+\beta) = \sigma^{(n)}(\alpha)+\sigma^{(n)}(\beta) = \alpha+\beta \text{ and } \sigma^{(n)}(\alpha\cdot\beta) = \sigma^{(n)}(\alpha)\cdot\sigma^{(n)}(\beta) = \alpha\cdot\beta.$$

So $\alpha + \beta$ and $\alpha \cdot \beta$ are in F. Therefore F is closed under addition and multiplication. For $\alpha \in F$ we also have that

$$\sigma^{(n)}(-\alpha) = -\sigma^{(n)}(\alpha) = -\alpha,$$

and so $-\alpha \in F$. Suppose $\alpha \in F \setminus \{0\}$. Then $\alpha^{-1} \in E$, and

$$\sigma^{(n)}(\alpha^{-1}) = (\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1},$$

which implies that $\alpha^{-1} \in F$. This completes the proof. □

Next we want to show that $|F| = q$, which completes the proof of the existence of a field of order q.

Corollary 18.2.2. *In the above setting, the order of F is the same of the number of distinct zeros of $x^q - x$ in E.*

Proof. Since E is a splitting field of $x^q - x$ over $\mathbb{Z}_p$, there are $\alpha_1, \ldots, \alpha_q \in E$ such that

$$x^q - x = \prod_{i=1}^{q}(x - \alpha_i).$$

Notice that $\alpha \in F$ if and only if α is a zero of $x^q - x$. Since E is an integral domain, we obtain that

$$F = \{\alpha_1, \ldots, \alpha_n\}.$$

The claim follows. □

By Corollary 18.2.2, we have that $|F| = q$ if and only if zeros of $x^q - x$ in its splitting field are distinct. So we need to find a mechanism to determine whether zeros of a polynomial in its splitting field are distinct.

18.3 Separability: having distinct zeros in a splitting field.

We need to come up with a technique of finding out whether or not $f(x)$ has a multiple zero. Recall that we say $a \in A$ is a *multiple zero* of f if $f(x) = (x-a)^2 g(x)$ for some $g(x) \in A[x]$. We use an idea from calculus: a polynomial $f(x) \in \mathbb{C}[x]$ has a multiple zero at z if and only if $f(z) = f'(z) = 0$. This means we need to define the derivative of a polynomial in $A[x]$ for an arbitrary unital commutative ring A.

Definition 18.3.1. *Suppose $f(x) := \sum_{i=0}^{\infty} a_i x^i \in A[x]$ where A is a unital commutative ring. We let*

$$f'(x) := \sum_{i=1}^{\infty} i a_i x^{i-1}, \tag{18.2}$$

and call it the derivative *of f.*

Sometimes it is useful to write the sum in (18.2) starting from 0

$$f'(x) = \sum_{i=0}^{\infty} i a_i x^{i-1}.$$

One can check that the following properties of ordinary derivatives still hold for polynomials in a general setting.

Lemma 18.3.2. *Suppose A is a unital commutative ring, $f, g \in A[x]$, and $a, b \in A$. Then the derivative of $af(x) + bg(x)$ is $af'(x) + bg'(x)$ and the product rule*

$$(fg)' = f'g + fg'$$

holds.

Proof. It is easy to check that $(af + bg)' = af' + bg'$. Here we only discuss the product rule. Suppose $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{j=0}^{\infty} b_j x^j$. Then the coefficient of x^k in fg is

$$c_k := \sum_{i+j=k, i,j \geq 0} a_i b_j.$$

Thus $(fg)' = \sum_{k=0}^{\infty} k c_k x^{k-1}$. Since $f'(x) = \sum_{i=0}^{\infty} i a_i x^{i-1}$ and $g'(x) = \sum_{j=0}^{\infty} j b_j x^{j-1}$, the coefficient of x^{k-1} in $f'g$ is

$$\sum_{i+j=k, i,j \geq 0} i a_i b_j$$

and the coefficient of x^{k-1} in fg' is

$$\sum_{i+j=k, i,j \geq 0} j a_j b_j.$$

Hence

$$f'g + fg' = \sum_{k=0}^{\infty} \Big(\sum_{i+j=k, i,j \geq 0} (i+j) a_i b_j \Big) x^{k-1} = \sum_{k=0}^{\infty} k c_k x^{k-1}.$$

The claim follows. □

Lemma 18.3.3. *Suppose A is a unital commutative ring and for $a \in A$ and $f, g \in A[x]$, we have $f(x) = (x-a)^2 g(x)$. Then $f(a) = f'(a) = 0$.*

Proof. Clearly $f(a) = 0$. By the product rule, we have that

$$f'(x) = (x-a)^2 g(x) + 2(x-a)g(x) = (x-a)((x-a)g'(x) + 2g(x)).$$

Hence $f'(a) = 0$. The claim follows. □

Proposition 18.3.4. *Suppose F is a field, $f(x) \in F[x] \setminus F$, and E is a splitting field of f over F. Then $f(x)$ does not have multiple zeros in E if and only if $\gcd(f, f') = 1$ in $F[x]$*[1].

Proof. ($\Rightarrow$) Suppose $\gcd(f, f') \neq 1$. Then there is a non-constant monic polynomial $q(x) \in F[x]$ which divides both $f(x)$ and $f'(x)$. Since E is a splitting field of f over F, there are $\alpha_1, \ldots, \alpha_n \in E$ such that

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n),$$

for some $a \in F$. As $q(x)|f(x)$, $x - \alpha_i$'s are irreducible in $E[x]$, and $E[x]$ is a UFD, we have that

$$q(x) = (x-\alpha_{i_1})\cdots(x-\alpha_{i_k})$$

for some $i_1, \ldots, i_k$. Since $q(x)|f'(x)$, we have that $f'(\alpha_{i_1}) = 0$. After rearranging the indexes, if necessary, we can and will assume that $i_1 = 1$. Thus $f'(\alpha_1) = 0$. By the product rule, we have that $f'(x)$ is equal to

$$a((x-\alpha_2)\cdots(x-\alpha_n)+(x-\alpha_1)(x-\alpha_3)\cdots(x-\alpha_n)+\cdots+(x-\alpha_1)\cdots(x-\alpha_{n-1})).$$

Hence

$$f'(\alpha_1) = a(\alpha_1-\alpha_2)\cdots(\alpha_1-\alpha_n).$$

Therefore $f'(\alpha_1) = 0$ implies that $\alpha_1 = \alpha_j$ for some index $j \geq 2$. This means f has multiple zeros.

($\Leftarrow$) Suppose $f(x) = (x-\alpha)^2 g(x)$. Then by Lemma 18.3.3, $f'(\alpha) = 0$. As $f'(x) \in F[x]$, we deduce that $m_{\alpha,F}(x)|f'(x)$ in $F[x]$. Similarly, since $f(\alpha) = 0$ and $f(x) \in F[x]$, we have $m_{\alpha,F}(x)|f(x)$. Therefore $m_{\alpha,F}(x)$ is a common divisor of f and f' in $F[x]$, which implies that $\gcd(f, f') \neq 1$. This completes the proof. □

[1] Here we are using the convention that the greatest common divisor of polynomials with coefficients in a field are monic.

18.4 Finite field: existence

Let's recall some of the notation and results from Section 18.2. Let $q = p^n$ where p is a prime and n is a positive integer. Let E be a splitting field of $x^q - x$ over $\mathbb{Z}_p$. Let

$$F := \{\alpha \in E \mid \alpha^q = \alpha\}.$$

By Lemma 18.2.1, F is a field, and by Corollary 18.2.2, the order of F is the number of distinct zeros of $x^q - x$ in E.

Lemma 18.4.1. *In the above setting, $|F| = q$.*

Proof. Since $|F|$ is the number of distinct zeros of $x^q - x$ in its splitting field, it is enough to show that $x^q - x$ does not have multiple zeros in its splitting fields. By Proposition 18.3.4, $f(x) := x^q - x$ does not have multiple zeros in E if and only if $\gcd(f, f') = 1$ in $F[x]$. Notice that $f'(x) = qx^{q-1} - 1 = -1$ in $F[x]$ as $\mathrm{char}(F) = p$. Hence $\gcd(f, f') = 1$, and the claim follows. □

Altogether, we have proved:

Theorem 18.4.2 (Existence)**.** *Suppose p is prime and n is positive integer. Then there is a finite field of order p^n.*

Theorem 18.4.3 (Construction)**.** *Finite field of order p^n is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.*

We let $\mathbb{F}_{p^n}$ denote a finite field of order p^n. Notice that by Theorem 18.4.2, there is such a finite field, and by Theorem 18.1.4, $\mathbb{F}_{p^n}$ is unique up to an isomorphism.

Chapter 19

Lecture 19

19.1 Vector spaces over a field

Let's recall a couple of results that we have proved a while ago.

Proposition. *(See Proposition 8.3.1) Suppose F is a field and $f(x) \in F[x]$ is a polynomial of degree n. Then every element of $F[x]/\langle f\rangle$ can be uniquely written as*

$$c_0\overline{1} + c_1\overline{x} + \cdots + c_{n-1}\overline{x}^{n-1}$$

for some $c_0, \ldots, c_{n-1} \in F$ where $\overline{1} := 1 + \langle f\rangle$ and $\overline{x} := x + \langle f\rangle$.

Proposition. *(See Theorem 9.1.1) Suppose E is a field extension oof F, and $\alpha \in E$ is algebraic over F. Suppose $\deg m_{\alpha,F} = n$. Then every element of $F[\alpha]$ can be uniquely written as*

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

for some $c_0, \cdots, c_{n-1} \in F$.

In both of these statements, elements are *uniquely* written as an F-linear combination of certain elements. This is similar to the main property of a *basis* in a vector space. It brings us to the definition of a vector space over a field F.

Definition 19.1.1. *Suppose F is a field. We say V is a vector space over F if:*

(1) $(V, +)$ is an abelian group.

(2) There is a scalar multiplication $F \times V \to V$ and for every $c \in F$ and $v \in V$, the scalar multiplication of c by v is denoted by $c \cdot v$ (or simply cv). This scalar multiplication is supposed to have the following properties.

a) For every $c_1, c_2 \in F$ and $v \in V$,

$$(c_1 + c_2) \cdot v = c_1 \cdot v + c_2 \cdot v.$$

b) For every $c \in F$ and $v_1, v_2 \in V$,

$$c \cdot (v_1 + v_2) = c \cdot v_1 + c \cdot v_2.$$

c) For every $v \in V$, $1 \cdot v = v$.

Example 19.1.2. *Suppose F is a field and n is a positive integer. Then*

$$F^n := \underbrace{F \times \cdots \times F}_{n \text{ times}}$$

is a vector space with respect to the following scalar multiplication

$$c \cdot (a_1, \ldots, a_n) := (ca_1, \ldots, ca_n).$$

Another example which plays an important role in this course is the following.

Example 19.1.3. *Suppose A is a unital ring, F is a subfield of A, and $1_A = 1_F$. Then A is a vector space over F with respect to the following scalar multiplication:*

$$\forall c \in F, a \in A, \quad c \cdot a := ca$$

where ca is the multiplication in A.

Let's recall some basic terminologies in linear algebra.

Definition 19.1.4. *Suppose V is a vector space over a field F.*

1. *We say $v_1, \cdots, v_n \in V$ are F-*linearly independent *if, for $c_1, \ldots, c_n \in F$,*

$$c_1 \cdot v_1 + \cdots + c_n v_n = 0 \textit{ implies that } c_1 = \cdots = c_n = 0.$$

2. *If $v_1, \ldots, v_n \in V$ are not F-linearly independent, we say they are F-*linearly dependent.

3. *We say $\{v_1, \ldots, v_n\} \subseteq V$ is an F-*spanning set *if every element of V can be written as an F-linear combination of $v_1, \ldots, v_n$; that means for every $v \in V$ there are $c_1, \ldots, c_n \in F$ such that*

$$v = c_1 \cdot v_1 + \cdots + c_n \cdot v_n.$$

   When $\{v_1, \ldots, v_n\}$ is an F-spanning set, we say $v_1, \ldots, v_n$ span V.

4. *We say $(v_1, \ldots, v_n)$ is an F-*basis of *V if $v_1, \ldots, v_n$ are F-linearly independent and $\{v_1, \ldots, v_n\}$ is an F-spanning set.*

Though a basis is formally an *ordered* set, we sometimes refer to a set as a basis if it is an F-spanning set and consists of F-linearly independent vectors.

19.2 Subspace and linear map

As always, when we learn a new math object, we should talk about its substructures and the maps that preserves its structure.

Definition 19.2.1. *Suppose V is vector space over a field F. We say $W \subseteq V$ is a* subspace *of V if W is closed under addition and scalar multiplication.*

Definition 19.2.2. *Suppose V_1 and V_2 are two vector spaces over a field F.*

1. *We say $f : V_1 \to V_2$ is F-linear if*

$$f(v + v') = f(v) + f(v') \quad \textit{and} \quad f(c \cdot v) = c \cdot f(v)$$

for every $c \in F$ and $v, v' \in V$; alternatively we can write $f(cv + v') = cf(v) + f(v')$.

2. *We say $f : V_1 \to V_2$ is an* isomorphism *of F-vector spaces if*
   - *a) f is F-linear,*
   - *b) f is bijective, and*
   - *c) f^{-1} is F-linear.*

It is a good exercise to show that if f is F-linear and it is bijective, then f^{-1} is F-linear. So the last condition for being an F-vector space isomorphism is redundant.

Let's also point out that similar to Lemma 1.3.1, one can use the distribution properties and show that

$$0_F \cdot v = 0_V \quad \text{and} \quad c \cdot 0_V = 0_V$$

for every $v \in V$ and $c \in F$.

Lemma 19.2.3. *Suppose V is a vector space over a field F, and $v_1, \ldots, v_n \in V$. Then the smallest subspace of V which contains v_i's is*

$$\Big\{ \sum_{i=1}^{n} c_i v_i \mid c_i \in F \Big\}.$$

*(This is denoted by $\operatorname{Span}_F\{v_1, \ldots, v_n\}$ or $\operatorname{Span}_F(v_1, \ldots, v_n)$, and it is called either the F-*span *of v_i's, or the* subspace spanned *by $v_1, \ldots, v_n$).*

Proof. Suppose W is a subspace of V which contains v_i's. Since W is closed under scalar multiplication, we have $c_i v_i \in W$ for every $c_i \in F$. Since W is closed under addition, we deduce that $\sum_{i=1}^n c_i v_i \in W$. Hence $\operatorname{Span}_F(v_1, \ldots, v_n) \subseteq W$.

Next we show that $\operatorname{Span}(v_1, \ldots, v_n)$ is a subspace. Suppose $c \in F$ and w, w' are in $\operatorname{Span}_F(v_1, \ldots, v_n)$. Then $w = \sum_{i=1}^n c_i v_i$ and $w' = \sum_{i=1}^n c_i' v_i$ for some $c_i, c_i' \in F$. Hence

$$cw + w' = c\sum_{i=1}^{n} c_i v_i + \sum_{i=1}^{n} c_i' v_i = \sum_{i=1}^{n} (cc_i + c_i')v_i \in \operatorname{Span}_F(v_1, \ldots, v_n).$$

Therefore $\operatorname{Span}_F(v_1, \ldots, v_n)$ is a subspace.

Finally we notice that

$$v_i = 0 \cdot v_1 + \cdots + 0 \cdot v_{i-1} + 1 \cdot v_i + 0 \cdot v_{i+1} + \cdots + 0 \cdot v_n \in \operatorname{Span}_F(v_1, \ldots, v_n).$$

Altogether, we proved that $\operatorname{Span}_F(v_1, \ldots, v_n)$ is a subspace which contains v_i's and every other subspace that contains v_i' contains $\operatorname{Span}_F(v_1, \ldots, v_n)$ as a subset. This completes the proof. □

Next lemma shows the importance of Example 19.1.2.

Lemma 19.2.4. *Suppose V is a vector space over a field F, and $\mathfrak{B} := (v_1, \ldots, v_n)$ is an F-basis of V. Then*

1. *for every $v \in V$, there is a unique*

$$(c_1, \ldots, c_n) \in F^n$$

such that $v = c_1 v_1 + \cdots + c_n v_n$. We let $[v]_{\mathfrak{B}} := (c_1, \ldots, c_n)$.

2. *The map $V \to F^n, v \mapsto [v]_{\mathfrak{B}}$ is a vector space isomorphism.*

Proof. (1) Since $\mathfrak{B}$ spans V, every $v \in V$ can be written as an F-linear combination of v_i's; that means that there are c_i's in F such that

$$v = c_1 v_1 + \cdots + c_n v_n.$$

Now we want to show the uniqueness. So suppose $\sum_{i=1}^n c_i v_i = \sum_{i=1}^n c_i' v_i$ for some $c_i, c_i' \in F$. Then

$$(c_1 - c_1')v_1 + \cdots + (c_n - c_n')v_n = 0. \tag{19.1}$$

As v_i's are F-linearly independent and $c_i - c_i' \in F$, by (19.1) we have that $c_i - c_i' = 0$ for every i. Hence

$$(c_1, \ldots, c_n) = (c_1', \ldots, c_n').$$

(2) By part (1), $v \mapsto [v]_{\mathfrak{B}}$ is well-defined and it is the inverse function of

$$F^n \to V, \ \ (c_1, \ldots, c_n) \mapsto \sum_{i=1}^n c_i v_i.$$

Hence $v \mapsto [v]_{\mathfrak{B}}$ is a bijection. Let $[v]_{\mathfrak{B}} = (a_1, \ldots, a_n)$ and $[v']_{\mathfrak{B}} = (a_1', \ldots, a_n')$. Then $v = \sum_{i=1}^n a_i v_i$ and $v' = \sum_{i=1}^n a_i' v_i$. Therefore for every $c, c' \in F$, we have $cv + cv' = \sum_{i=1}^n (ca_i + a'a_i')v_i$, which implies that

$$\begin{aligned}[cv + cv']_{\mathfrak{B}} =&(ca_1 + c'a_1', \ldots, ca_n + c'a_n')\\ =&c(a_1, \ldots, a_n) + c'(a_1', \ldots, a_n')\\ =&c[v]_{\mathfrak{B}} + c'[v']_{\mathfrak{B}},\end{aligned}$$

this completes the proof. □

19.3 Dimension of a vector space

The following theorem plays helps us define the dimension of a vector space and more.

Theorem 19.3.1. *Suppose V is a vector space over a field F. Suppose $\{v_1, \ldots, v_n\}$ is an F-spanning set, and $w_1, \ldots, w_m$ are F-linearly independent. Then $n \geq m$.*

Proof. Inductively we will find distinct indexes $i_1, \ldots, i_m$ such that for every integer k in $[0, m]$,

$$(\{v_1, \ldots, v_n\} \setminus \{v_{i_1}, \ldots, v_{i_k}\}) \cup \{w_1, \ldots, w_k\}$$

is an F-spanning set. We are substituting w_j for v_{i_j} in $\{v_1, \ldots, v_n\}$ and still spanning V.

Notice that finding these distinct indexes

$$1 \leq i_1, \ldots, i_m \leq n$$

implies that $m \leq n$, and the claim follows.

The base of induction ($k = 0$) follows from the assumption that $\{v_1, \ldots, v_n\}$ is an F-spanning set. Now we show the induction step. Suppose we have already found $i_1, \ldots, i_k$ such that

$$(\{v_1, \ldots, v_n\} \setminus \{v_{i_1}, \ldots, v_{i_k}\}) \cup \{w_1, \ldots, w_k\}$$

is an F-spanning set. To simplify our notation, after rearranging v_i's, we can and will assume that $i_1 = 1, \ldots, i_k = k$; and so

$$\mathrm{Span}_F(w_1, \ldots, w_k, v_{k+1}, \ldots, v_n) = V. \tag{19.2}$$

In particular, w_{k+1} can be written as an F-linear combination of $w_1, \ldots, w_k, v_{k+1}, \ldots, v_n$. Hence there are c_i's in F such that

$$w_{k+1} = c_1 w_1 + \cdots + c_k w_k + c_{k+1} v_{k+1} + \cdots + c_n v_n. \tag{19.3}$$

Claim. There exists $j \geq k + 1$ such that $c_j \neq 0$.

Proof of Claim. If not, $w_{k+1} = \sum_{i=1}^{k} c_i w_i$. This contradicts the assumption that w_i's are F-linearly independent.

Without loss of generality, after rearranging v_l's, we can and will assume that $c_{k+1} \neq 0$.

Claim. $\mathrm{Span}_F(w_1, \ldots, w_{k+1}, v_{k+2}, \ldots, v_n) = V$.

Proof of Claim. Because of (19.2), to show the Claim it is sufficient to prove that v_{k+1} is in the F-span of $w_1, \ldots, w_{k+1}, v_{k+2}, \ldots, v_n$. By (19.3),

$$c_{k+1} v_{k+1} = -\sum_{i=1}^{k} c_i w_i + w_{k+1} - \sum_{i=k+2}^{n} c_i v_i.$$

Notice that since $c_{k+1} \neq 0$ and F is a field, c_{k+1}^{-1} exists. Hence

$$\begin{aligned} v_{k+1} =& -\sum_{i=1}^{k}(c_{k+1}^{-1}c_i)w_i + c_{k+1}^{-1}w_{k+1} - \sum_{i=k+2}^{n}(c_{k+1}^{-1}c_i)v_i \\ &\in \operatorname{Span}_F(w_1,\ldots,w_{k+1},v_{k+2},\ldots,v_n), \end{aligned}$$

and the claim follows. □

Theorem 19.3.2. *Suppose V is a vector space over a field F. Suppose V is the F-span of a finite set $\{v_1,\ldots,v_n\}$. Then*

1. *V has an F-basis which is a subset of $\{v_1,\ldots,v_n\}$.*
2. *If $\mathfrak{B} := (w_1,\ldots,w_m)$ and $\mathfrak{B}' := (w'_1,\ldots,w'_k)$ are two F-bases, then $m = k$.*

The size of a basis of V is called the *dimension* of V over F and we denote it by $\dim_F V$.

Proof of Theorem 19.3.2. (1) Suppose $\{v_{i_1},\ldots,v_{i_m}\}$ is a maximal subset of $\{v_1,\ldots,v_n\}$ that consists of F-linearly independent vectors. Then for every $j \notin \{i_1,\ldots,i_m\}$, the vectors $v_{i_1},\ldots,v_{i_m},v_j$ are F-linearly dependent. This means there are $c_1,\ldots,c_{m+1} \in F$ that are not all zero and

$$c_1v_{i_1} + \cdots + c_mv_{i_m} + c_{m+1}v_j = 0.$$

Since $v_{i_1},\ldots,v_{i_m}$ are F-linearly independent, $c_{m+1} \neq 0$. Hence c_{m+1}^{-1} exists (as F is a field). Therefore

$$\begin{aligned} v_j =& -(c_{m+1}^{-1}c_1)v_{i_1} - \cdots - (c_{m+1}^{-1}c_m)v_{i_m} \\ &\in \operatorname{Span}_F(v_{i_1},\ldots,v_{i_m}). \end{aligned} \tag{19.4}$$

Since (19.4) holds for every j not in $\{i_1,\ldots,i_m\}$, we deduce that

$$\operatorname{Span}_F(v_{i_1},\ldots,v_{i_m}) = \operatorname{Span}_F(v_1,\ldots,v_n) = V.$$

Hence $(v_{i_1},\ldots,v_{i_m})$ is an F-basis as it consists of F-linearly independent vectors and it is an F-spanning set.

(2) Since $\{w_1,\ldots,w_m\}$ is an F-spanning set and $w'_1,\ldots,w'_k$ are F-linearly independent, by Theorem 19.3.1 we have $k \leq m$. Similarly, since $\{w'_1,\ldots,w'_k\}$ is an F-spanning set and $w_1,\ldots,w_m$ are F-linearly independent, by Theorem 19.3.1 we have $m \leq k$. Altogether we get $m = k$, and this completes the proof. □

19.4 Quotient spaces

Similar to groups and rings, we want to define the quotient of a vector space. Suppose V is a vector space over a field F, and W is a subspace of V. Then in particular W is a (normal) subgroup of V. Hence we can consider the abelian group V/W.

Proposition 19.4.1. *Suppose V is a vector space over a field F, and W is a subspace of V. Then the following is a well-defined scalar multiplication*

$$F \times V/W \to V/W, \quad (c, v+W) \mapsto c \cdot (v+W) := cv + W.$$

Moreover V/W with its quotient abelian group structure and the above given scalar product is an F-vector space.

Proof. Let's start with arguing why $\cdot$ is a well-defined operation. So assuming $v_1+W = v_2 + W$, we have to show that $cv_1 + W = cv_2 + W$ for every $c \in F$. Notice that $v_1+W = v_2+W$ implies that $v_1-v_2 \in W$. As W is closed under scalar multiplication, we have that $c(v_1 - v_2) \in W$ for every c in F. Therefore $cv_1 - cv_2 \in W$, from which we deduce that $cv_1 + W = cv_2 + W$. This shows that $\cdot$ is a well-defined operation.

Next, we check why V/W is an F-vector space. For every $c \in F$ and $v_1, v_2 \in V$, we have

$$\begin{aligned} c \cdot ((v_1 + W) + (v_2 + W)) =& c \cdot ((v_1 + v_2) + W) \\ =& c(v_1 + v_2) + W \\ =& (cv_1 + cv_2) + W \\ =& (cv_1 + W) + (cv_2 + W) \\ =& c \cdot (v_1 + W) + c \cdot (v_2 + W). \end{aligned}$$

Similarly we can check that

$$(c_1 + c_2) \cdot (v + W) = c_1 \cdot (v + W) + c_2 \cdot (v + W)$$

for every $c_1, c_2 \in F$ and $v \in V$.

Finally we observe that

$$1 \cdot (v + W) = (1\ v) + W = v + W$$

for every $v \in V$. This completes the proof. □

Notice that the natural quotient map

$$p_W : V \to V/W,\ p_W(v) := v + W$$

is F-linear and $\ker p_W = W$.

Since by Lemma 19.2.4 an F-vector space of a given dimension is unique up to an isomorphism, we want to understand the dimension of V/W.

Proposition 19.4.2. *Suppose V is a vector space over F and W is a subspace of V. Then*

$$\dim_F W + \dim_F V/W = \dim_F V;$$

in particular if one of the sides is finite, then the other side is finite as well.

Proof. First notice that if $\dim_F V < \infty$, then there is a finite F-spanning set $\{v_1, \ldots, v_n\}$. Then by Theorem 19.3.1, every subset of W that consists of F-linearly independent vectors has cardinality at most n; in particular, $\dim_F W < \infty$. We also observe that $\{v_1 + W, \ldots, v_n + W\}$ is an F-spanning subset of V/W, and so by the first part of Theorem 19.3.2, we have $\dim_F V/W < \infty$. Hence from this point on, we can and will assume that

$$\dim_F W = m < \infty \quad \text{and} \quad \dim_F V/W = k < \infty.$$

Suppose $(w_1, \ldots, w_m)$ is an F-basis of W, and $(v_1 + W, \ldots, v_k + W)$ is an F-basis of V/W. We show that $(w_1, \ldots, w_m, v_1, \cdots, v_k)$ is an F-basis of V. We prove this in two steps. First we show this is an F-spanning set, and second we show that it consists of F-linearly independent vectors.

Step 1. $\mathrm{Span}_F(w_1, \ldots, w_m, v_1, \cdots, v_k) = V$.

Proof of Step 1. Let $W' := \mathrm{Span}_F(w_1, \ldots, w_m, v_1, \cdots, v_k)$. Then $W \subseteq W'$ as w_i's span W and they are in W'. Hence W'/W is a subspace of V/W. Since $v_i + W$'s are in W'/W and they span V/W, we deduce that $W'/W = V/W$. Therefore by the correspondence theorem for the subgroups of a quotient group, we have that $V = W'$. (We can avoid using the correspondence theorem and use the following argument: for every $v \in V$, knowing that $v + W \in W'/W$, we can deduce that there is $w' \in W$ such that $v + W = w' + W$. This means $v - w' = w$ for some $w \in W \subseteq W'$. Hence

$$v = w' + w \in W'.$$

Altogether we proved that every element v of V is in W. Therefore $V = W'$.)

Step 2. $w_1, \ldots, w_m, v_1, \cdots, v_k$ are F-linearly independent.

Proof of Step 2. Suppose

$$\sum_{i=1}^{m} c_i w_i + \sum_{j=1}^{k} c_{m+j} v_j = 0 \tag{19.5}$$

for some c_i's in F. Then

$$p_W\Big(\sum_{i=1}^{m} c_i w_i + \sum_{j=1}^{k} c_{m+j} v_j\Big) = 0,$$

where $p_W : V \to V/W, \quad p_W(v) := v + W$ is the natural quotient map. Since $W = \ker p_W$, we obtain that

$$\sum_{j=1}^{k} c_{m+j} \cdot p_W(v_j) = 0,$$

and so

$$c_{m+1} \cdot (v_1 + W) + \cdots + c_{m+k} \cdot (v_k + W) = 0. \tag{19.6}$$

As $v_j + W$'s are F-linearly independent, we deduce that $c_{m+1} = \cdots = c_{m+k} = 0$. Hence by (19.5), we obtain that

$$\sum_{i=1}^{m} c_i w_i = 0.$$

As w_i's are F-linearly independent, we have $c_1 = \cdots = c_m = 0$. Altogether we deduce that all the coefficients in (19.6) are zero. This completes the proof of the second step.

By Steps 1 and 2, we obtain that

$$(w_1, \ldots, w_m, v_1, \ldots, v_k)$$

is an F-basis. Hence

$$\dim_F V = m + k = \dim_F W + \dim_F V/W,$$

which completes the proof. □

19.5 The first isomorphism theorem for vector spaces

Similar to groups and rings, next we prove the first isomorphism theorem. Then we use this result to show the kernel-image theorem.

Theorem 19.5.1. *Suppose V_1 and V_2 are two F-vector spaces, and $f : V_1 \to V_2$ is an F-linear map. Then*

1. $\operatorname{Im}(f)$ *is a subspace of* V_2*, and* $\ker f$ *is a subspace of* V_1.
2. $\overline{f} : V_1/\ker f \to \operatorname{Im} f$, $\quad \overline{f}(v_1 + \ker f) := f(v_1)$ *is an isomorphism of F-vector spaces.*
3. $\dim_F(\ker f) + \dim_F(\operatorname{Im} f) = \dim_F V_1$.

Proof. (1) Since f is an additive group homomorphism, $\operatorname{Im} f$ is a subgroup of V_2 and $\ker f$ is a subgroup of V_1. So it is sufficient to prove that $\operatorname{Im} f$ and $\ker f$ are closed under scalar multiplication. Suppose $v_2 \in \operatorname{Im} f$. Then $v_2 = f(v_1)$ for some $v_1 \in V_1$. Hence for every $c \in F$, we have

$$cv_2 = cf(v_1) = f(cv_1) \in \operatorname{Im} f.$$

This shows that $\operatorname{Im} f$ is closed under scalar multiplication, and so it is a subspace of V_2.

Suppose $v_1 \in \ker f$ and $c \in F$. Then

$$f(cv_1) = cf(v_1) = c0 = 0,$$

which implies that $cv_1 \in \ker f$. Hence $\ker f$ is closed under scalar multiplication, which implies that $\ker f$ is a subspace of V_1.

(2) By the first isomorphism theorem for groups, we have that

$$\overline{f} : V_1/\ker f \to \operatorname{Im} f, \quad \overline{f}(v_1 + \ker f) := f(v_1)$$

is a well-defined group isomorphism. So to show that $\overline{f}$ is an F-vector space isomorphism, it suffices to argue why $\overline{f}$ preserves the scalar multiplication. For every $c \in F$

and $v_1 \in V_1$, we have

$$\begin{aligned}\overline{f}(c \cdot (v_1 + \ker f)) =& \overline{f}(cv_1 + \ker f) \\ =& f(cv_1) \\ =& cf(v_1) \\ =& c \cdot \overline{f}(v_1 + \ker f),\end{aligned}$$

and part (2) follows.

(3) By Proposition 19.4.2 and the second part, we have

$$\dim_F(\operatorname{Im} f) = \dim_F(V_1/\ker f) = \dim_F V_1 - \dim_F(\ker f),$$

and the claim follows. □

Chapter 20

Lecture 20

We have proved basic properties of vector spaces over a field F. Here we will explore their implications in *field theory*.

20.1 Previous results in the language of linear algebra

We have motivated our digression to vector spaces over fields by considering the conclusions of Proposition 8.3.1 and Theorem 9.1.1. Here we rephrase those conclusions using terminologies from linear algebra.

Proposition 20.1.1. *Suppose F is a field and $f(x) \in F[x]$ is a polynomial of degree n, where n is a positive integer. Then $(\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1})$ is an F-basis of $F[x]/\langle f\rangle$, where $\overline{x}^i := x^i + \langle f\rangle$ for every integer i in $[0, n-1]$. In particular,* $\dim_F F[x]/\langle f\rangle = \deg f$.

Proof. By Proposition 8.3.1, every element of $F[x]/\langle f\rangle$ can be uniquely written as

$$(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}) + \langle f\rangle = \sum_{i=0}^{n-1} c_i \overline{x}^i.$$

Hence the F-span of $\{\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}\}$ is $F[x]/\langle f\rangle$. Moreover if $\sum_{i=0}^{n-1} c_i\overline{x}^i = 0$, then because of the uniqueness the above expression we obtain that c_i's are 0. This implies that $\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}$ are F-linearly independent. The claim follows. □

Proposition 20.1.2. *Suppose E is a field extension of F, and $\alpha \in E$ is algebraic over F. Then $(1, \alpha, \ldots, \alpha^{n-1})$ is an F-basis of $F[\alpha]$ where $n = \deg m_{\alpha,F}$. In particular,* $\dim_F F[\alpha] = \deg m_{\alpha,F}$.

Proof. By Theorem 9.1.1, every element of $F[\alpha]$ can be uniquely written as

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

for some $c_0, \ldots, c_{n-1} \in F$ where $n = \deg m_{\alpha,F}$. Hence the F-span of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is $F[\alpha]$. Moreover if $\sum_{i=0}^{n-1} c_i\alpha^i = 0$, then because of the uniqueness the above expression we obtain that c_i's are 0. This implies that $1, \alpha, \ldots, \alpha^{n-1}$ are F-linearly independent. The claim follows. □

20.2 Finite fields and vector spaces

Suppose F is a finite field and V is a vector space over F. If $\dim_F V = n$, then by Lemma 19.2.4, we have that $V \simeq F^n$, and so

$$|V| = |F|^{\dim_F V}. \tag{20.1}$$

This helps us get a strong condition for the tower of finite fields.

Proposition 20.2.1. *If $\mathbb{F}_{p^m}$ can be embedded into $\mathbb{F}_{p^n}$, then $m|n$.*

Proof. If $\mathbb{F}_{p^m}$ can be embedded into $\mathbb{F}_{p^n}$, we can view $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_{p^m}$. Since these are finite sets, $\dim_{\mathbb{F}_{p^m}} \mathbb{F}_{p^n} = d < \infty$. Hence by (20.1), we have

$$|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d, \qquad \text{which implies that} \qquad n = md.$$

This completes the proof. □

One can use the cardinality of the group of units of finite fields to prove the same result. Assuming that $\mathbb{F}_{p^m}$ can be embedded in $\mathbb{F}_{p^n}$, we deduce that the group of units of $\mathbb{F}_{p^m}$ can be embedded into the group of units of $\mathbb{F}_{p^n}$. Hence $p^m - 1|p^n - 1$. From this one can show that $m|n$. As you can see the presented proof, which is based on linear algebra, is much more natural.

Exercise 20.2.2. *Suppose m and n are positive integers and $m|n$. Prove that $\mathbb{F}_{p^m}$ can be embedded into $\mathbb{F}_{p^n}$.*

20.3 Tower rule for field extensions

We have already seen in Proposition 20.2.1 how useful it is to think about a field extension E of F as an F-vector space.

Definition 20.3.1. *Suppose E is a field extension of F. Then we can view E as an F-vector space (see Example 19.1.3). The dimension $\dim_F E$ of E as an F-vector space is denoted by $[E : F]$ and it is called the* degree of this field extension.

Theorem 20.3.2 (Tower rule)**.** *Suppose L is a field extension of E, and E is a field extension of F. Then*

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

in particular, if one of the sides is finite, then the other side is finite as well.

$$\begin{tikzcd} L \arrow[d, dash] \\ E \arrow[d, dash] \\ F \end{tikzcd} \tag{20.2}$$

We often use a diagram as in (20.2) to show field extensions. In this type of diagram, we connect two fields if one is a subfield of the other. The subfield is located lower than the larger field.

Proof of Theorem 20.3.2. If $[L : F] = n < \infty$, then there is a finite F-spanning set $\{v_1, \ldots, v_n\}$. Hence the L-span of $\{v_1, \ldots, v_n\}$ is also L, and so by Theorem 19.3.2, $[L : E] \le n$. And also, by Proposition 19.4.2, we have

$$[E : F] = \dim_F E \le \dim_F L < \infty.$$

Therefore from this point on, we can and will assume that

$$[L : E] = m < \infty \quad \text{and} \quad [E : F] = n < \infty.$$

Suppose $(\ell_1, \ldots, \ell_m)$ is an E-basis of L, and $(e_1, \ldots, e_n)$ is an F-basis of E. We prove that

$$\{\ell_i e_j \mid 1 \le i \le m, 1 \le j \le n\}$$

(with respect to some ordering) is an F-basis of L. We do this in two steps.

Step 1. $\mathrm{Span}_F(\ell_i e_j \mid 1 \le i \le m, 1 \le j \le n) = L$.

Proof of Step 1. Every $\ell \in L$ can be written as an E-linear combination of ℓ_i's. This means there are $x_i \in E$ such that

$$\ell = x_1 \ell_1 + \cdots + x_m \ell_m. \tag{20.3}$$

Every element of E can be written as an F-linear combination of e_j's. Hence for every i, there are $y_{ij} \in F$ such that

$$x_i = y_{i1} e_1 + \cdots + y_{in} e_n. \tag{20.4}$$

By (20.3) and (20.4), we deduce that

$$\begin{aligned}\ell &= \sum_{i=1}^m x_i \ell_i = \sum_{i=1}^m \Big(\sum_{j=1}^n y_{ij} e_j\Big)\ell_i \\ &= \sum_{1 \le i \le m, 1 \le j \le n} y_{ij}\ \ell_i e_j.\end{aligned}$$

This means ℓ can be written as an F-linear combination of $\ell_i e_j$'s. This completes the proof of Step 1.

Step 2. $\ell_i e_j$'s are F-linearly independent.

Proof of Step 2. Suppose

$$\sum_{1 \le i \le m, 1 \le j \le n} y_{ij}\ \ell_i e_j = 0 \tag{20.5}$$

for some y_{ij}'s in F. Then by (20.5), we have

$$\sum_{i=1}^m \Big(\sum_{j=1}^n y_{ij} e_j\Big)\ell_i = 0. \tag{20.6}$$

Notice that for every i, $x_i := \sum_{j=1}^n \sum_{j=1}^n y_{ij} e_j$ is in E. Since ℓ_i's are E-linearly independent, by (20.6) we deduce that $x_i = 0$ for every i. Hence we have

$$\sum_{j=1}^n \sum_{j=1}^n y_{ij} e_j = 0 \tag{20.7}$$

for every index i. Since e_j's are F-linearly independent, by (20.7) we obtain that $y_{ij} = 0$ for every pair of indexes i and j. This completes the proof of the second step.

By Steps 1 and 2, we deduce that

$$[L : F] = |\{\ell_i e_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}| = mn = [L : E][E : F],$$

which completes the proof. □

20.4 Some applications of the Tower Rule for field extensions

Here we mention some examples on how one can use the Tower Rule.

Example 20.4.1. *Suppose E is a field extension of $\mathbb{Q}$ such that $[E : \mathbb{Q}] = 2^n$ for some positive integer n. Then $x^3 - 2$ is irreducible in $E[x]$.*

Proof. Suppose to the contrary that $x^3 - 2$ is not irreducible in $E[x]$. Then by the irreducibility criterion for degree 2 and 3 polynomials (see 10.1.1), we deduce that there is $\alpha \in E$ which is a zero of $x^3 - 2$. Then $\mathbb{Q}[\alpha]$ is an *intermediate field*; that means we have the tower of field extensions given in (20.9). Hence by the Tower Rule (see Theorem 20.3.2), we have $[E : \mathbb{Q}] = [E : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}]$. Therefore by Proposition 20.1.2 and our hypothesis, we obtain that

$$2^n = [E : \mathbb{Q}[\alpha]] \deg m_{\alpha,\mathbb{Q}}. \tag{20.8}$$

$$\begin{tikzcd} E \arrow[d, dash] \\ \mathbb{Q}[\alpha] \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd} \tag{20.9}$$

So we it is useful to find the minimal polynomial $m_{\alpha,\mathbb{Q}}$ of α over $\mathbb{Q}$. Notice that α is a zero of $x^3 - 2$, $x^3 - 2$ is monic, and by Eisenstein's irreducibility criterion (see Theorem 12.2.1), $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$. Hence by Theorem 8.2.5, $m_{\alpha,\mathbb{Q}}(x) = x^3 - 2$. Thus by (20.8), 3 is a divisor of 2^n which is a contradiction. This completes the proof. □

Example 20.4.2. *Suppose E is a field extension of F and $\alpha \in E$ is algebraic over F. Suppose $[F[\alpha] : F]$ is odd. Then $F[\alpha] = F[\alpha^2]$.*

Proof. Notice that $F[\alpha]$ is a field extension of $F[\alpha^2]$.

So we have the tower of field extensions given in (20.11). Hence by the Tower Rule (see Theorem 20.3.2), we have

$$[F[\alpha] : F] = [F[\alpha] : F[\alpha^2]][F[\alpha^2] : F].$$

Therefore by Proposition 20.1.2 and our hypothesis, we obtain that

$$(\deg m_{\alpha,F[\alpha^2]})[F[\alpha^2] : F] \text{ is odd.} \tag{20.10}$$

$$\begin{tikzcd} F[\alpha] \arrow[d, dash] \\ F[\alpha^2] \arrow[d, dash] \\ F \end{tikzcd} \tag{20.11}$$

By (20.10), we have that $\deg m_{\alpha,F[\alpha^2]}$ is odd. Notice that α is a zero of $x^2 - \alpha^2 \in F[\alpha^2]$. Hence $\deg m_{\alpha,F[\alpha^2]} \leq 2$. As the only positive odd integer less than or equal to 2 is 1, we have $\deg m_{\alpha,F[\alpha^2]} = 1$. This implies that $\alpha \in F[\alpha^2]$, and so $F[\alpha] \subseteq F[\alpha^2]$. The claim follows. □

Example 20.4.3. *Suppose $\alpha, \beta \in \mathbb{C}$ are algebraic over $\mathbb{Q}$. Let $f(x) := m_{\alpha,\mathbb{Q}}(x)$ and $g(x) := m_{\beta,\mathbb{Q}}(x)$. Then*

$$f \text{ is irreducible in } (\mathbb{Q}[\beta])[x] \iff g \text{ is irreducible in } (\mathbb{Q}[\alpha])[x].$$

Proof. ($\Rightarrow$) We will be using the right and the left legs of the diagram given in (20.12).

$$\begin{tikzcd}
& \mathbb{Q}[\alpha,\beta] \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
\mathbb{Q}[\alpha] \arrow[dr, dash] & & \mathbb{Q}[\beta] \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd} \tag{20.12}$$

Going through the right leg of the diagram in (20.12), using the Tower Rule (see Theorem 20.3.2) and Proposition 20.1.2, we obtain that

$$\begin{aligned}
[\mathbb{Q}[\alpha,\beta] : \mathbb{Q}] =& [\mathbb{Q}[\alpha,\beta] : \mathbb{Q}[\beta]][\mathbb{Q}[\beta] : \mathbb{Q}] \\
=& (\deg m_{\alpha,\mathbb{Q}[\beta]})(\deg m_{\beta,\mathbb{Q}}).
\end{aligned} \tag{20.13}$$

Notice that since α is a zero of f, f is monic and irreducible in $(\mathbb{Q}[\beta])[x]$, by Theorem 8.2.5, we have $m_{\alpha,\mathbb{Q}[\beta]}(x) = f(x) = m_{\alpha,\mathbb{Q}}(x)$. Hence, by (20.13), we have that

$$[\mathbb{Q}[\alpha,\beta] : \mathbb{Q}] = (\deg m_{\alpha,\mathbb{Q}})(\deg m_{\beta,\mathbb{Q}}). \tag{20.14}$$

Going through the left leg of the diagram in (20.12), using the Tower Rule (see Theorem 20.3.2) and Proposition 20.1.2, we obtain that

$$\begin{aligned}
[\mathbb{Q}[\alpha,\beta] : \mathbb{Q}] =& [\mathbb{Q}[\alpha,\beta] : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}] \\
=& (\deg m_{\beta,\mathbb{Q}[\alpha]})(\deg m_{\alpha,\mathbb{Q}}).
\end{aligned} \tag{20.15}$$

By (20.14) and (20.15), we deduce that

$$\deg m_{\beta,\mathbb{Q}[\alpha]} = \deg m_{\beta,\mathbb{Q}}. \tag{20.16}$$

Notice that since β is a zero of $m_{\beta,\mathbb{Q}} \in (\mathbb{Q}[\alpha])[x]$, we obtain that

$$m_{\beta,\mathbb{Q}[\alpha]} | \deg m_{\beta,\mathbb{Q}}. \tag{20.17}$$

By (20.16) and (20.17), we obtain that $g(x) = m_{\beta,\mathbb{Q}}(x) = m_{\beta,\mathbb{Q}[\alpha]}(x)$. This implies that $g(x)$ is irreducible in $(\mathbb{Q}[\alpha])[x]$.

($\Leftarrow$) This direction follows by a similar argument. □

Let's remark that if L is a field extension of E, E is a field extension of F, and $\alpha \in L$ is algebraic over F, then α is a zero of $m_{\alpha,F} \in E[x]$. Hence $m_{\alpha,E} | m_{\alpha,F}$; this is a generalization of (20.17).

20.5 Algebraic closure in a field extension

Suppose E is a field extension of F. The *algebraic closure of F in E* is the set of all the elements of E that are algebraic over F. Here we will prove that the algebraic closure of F in E is a subfield of E. We start with proving that a field extension of finite degree is an algebraic extension.

Lemma 20.5.1. *Suppose E is a field extension of F of finite degree. Then every $\alpha \in E$ is algebraic over F.*

We say a field extension E of F is an *algebraic extension* if every $\alpha \in E$ is algebraic. So we are proving that a field extension of finite degree is algebraic.

Proof of Lemma 20.5.1. Suppose $[E : F] = n$. Then by Theorem 19.3.1, every $n + 1$ elements of E are F-linearly dependent. Hence $1, \alpha, \ldots, \alpha^n$ are F-linearly dependent. Thus there are $c_0, \ldots, c_n \in F$ that are not all zero and

$$c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0.$$

This means that α is algebraic over F. □

Theorem 20.5.2 (Algebraic closure in a field extension)**.** *Suppose E is a field extension of F. Let*

$$K := \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}.$$

Then K is a field extension of F.

Proof. Suppose $\alpha, \beta \in K$. Then by Proposition 20.1.2, we have $[F[\alpha] : F] = \deg m_{\alpha,F} < \infty$. Moreover as β is algebraic over $F[\alpha]$, we have $[F[\alpha, \beta] : F[\alpha]] < \infty$. Hence by the Tower Rule (see Theorem 20.3.2) we obtain that

$$[F[\alpha, \beta] : F] = [F[\alpha, \beta] : F[\alpha]][F[\alpha] : F] < \infty. \tag{20.18}$$

By Lemma 20.5.1 and (20.18), we deduce that $F[\alpha, \beta]$ is an algebraic extension of F; this means that $F[\alpha, \beta] \subseteq K$. This implies that $F \subseteq K$, $\alpha \pm \beta$ and $\alpha\beta$ are in K, and if $\beta \neq 0$, then $\alpha\beta^{-1}$ is in K, as well. Altogether, we deduce that K is field extension of F. This completes the proof. □

20.6 Geometric constructions by ruler and compass

Let's recall some ancient Euclidean geometry problems. *Can we construct* $\sqrt[3]{2}, \pi$, *or angle* $20°$ *using ruler and compass?* Let's formulate it properly what it means to *construct* a number. We start with a unit segment. The end points are considered *constructed*. If two points are constructed, then the line which passes through them is considered constructed. The circles that are centered at one of these points and pass through the other are called constructed. The points of intersection of constructed circles and lines are considered constructed points. A number is called constructed if its absolute value is the distance of two constructed points. The following theorem gives us an excellent understanding of constructed points.

Theorem 20.6.1. *Suppose the initial points are* $(0,0)$ *and* $(1,0)$*. If* (α,β) *is a constructed point, then* $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ *and* $[\mathbb{Q}[\beta]:\mathbb{Q}]$ *are powers of* 2*.*

Here only the main ideas will be presented. To get to the point (α,β), we have to construct finitely many lines and circles, and consider their intersection points. To find the coordinates of intersection points we end up solving degree 1 and degree 2 polynomials with coefficients that are in the ring generated by the coordinates of the constructed points that we have so far. This means there is a tower of field extensions

$$\mathbb{Q} =: F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$$

such that $[F_{i+1}:F_i]=2$ for every i and $\alpha\in F_n$. By the Tower Rule, $[F_n:\mathbb{Q}]$ is power of 2. Since $\mathbb{Q}[\alpha]$ is an intermediate subfield, by the Tower Rule we deduce that $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ divides $[F_n:\mathbb{Q}]$. Hence $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ is a power of 2.

Corollary 20.6.2. $\sqrt[3]{2}$ *and* π *cannot be constructed by ruler and compass.*

Proof. By Theorem 20.6.1, if α can be constructed by ruler and compass, then $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ is a power of 2. In particular, α is algebraic. Hence π cannot be constructed (we do not prove this here, but it can be proved that π is not algebraic over $\mathbb{Q}$). Notice that $\deg m_{\sqrt[3]{2},\mathbb{Q}}=3$, and so $\sqrt[3]{2}$ cannot be constructed by ruler and compass. □

Exercise 20.6.3. *Show that* $\deg m_{\cos 20^\circ,\mathbb{Q}}=3$*, and use this to deduce the angle* 20° *cannot be constructed by ruler and compass. (Hint:* $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$*.)*

By the above Exercise, we can deduce that there is no general method of dividing a given angle into three equal parts using only ruler and compass.

Chapter 21

Lecture 21

By now we have a basic understanding of vector spaces over a field and how it can help us study field extensions. We go back and further study splitting fields. Here we focus on the splitting field of $x^n - 1$ over $\mathbb{Q}$. Let us recall that by Example 17.2.1, we have that $\mathbb{Q}[\zeta_n]$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$, where $\zeta_n := e^{2\pi i/n}$, and

$$x^n - 1 = (x-1)(x-\zeta_n)\cdots(x-\zeta_n^{n-1}). \tag{21.1}$$

This field has a historical significance, because of its role in the initial modern attempts towards proving Fermat's last conjecture. We want to answer a very basic question about this field: what is $[\mathbb{Q}[\zeta_n]:\mathbb{Q}]$? By Proposition 20.1.2, we have

$$[\mathbb{Q}[\zeta_n]:\mathbb{Q}] = \deg m_{\zeta_n,\mathbb{Q}}.$$

Hence we need to find the minimal polynomial of ζ_n over $\mathbb{Q}$.

21.1 Cyclotomic polynomials

In this section, we will arrive at the definition of the n-th cyclotomic polynomial. This will be done as we investigate the minimal polynomial of ζ_n over $\mathbb{Q}$.

Notice that since ζ_n is a zero of $x^n - 1$, $m_{\zeta_n,\mathbb{Q}}$ divides $x^n - 1$. Hence by (21.1) and the fact the $\mathbb{C}[x]$ is a UFD, we deduce that

$$m_{\alpha,\mathbb{Q}}(x) = (x-\zeta_n^{i_1})\cdots(x-\zeta_n^{i_m})$$

for some integers i_j's in $[1,n]$. As ζ_n is a zero of $m_{\zeta_n,\mathbb{Q}}$, without loss of generality, we can and will assume that $i_1 = 1$.

By Lemma 16.2.2, if E is a field extension of F and $\alpha, \alpha' \in E$ are two zeros of an irreducible polynomial $f \in F[x]$, then there is an *F-isomorphism* $\theta : F[\alpha] \to F[\alpha']$ such that $\theta(\alpha) = \alpha'$; an F-isomorphism is a ring isomorphism which F-linear. Applying this result for the two zeros ζ_n and $\zeta_n^{i_j}$ of the irreducible polynomial $m_{\zeta_n,\mathbb{Q}} \in \mathbb{Q}[x]$, we obtain a $\mathbb{Q}$-isomorphism $\theta_j : \mathbb{Q}[\zeta_n] \to \mathbb{Q}[\zeta_n^{i_j}]$ such that $\theta_j(\zeta_n) = \zeta_n^{i_j}$. Notice that, since θ_j is a ring isomorphism, the multiplicative order of ζ_n and $\theta_j(\zeta_n)$ are the same. As $o(g^k) = \frac{o(g)}{\gcd(o(g),k)}$, $o(\zeta_n) = n$, and $\theta_j(\zeta_n) = \zeta_n^{i_j}$, we deduce that $\gcd(n, i_j) = 1$ for every j. This takes us to the definition of the n-th cyclotomic polynomial.

Definition 21.1.1. *The n-th cyclotomic polynomial is*

$$\Phi_n(x) := \prod_{1 \le i \le n, \gcd(i,n)=1} (x - \zeta_n^i).$$

In particular, Φ_n is a monic polynomial of degree $\phi(n)$, wherer ϕ is the Euler-phi function.

By the above discussion, we have that $m_{\zeta_n,\mathbb{Q}}(x)$ divides $\Phi_n(x)$ in $\mathbb{C}[x]$. We will prove that $m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x)$.

21.2 Cyclotomic polynomials are integer polynomials

The following is a key property of cyclotomic polynomials that, among other things, help us prove cyclotomic polynomials are integer polynomials.

Theorem 21.2.1. *For every positive integer n, we have*

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{21.2}$$

Before we go to the details of the proof of Theorem 21.2.1, let us compare the degrees of the both sides of (21.2):

$$n = \sum_{d|n} \phi(d). \tag{21.3}$$

Proof of this formula is based on the partitioning of the set $[1..n] := \{1, \ldots, n\}$ in terms of the greatest common divisor of the elements with n. To be more precise, we let

$$C_{d,n} := \{i \in [1..n] \mid \gcd(i, n) = d\}. \tag{21.4}$$

Then $\{C_{d,n} \mid d|n\}$ is a partitioning of $[1..n]$. Moreover

$$i \in C_{d,n} \iff \gcd(i, n) = d \iff i = dj \text{ and } \gcd\left(j, \frac{n}{d}\right) = 1.$$

Hence

$$C_{d,n} = \{dj \mid j \in C_{1,\frac{n}{d}}\} \text{ which imlies that } |C_{d,n}| = |C_{1,\frac{n}{d}}| = \phi\Big(\frac{n}{d}\Big). \tag{21.5}$$

Therefore

$$n = |[1..n]| = \sum_{d|n} |C_{d,n}| = \sum_{d|n} \phi\Big(\frac{n}{d}\Big).$$

Finally we notice that as d ranges over all the positive divisors of n, so does $\frac{n}{d}$; that means $d \mapsto \frac{n}{d}$ is a bijection from the set of positive divisors of n to itself. Hence $\sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d)$, and (21.3) follows. We will be following the same steps to prove (21.2).

Proof of Theorem 21.2.1. Since $x^n - 1 = \prod_{i\in[1..n]}(x-\zeta_n^i)$ and $\{C_{d,n} \mid d|n\}$ is a partition of $[1..n]$, we have that

$$x^n - 1 = \prod_{d|n} \prod_{i\in C_{d,n}} (x-\zeta_n^i). \tag{21.6}$$

By (21.5), we have that

$$\prod_{i\in C_{d,n}} (x-\zeta_n^i) = \prod_{j\in C_{1,\frac{n}{d}}} (x-\zeta_n^{dj}). \tag{21.7}$$

Notice that $\zeta_n^d = e^{(2\pi i/n)d} = e^{2\pi i/(\frac{n}{d})} = \zeta_{\frac{n}{d}}$. So by (21.7), we deduce that

$$\prod_{i\in C_{d,n}} (x-\zeta_n^i) = \prod_{0\le j<\frac{n}{d}, \gcd(j,\frac{n}{d})=1} (x-\zeta_{\frac{n}{d}}^j) = \Phi_{\frac{n}{d}}(x). \tag{21.8}$$

By (21.6) and (21.8), we obtain

$$x^n - 1 = \prod_{d|n} \Phi_{\frac{n}{d}}(x). \tag{21.9}$$

As it is mentioned earlier, $d \mapsto \frac{n}{d}$ is a bijection from the set of positive divisors of n to itself. Hence by (21.9), (21.2) follows. □

Using we are ready to prove that cyclotomic polynomials are integer polynomials.

Corollary 21.2.2. *For every positive integer n, $\Phi_n(x) \in \mathbb{Z}[x]$.*

Proof. We proceed by strong induction on n. The base case is clear as $\Phi_1(x) = x - 1$. Next we prove the strong induction step. By the strong induction hypothesis, for every positive integer $m < n$, $\Phi_m(x) \in \mathbb{Z}[x]$. Hence

$$\Psi_n(x) := \prod_{d|n, d\neq n} \Phi_d(x) \in \mathbb{Z}[x], \tag{21.10}$$

and as Φ_d's are monic, $\Psi_n(x)$ is monic as well. By Theorem 21.2.1, we have

$$x^n - 1 = \Phi_n(x)\Psi_n(x). \tag{21.11}$$

As $x^n - 1, \Psi_n(x) \in \mathbb{Z}[x]$ and $\Psi_n(x)$ is monic, by the Long Division for elements in $\mathbb{Z}[x]$ (see Theorem 6.4.1) there are unique $q(x), r(x) \in \mathbb{Z}[x]$ such that

1. $x^n - 1 = q(x)\Psi_n(x) + r(x)$ and
2. $\deg r < \deg \Psi_n$.

Using the Long Division for elements in $\mathbb{C}[x]$, we see that the same q and r are the quotient and remainder of $x^n - 1$ divided by $\Psi_n(x)$ as elements of $\mathbb{C}[x]$. By (21.11), however, we have that the quotient and the remainder of $x^n - 1$ divided by $\Psi_n(x)$ as elements of $\mathbb{C}[x]$ are $\Phi_n(x)$ and 0, respectively. Hence $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$, and the claim follows. □

Let us remark that the last part of the above argument implies the following:

Lemma 21.2.3. *Suppose A is a subring of a unital commutative ring B and $1_B \in A$. Suppose $f, g \in A[x]$ and $\operatorname{ld}(f) \in A^\times$. If $f|g$ in $B[x]$, then $f|g$ in $A[x]$.*

Use long division in $A[x]$ and $B[x]$ to prove this Lemma. I leave it to you to fill out the details.

21.3 Cyclotomic polynomials are irreducible

The main goal of this section is to prove the following:

Theorem 21.3.1. *For every integer n, $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.*

As before the general steps are proceeding by contradiction, going from $\mathbb{Q}$ to $\mathbb{Z}$, and using the residue maps modulo primes. The last step, however, will be more subtle than the other examples that we have done so far.

Proof of Theorem 21.3.1. Suppose to the contrary that $\Phi_n(x)$ is not irreducible in $\mathbb{Q}[x]$. Then $\Phi_n(x) = f(x)g(x)$ for some non-constant smaller degree polynomials f and g. Since $\Phi_n(x)$ is a monic integer polynomial, it is a primitive polynomial. By Gauss's lemma (see Corollary 15.4.3), we have $\Phi_n(x) = \overline{f}(x)\overline{g}(x)$ where $\overline{f}$ and $\overline{g}$ are primitive forms of f and g, respectively. Notice that ζ_n is a zero Φ_n, it is either a zero of $\overline{f}$ or a zero of $\overline{g}$. Without loss of generality, we can and will assume that ζ_n is a zero of $\overline{f}$. Every other zero ζ of $\overline{f}$ is a zero of $\Phi_n(x)$, and so the multiplicative order of ζ (as an element of $\mathbb{C}^\times$) is n.

(Here is where the magic is happening.)

If p is a prime which does not divide n and $\zeta \in \mathbb{C}^\times$ has multiplicative order n, then the multiplicative order of ζ^p is also n. Therefore ζ^p is a zero of $\Phi_n(x)$, and so it is a zero of either $\overline{f}$ or $\overline{g}$.

Claim 1. *If ζ is a zero of $\overline{f}$ and p is a prime which does not divide n, then ζ^p is a zero of $\overline{f}$ as well.*

Proof of Claim 1. Suppose to the contrary that $\overline{f}(\zeta^p) \neq 0$. Since $o(\zeta^p) = n$, $\Phi_n(\zeta^p) = 0$. As $\overline{f}(\zeta^p) \neq 0$ and $\Phi_n(\zeta^p) = \overline{f}(\zeta^p)\overline{g}(\zeta^p)$, we deduce that $\overline{g}(\zeta^p) = 0$. This means ζ is a common zero of $\overline{f}(x)$ and $\overline{g}(x^p)$. Thus $m_{\zeta,\mathbb{Q}}(x)$ is a common divisor of $\overline{f}(x)$ and $\overline{g}(x^p)$ in $\mathbb{Q}[x]$. Let $h(x)\mathbb{Z}[x]$ be the primitive form of $m_{\zeta,\mathbb{Q}}(x)$. By Gauss's lemma (see Corollary 15.4.3), $h(x)$ is a common divisor of $\overline{f}(x)$ and $\overline{g}(x^p)$ in $\mathbb{Z}[x]$. As $\overline{f}$ is monic, so is h. Therefore $c_p(h)$ is a common divisor of $c_p(\overline{f}(x))$ and $c_p(\overline{g}(x^p))$ where $c_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is the residue map modulo p. Notice that h is a monic non-constant polynomial, so is $c_p(h)$.

(Here you see why we considered raising to power p at the first place.)

Since $\mathbb{Z}_p[x]$ is of characteristic p, by Fermat's little theorem we have

$$c_p(h(x))^p = c_p(h(x^p)). \tag{21.12}$$

To see this better, notice that in $\mathbb{Z}_p[x]$ we have

$$(\sum_{i=0}^{\infty} a_i x^i)^p = \sum_{i=0}^{\infty} a_i^p (x^i)^p = \sum_{i=0}^{\infty} a_i (x^p)^i.$$

So $c_p(h)$ is a non-constant common divisor of $c_p(\overline{f})$ and $c_p(\overline{g})^p$. Let $\ell(x)$ be a prime factor of $c_p(h)$. Then $\ell(x)$ divides $c_p(\overline{g})^p$, and so $\ell(x)$ divides $c_p(\overline{g})$ as $\mathbb{Z}_p[x]$ is a UFD. Therefore $\ell(x)^2$ divides

$$c_p(\overline{f})c_p(\overline{g}) = c_p(\overline{f}\overline{g}) = c_p(\Phi_n). \tag{21.13}$$

As $c_p(\Phi_n)$ divides $x^n - 1$ in $\mathbb{Z}_p[x]$, $\ell(x)^2$ divides $x^n - 1$ in $\mathbb{Z}_p[x]$. Hence $x^n - 1$ has multiple zeros in its splitting field over $\mathbb{Z}_p$. By Proposition 18.3.4, we deduce that $\gcd(x^n - 1, nx^{n-1}) \neq 1$. This is a contradiction as $p \nmid n$ and $x \nmid x^n - 1$. This completes the proof of Claim 1. □

Claim 2. Suppose i is a positive integer and $\gcd(i, n) = 1$. If ζ is a zero of $\overline{f}$, then ζ^i is a zero of $\overline{f}$.

Proof of Claim 2. We proceed by induction on the number k of prime factors of i. In the base case of $k = 0$, we have $i = 1$, and there is nothing to prove. Suppose $i = p_1 \cdots p_{k+1}$, where p_j's are primes that do not divide n. By the induction hypothesis $\zeta^{p_1 \cdots p_k}$ is a zero of $\overline{f}$. By Claim 1, we deduce that

$$(\zeta^{p_1 \cdots p_k})^{p_{k+1}} = \zeta^i$$

is a zero of $\overline{f}$. This completes the proof of Claim 2. □

By Claim 2, since ζ_n is a zero of $\overline{f}$, ζ_n^i is a zero of $\overline{f}$ if i is a positive integer and $\gcd(i, n) = 1$. This implies that $\Phi_n(x)$ divides $\overline{f}$, which is a contradiction as $\deg \overline{f} < \deg \Phi_n$. This completes the proof. □

21.4 The degree of cyclotomic extensions

Field $\mathbb{Q}[\zeta_n]$ is called a *cyclotomic extension*.

Theorem 21.4.1. *Suppose n is a positive integer and $\zeta_n := e^{2\pi i/n}$. Then the minimal polynomial of ζ_n over $\mathbb{Q}$ is $m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x)$ and $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n)$.*

Proof. We have that ζ_n is a zero of $\Phi_n(x)$, $\Phi_n(x)$ is a monic polynomial, and $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$ (by Theorem 21.3.1). Hence by Theorem 8.2.5, we have that $m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x)$. By Proposition 20.1.2, we have

$$[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \deg m_{\zeta_n,\mathbb{Q}} = \deg \Phi_n = \phi(n),$$

which completes the proof. □

Chapter 22

Lecture 22

22.1 The group of automorphism of a field extension.

Through out this course one of our main goals has been understanding zeros of polynomials. We proved the existence and the uniqueness (up to an isomorphism) of a smallest field which contains all the zeros of a given polynomial (a splitting field). A better understanding of splitting fields can help us to learn more about the zeros of polynomials. One of our main tools of characterizing (intricate) objects is their group of *symmetries*. The group of symmetries of a field extension E of F is defined as follows.

Definition 22.1.1. *For a field extension E of F, let*

$$\mathrm{Aut}_F(E) := \{\theta : E \to E \mid \theta \textit{ is a ring isomorphism, and } F\textit{-linear}\}.$$

An element of $\mathrm{Aut}_F(E)$ *is called an* F-automorphism. *An F-linear, ring homomorphism is called an* F-homomorphism.

One can easily see that $\mathrm{Aut}_F(E)$ is a group under composition. We would like to know how much $\mathrm{Aut}_F(E)$ tells us about the field extension.

Similar to the proof of the uniqueness of splitting fields, we need to work with two, possibly different, copies of the *base* field F, and with not necessarily surjective ring homomorphisms: we proved the *isomorphism extension theorem* in order to deduce the *uniqueness of splitting fields* up to an isomorphism. That is why we introduce the following notation.

Definition 22.1.2. *Suppose $\theta : F \to F'$ is a field isomorphism, E is a field extension of F, and L' is a field extension of F'. Then*

$$\mathrm{Emb}_\theta(E, L') := \{\widehat{\theta} : E \to L' \mid \widehat{\theta} \textit{ injective ring homomorphism and } \widehat{\theta}|_F = \theta\}$$

and an element of $\mathrm{Emb}_\theta(E, L')$ *is called an* θ-embedding. *An isomorphism which is an θ-embedding is called an* θ-isomorphism, *and the set of θ-isomorphisms is denoted by* $\mathrm{Iso}_\theta(E, L')$. *When $F' = F$ and $\theta = \mathrm{id}_F$, we write* $\mathrm{Emb}_F(E, L')$ *instead of* $\mathrm{Emb}_{\mathrm{id}_F}(E, L')$. *Instead of saying* id_F*-embedding, we say* F-embedding.

Notice that $\widehat{\theta}$ is in $\mathrm{Emb}_\theta(E, L')$ exactly when the following is a commutative diagram.

$$\begin{tikzcd}
E \arrow[r, "\widehat{\theta}"] \arrow[d, dash] & L' \arrow[d, dash] \\
F \arrow[r, "\theta"] & F'
\end{tikzcd}$$

Lemma 22.1.3. *If $[E : F] < \infty$, then $\mathrm{Emb}_F(E, E) = \mathrm{Aut}_F(E)$.*

Proof. Clearly $\mathrm{Aut}_F(E) \subseteq \mathrm{Emb}_F(E, E)$. Suppose $\theta \in \mathrm{Emb}_F(E, E)$. To show that θ is an F-automorphism, it suffices to argue why θ is surjective. By the first isomorphism theorem for vector spaces (see Theorem 19.5.1), we have

$$\dim_F \mathrm{Im}(\theta) + \dim_F \ker(\theta) = \dim_F E.$$

Since θ is a injective, $\ker \theta = 0$. Hence $\dim_F \mathrm{Im}(\theta) = \dim_F E$. Since $\mathrm{Im}_F(\theta)$ is a subspace of E and it has the same dimension as E, by Proposition 19.4.2 $\mathrm{Im}(\theta) = E$. This completes the proof. □

The following easy lemma is the corner stone of our understanding of the group of symmetries of algebraic field extensions.

Lemma 22.1.4. *Suppose $\theta : F \to F'$ is a field isomorphism, E is a field extension of F, and L' is a field extension of F'. Suppose $f(x) \in F[x]$ and $\alpha \in E$ is a zero of f. Then*

$$\textit{for every } \widehat{\theta} \in \mathrm{Emb}_\theta(E, L'),\ \widehat{\theta}(\alpha) \textit{ is a zero of } \theta(f).$$

In particular, if L is a field extension of F, then

$$\textit{for every } F\textit{-embedding } \widehat{\theta} : E \to L,\ \theta(\alpha) \textit{ is a zero of } f.$$

Proof. Suppose $f(x) = \sum_{i=0}^n c_i x^i$. Then $\sum_{i=0}^n c_i \alpha^i = 0$. Therefore

$$0 = \widehat{\theta}\Big(\sum_{i=0}^n c_i \alpha^i\Big) = \sum_{i=0}^n \widehat{\theta}(c_i)\widehat{\theta}(\alpha)^i = \sum_{i=0} \theta(c_i)\widehat{\theta}(\alpha)^i = \theta(f)(\widehat{\theta}(\alpha)),$$

and the claim follows. □

22.2 Normal extensions

The following theorem and the ideas involved in its proof play an important role in our understanding of field extensions of finite degree.

Theorem 22.2.1. *Suppose E is a field extension of F and $[E : F] < \infty$. Then the following statements are equivalent.*

1. *There is $f \in F[x]$ such that E is a splitting field of f over F.*

2. *For every field extension L of E and $\theta \in \mathrm{Aut}_F(L)$, we have $\theta(E) = E$.*

3. *For every $\beta \in E$, $m_{\beta,F}(x) = (x - \beta_1)\cdots(x - \beta_m)$ for some $\beta_1, \ldots, \beta_m \in E$.*

Each one of these properties gives us a very different perspective of the given field extension.

1. The first property (in terms of splitting fields) is very *concrete* and one can construct many examples with it.

2. The second property gives us a relation between symmetries of field extensions of E over F and symmetries of E over F. It is quite surprising that a property about E and F tells us something about symmetries of every field extension of E.

3. In contrast with the second property, the third property is completely internal. It is all about E and F and no other additional information is involved.

The second and the third properties make sense even if the given field extension is not of finite degree. The first property, however, implies that the field extension is of finite degree. One can talk about a *splitting field of a family of polynomials*, replace the statement with this extended notation, and still get equivalent properties. This is a key result for understanding algebraic extensions of infinite degree. Here, however, we do not discuss infinite degree algebraic extensions.

Definition 22.2.2. *Suppose E is an algebraic extension of F. We say E is a* normal *field extension of F if the third property in Theorem 22.2.1 holds.*

Proof of Theorem 22.2.1. (1) ⇒ (2) Since E is a splitting field of f over F, there are $\alpha_1, \ldots, \alpha_n \in E$ such that

$$f(x) = \mathrm{ld}(f)\prod_{i=1}^{n}(x - \alpha_i) \quad \text{and} \quad E = F[\alpha_1, \ldots, \alpha_n].$$

Suppose L is a field extension of E and $\theta \in \mathrm{Aut}_F(L)$. Then by Lemma 22.1.4, $\theta(\alpha_i)$ is a zero of f in L. Since $\alpha_1, \ldots, \alpha_n$ are the only zeros of f in $E \subseteq L$, we obtain that

$$\theta(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\} \tag{22.1}$$

for every i. As θ is injective, form (22.1) we deduce that θ permutes elements of $\{\alpha_1, \ldots, \alpha_n\}$. Therefore

$$\theta(E) = \theta(F[\alpha_1, \ldots, \alpha_n]) = \theta(F)[\theta(\alpha_1), \ldots, \theta(\alpha_n)] = F[\alpha_1, \ldots, \alpha_n] = E.$$

(2) ⇒ (3) This is the most technical part of the proof. For every $\beta \in E$, we want to show that there are β_i's in E such that $m_{\beta,F}(x) = \prod_{i=1}^{m}(x - \beta_i)$. The second property is about the field extensions of E. Hence we need to work with field extensions of E that contain all the zeros β_i of $m_{\beta,F}$, say L is such a field. Since β and β_i

are zeros of the irreducible polynomial $m_{\beta,F}(x)$, by Lemma 16.2.2 there is an F-isomorphism $\theta_i : F[\beta] \to F[\beta_i]$ such that $\theta_i(\beta) = \beta_i$. *If we manage to extend θ_i to an F-automorphism $\widehat{\theta}_i$ of L*, then by hypothesis, $\widehat{\theta}_i(E) = E$, which implies that

$$\widehat{\theta}_i(\beta) = \theta_i(\beta) = \beta_i$$

is in E, and the claim follows. Hence we focus on extending θ_i to an F-isomorphism from L to itself. This reminds of the *isomorphism extension theorem* (see Theorem 17.1.1). By the isomorphism extension theorem, we can extend θ_i to an F-automorphism $\widehat{\theta}_i$ of L if L is a splitting field of a polynomial over F.

Altogether we have proved that the claim follows if we show the existence of a field L with the following properties.

1. L is a field extension of E.
2. There are β_i's in L such that $m_{\beta,F}(x) = \prod_{i=1}^{m}(x - \beta_i)$.
3. There is $f \in F[x]$ such that L is a splitting field of f over F.

Notice that the conditions (2) and (3) are satisfied by a splitting field of $m_{\beta,F}$ over F, but this field does not necessarily contain E as a subfield. The following is a common technique that is used to construct a field which is a splitting field of a polynomial over F and contains E as a subfield. [1]

Suppose $(\gamma_1, \ldots, \gamma_n)$ is an F-basis of E, and let

$$f(x) := m_{\beta,F}(x) m_{\gamma_1,F}(x) \cdots m_{\gamma_n,F}(x) \in F[x].$$

Suppose L is a splitting field of f over E. Clearly L satisfies the first and the second desired properties that are mentioned above. Next we show that L is a splitting field of f over F. Since L is a splitting field of f over E, there are β_i's and $\gamma_{i,j}$'s in L such that

$$m_{\beta,F}(x) = \prod_{i=1}^{m}(x - \beta_i) \quad \text{and} \quad m_{\gamma_i,F}(x) = \prod_{j=1}^{m_i}(x - \gamma_{i,j}), \tag{22.2}$$

and

$$L = E[\beta_1, \ldots, \beta_m, \gamma_{1,1}, \ldots, \gamma_{n,m_n}]. \tag{22.3}$$

Since $\gamma_i \in E \subseteq L$ is a zero of $m_{\gamma_i,F}$, $\gamma_i \in \{\gamma_{i,1}, \ldots, \gamma_{i,m_i}\}$. Hence without loss of generality we can and will assume that $\gamma_{i,1} = \gamma_i$ for every i.

Notice that (22.3) means that if a subfield of L contains E, β_i's and $\gamma_{i,j}$'s, then it is the entire L. On the other hand, as γ_i's form an F-basis of E, if a subfield of L contains F and γ_i's, then it contains E. Altogether we obtain that a subfield of L which contains F, β_i's, and $\gamma_{i,j}$'s is the entire L. This means

$$L = F[\beta_1, \ldots, \beta_m, \gamma_{1,1}, \ldots, \gamma_{n,m_n}]. \tag{22.4}$$

By (22.2) and (22.4), we deduce that L is a splitting field of f over F. This gives us a field L with the mentioned desired properties, and the claim follows.

[1] We will use this method to show the existence of a normal closure of a field extension.

(3) ⇒ (1) We use the same technique as in the proof of the previous step. Suppose $(\gamma_1, \ldots, \gamma_n)$ is an F-basis of E, and let

$$g(x) := m_{\gamma_1,F}(x) \cdots m_{\gamma_n,F}(x).$$

By hypothesis, $m_{\gamma_i,F}$ can be written as a product of degree one factors in $E[x]$. Hence there are α_i's in E such that

$$g(x) = (x - \alpha_1) \cdots (x - \alpha_d). \tag{22.5}$$

We also notice that γ_i's are zeros of g in E, and so

$$\gamma_i \in \{\alpha_1, \ldots, \alpha_d\} \tag{22.6}$$

for every i. Therefore

$$\begin{aligned} E = \operatorname{Span}_F(\gamma_1, \ldots, \gamma_n) \subseteq & F[\gamma_1, \ldots, \gamma_n] \\ \subseteq & F[\alpha_1, \ldots, \alpha_d] \subseteq E. \end{aligned}$$

Hence $E = F[\alpha_1, \ldots, \alpha_n]$, which together with (22.5) implies that E is a splitting field of g over F. This completes the proof. □

Chapter 23

Lecture 23

23.1 The group of automorphism of normal field extensions.

Using Theorem 22.2.1, we obtain the following result on the group of automorphisms.

Proposition 23.1.1. *Suppose E is a normal extension of F and $[E : F] < \infty$. Then*

1. *For every field extension L of E,*
$$r_{L,E} : \operatorname{Aut}_F(L) \to \operatorname{Aut}_F(E), \;\; r_{L,E}(\theta) := \theta|_E$$
is a well-defined group homomorphism. Moreover $\ker r_{L,E} = \operatorname{Aut}_E(L)$; in particular, $\operatorname{Aut}_E(L)$ is a normal subgroup of $\operatorname{Aut}_F(L)$.

2. *For every extension L of E which is a finite normal extension of F, $r_{L,E}$ is surjective and*
$$\operatorname{Aut}_F(L)/\operatorname{Aut}_E(L) \simeq \operatorname{Aut}_F(E).$$

Proof. (1) Since E is a finite normal extension of F, by Theorem 22.2.1 for every field extension L of E and every $\theta \in \operatorname{Aut}_F(L)$, $\theta(E) = E$. Hence $\theta|_E$ is an F-automorphism of E. Therefore $r_{L,E}$ is a well-defined map. It is easy to check that it is a group homomorphism.

Notice that $\theta \in \ker r_{L,E}$ if and only if $\theta|_E = \mathrm{id}_E$. Hence $\ker r_{L,E} = \operatorname{Aut}_E(L)$. From group theory, we know that kernel of a group homomorphism is a normal subgroup.

(2) Let's start by understanding what the surjectivity of $r_{L,E}$ means. It means that every $\overline{\theta} \in \operatorname{Aut}_F(E)$ can be extended to an F-automorphism of L. By the isomorphism extension theorem, $\overline{\theta}$ can be extended to an F-isomorphism from L to itself if L is a splitting field of a polynomial $f \in F[x]$. Let's explain why this is the case. If L is a splitting field of $f \in F[x]$ over F, then by $f = \theta(f)$ and $E = \theta(E)$, we observe that L is also a splitting field of $\theta(f)$ over $\theta(E)$. Therefore by the isomorphism extension theorem (see Theorem 17.1.1) we get the desired extension.

Since L is a finite normal extension of F, by Theorem 22.2.1 there is $f \in F[x]$ such that L is a splitting field of f over F. Hence as explained above by the isomorphism extension theorem, there is $\theta \in \operatorname{Aut}_F(L)$ such that $\theta|_E = \overline{\theta}$, and so $r_{L,E}$ is surjective.

By the first isomorphism theorem for groups, we have

$$\operatorname{Aut}_F(L)/\ker r_{L,E} \simeq \operatorname{Im} r_{L,E},$$

and so

$$\operatorname{Aut}_F(L)/\operatorname{Aut}_E(L) \simeq \operatorname{Aut}_F(E).$$

This completes the proof. □

The following commutative diagram captures the surjectivity of $r_{L,E}$ when L is a finite normal extension of F. In this diagram, every row is an isomorphism, and the dashed arrow means that for a given $\overline{\theta}$, we can find θ that makes the diagram commutative.

$$\begin{tikzcd}
L \arrow[r, dashed, "\theta"] \arrow[d, dash] & L \arrow[d, dash] \\
E \arrow[r, "\overline{\theta}"] \arrow[d, dash] & E \arrow[d, dash] \\
F \arrow[r, "\mathrm{id}"] & F
\end{tikzcd}$$

23.2 Normal extensions and tower of fields

When we learn about a property of field extensions, we have to ask ourselves how it behaves in a tower of fields. For instance, by the Tower Rule, we know that for a tower of fields $F \subseteq E \subseteq L$, L is a finite extension of F if and only if L is a finite extension of E and E is a finite extension of F. We will see that normal extensions do *not* have such a nice behavior. We, however, start with a positive result.

Lemma 23.2.1. *Suppose $F \subseteq E \subseteq L$ is a tower of field extensions. Then the following holds.*

1. *For every $\beta \in L$, $m_{\beta,E}|m_{\beta,F}$ in $E[x]$.*
2. *If L is a normal extension of F, then L is a normal extension of E.*

Proof. (1) Since β is a zero of $m_{\beta,F}(x) \in E[x]$, by Proposition 8.2.6 we have that $m_{\beta,E}$ divides $m_{\beta,F}$ in $E[x]$.

(2) Since L is a normal extension of F, for every β, $m_{\beta,F}(x)$ can be written as a product of degree one factors in $L[x]$. By part one, $m_{\beta,E}$ divides $m_{\beta,F}$ in $E[x]$, and so $m_{\beta,E}$ divides $m_{\beta,F}$ in $L[x]$. Since $L[x]$ is a UFD, degree one polynomials are irreducible in $L[x]$, $m_{\beta,F}$ can be written as a product of degree one factors, and $m_{\beta,E}|m_{\beta,F}$ in $L[x]$, we obtain that $m_{\beta,E}$ can be written as product of degree one factors in $L[x]$. This means L is a normal extension of E, which completes the proof. □

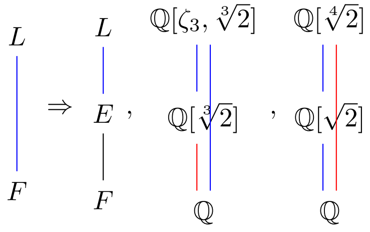
The following examples show us that the normal extension property cannot be deduced for other parts of a tower.

By Example 17.2.2 and Theorem 22.2.1, $\mathbb{Q}[\zeta_n, \sqrt[n]{2}]$ is a normal extension of $\mathbb{Q}$. We, however, claim that the intermediate field $\mathbb{Q}[\sqrt[n]{2}]$ is not a normal extension of $\mathbb{Q}$

if $n > 2$. By Eisenstein's criterion, $x^n - 2$ is irreducible in $\mathbb{Q}[x]$. As $\sqrt[n]{2}$ is a zero of $x^n - 2$, by Theorem 8.2.5 $m_{\sqrt[n]{2},\mathbb{Q}}(x) = x^n - 2$. This polynomial has at most two real zeros, and so not all of its zeros are in $\mathbb{Q}[\sqrt[n]{2}]$. Therefore $\mathbb{Q}[\sqrt[n]{2}]$ is not a normal extension of $\mathbb{Q}$. Notice that if $[E : F] = 2$, then for every $\alpha \in E \setminus F$ we have

$$1 < \deg m_{\alpha,F} = [F[\alpha] : F] \leq [E : F] = 2.$$

Hence for every $\alpha \in E$, we have $1 \leq \deg m_{\alpha,F} \leq 2$, and so all the zeros of $m_{\alpha,F}$ are in E. Therefore E is a normal extension of F. This implies that $\mathbb{Q}[\sqrt[4]{2}]$ is a normal extension of $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}]$ is a normal extension of $\mathbb{Q}$, but as we showed above $\mathbb{Q}[\sqrt[4]{2}]$ is not a normal extension of $\mathbb{Q}$.


L
F
$\Rightarrow$
L
E
F
,
$\mathbb{Q}[\zeta_3, \sqrt[3]{2}]$
$\mathbb{Q}[\sqrt[3]{2}]$
$\mathbb{Q}$
,
$\mathbb{Q}[\sqrt[4]{2}]$
$\mathbb{Q}[\sqrt{2}]$
$\mathbb{Q}$

23.3 Normal closure of a field extension

Suppose E is a finite field extension of F. We prove the existence of a smallest field extension of E which is a normal extension of F.

Proposition 23.3.1. *Suppose E is a finite field extension of F. Then there is a field extension L of E such that the following holds:*

1. *L is a normal extension of F.*
2. *If L' is a field extension of E and L' is a normal extension of F, then there is an E-embedding $\theta : L \to L'$.*

In particular, if L_1 and L_2 satisfy the above properties, then there is an E-isomorphism $\theta : L_1 \to L_2$.

A field L which satisfies the properties mentioned in Proposition 23.3.1 is called a *normal closure of the field extension E of F*.

Proof. We use an identical technique as in the proof of Theorem 22.2.1 (going from (2) to (3)). Suppose $(\gamma_1, \ldots, \gamma_d)$ is an F-basis of E. Let L be a splitting field of

$$f(x) := m_{\gamma_1,F}(x) \cdots m_{\gamma_d,F}(x)$$

over E. Then there are $\gamma_{i,j}$'s in L such that for every i

$$m_{\gamma_i,F}(x) = \prod_{j=1}^{n_i} (x - \gamma_{i,j}) \quad \text{and} \quad L = E[\gamma_{1,1}, \ldots, \gamma_{d,n_d}]. \tag{23.1}$$

Since $\gamma_i \in E$ is a zero of $m_{\gamma_i,F}(x)$ and $E \subseteq L$, we can and will assume that $\gamma_{i,1} = \gamma_i$ for every i. Therefore

$$E = \operatorname{Span}_F(\gamma_1, \ldots, \gamma_d) \subseteq F[\gamma_1, \ldots, \gamma_n] \subseteq F[\gamma_{1,1}, \ldots, \gamma_{d,n_d}]. \tag{23.2}$$

By (23.2), we obtain that

$$L = E[\gamma_{1,1}, \ldots, \gamma_{d,n_d}] \subseteq F[\gamma_{1,1}, \ldots, \gamma_{d,n_d}] \subseteq L.$$

Hence $L = F[\gamma_{1,1}, \ldots, \gamma_{d,n_d}]$, and so by (17.2) we deduce that L is a splitting field of f over F. Hence by Theorem 22.2.1, L is a normal field extension of F.

Suppose L' is a field extension of E and L' is a normal extension of F. Then for every i, $\gamma_i \in L'$. Since L' is a normal extension of F, there are $\gamma'_{i,j}$'s in L' such that

$$m_{\gamma_i,F}(x) = \prod_{j=1}^{n_i} (x - \gamma'_{i,j}). \tag{23.3}$$

Then $L'' := E[\gamma'_{1,1}, \ldots, \gamma'_{d,n_d}] \subseteq L'$ is a splitting field of $f(x)$ over E. Therefore by the uniqueness of splitting fields (see Theorem 17.1.2) there is an E-isomorphism $\theta : L \to L''$. As L'' is a subfield of L', θ can be viewed as an element in $\mathrm{Emb}_E(L, L')$.

If L_1 and L_2 satisfy these conditions, then there are $\theta_1 \in \mathrm{Emb}_E(L_1, L_2)$ and $\theta_2 \in \mathrm{Emb}_E(L_2, L_1)$. As L_i's are finite field extensions of E, we deduce that θ_i's are isomorphisms. This completes the proof. □

23.4 Normal extension and extending embeddings

The following result on extending embeddings is a variant of the isomorphism extension theorem.

Proposition 23.4.1. *Suppose $F \subseteq E \subseteq L$ is a tower of fields, and L is a finite normal extension of F. Suppose $\theta \in \mathrm{Emb}_F(E, L)$. Then there is $\widehat{\theta} \in \mathrm{Aut}_F(L)$ such that $\widehat{\theta}|_E = \theta$.*

Proof. Since L is a finite normal extension of F, there is $f \in F[x]$ such that L is a splitting field of f over F. So there are α_i's in L such that

$$f(x) = \mathrm{ld}(f) \prod_{i=1}^{n} (x - \alpha_i) \quad \text{and} \quad L = F[\alpha_1, \ldots, \alpha_n].$$

Notice that since E and $\theta(E)$ contain F as a subfield, L can be viewed as a splitting field of f over E and also as a splitting field of $\theta(f) = f$ over $\theta(E)$. Thus by the isomorphism extension theorem, there is $\widehat{\theta} : L \to L$ such that $\widehat{\theta}|_E = \theta$, and this completes the proof. □

23.5 Group of automorphisms of a field extension

For every field extension E of F, by Lemma 22.1.4 and Lemma 16.2.2, the following is a bijection

$$\mathrm{Emb}_F(F[\alpha], E) \to \{\alpha' \in E \mid m_{\alpha,F}(\alpha') = 0\}, \ \theta \mapsto \theta(\alpha). \tag{23.4}$$

Then by (23.4) we have

$$|\operatorname{Emb}_F(F[\alpha], E)| = \# \text{ of distinct zeros of } m_{\alpha,F} \text{ in } E \leq \deg m_{\alpha,F} = [F[\alpha] : F].$$

Suppose E is a finite normal extension of F and $E = F[\alpha]$. Then

$$|\operatorname{Aut}_F(E)| \leq [E : F]$$

and equality holds if $m_{\alpha,F}$ has distinct zeros in E. This takes us to the following questions.

1. What if E is not of the form $F[\alpha]$ for some α?

2. When can we be sure that $E = F[\alpha]$ for some α?

The following theorem addresses the first question (and more!).

Theorem 23.5.1. *Suppose $\theta : F \to F'$ is a field isomorphism, and $f(x) \in F[x]$. Suppose E is a splitting field of f over F, and E' is a splitting field of $\theta(f)$ over F'. Then*

$$|\operatorname{Iso}_\theta(E, E')| \leq [E : F].$$

Moreover the equality holds if irreducible factors of f in $F[x]$ do not have multiple zeros in E.

This is an extremely important result. Proof of this theorem has some similarities with the proof of the isomorphism extension theorem (see Theorem 17.1.1).

Proof of Theorem 23.5.1. We proceed by strong induction on $[E : F]$. If $[E : F] = 1$, then $E = F$ and $E' = F'$, and so $\operatorname{Iso}_\theta(E, E') = \operatorname{Iso}_\theta(F, F') = \{\theta\}$ has exactly 1 element, and equality holds.

Suppose $E \neq F$. Hence f has a zero $\alpha \in E$ which is not in F. Notice that for every $\widehat{\theta} \in \operatorname{Iso}_\theta(E, E')$, we have $\widehat{\theta}|_{F[\alpha]}$ is in $\operatorname{Emb}_\theta(F[\alpha], E')$. Notice that by Lemma 22.1.4

$$\operatorname{Emb}_\theta(F[\alpha], E') \to \{\alpha' \in E' \mid \theta(m_{\alpha,F})(\alpha') = 0\}, \quad \widehat{\theta} \mapsto \widehat{\theta}(\alpha) \tag{23.5}$$

is a well-defined function. Since a ring homomorphism $\theta_1 : F[\alpha] \to E'$ is uniquely determined by $\theta_1|_F$ and $\theta_1(\alpha)$, the function given in (23.5) is injective. If α' is a zero of $\theta(m_{\alpha,F})$ in E', then by Lemma 16.2.2 there is $\theta_1 \in \operatorname{Iso}_\theta(F[\alpha], F'[\alpha'])$, and so the function given in (23.5) is a bijection. Hence

$$\begin{aligned} |\operatorname{Emb}_\theta(F[\alpha], E')| &= \# \text{ of distinct zeros of } m_{\alpha,F} \text{ in } E \\ &\leq \deg m_{\alpha,F} = [F[\alpha] : F]. \end{aligned} \tag{23.6}$$

For every $\theta_1 \in \operatorname{Emb}_\theta(F[\alpha], E')$, notice that E is a splitting field of f over $F[\alpha]$, and E' is a splitting field of $\theta(f) = \theta_1(f)$ over $F'[\theta_1(\alpha)]$. Since $[E : F[\alpha]] < [E : F]$, by the strong induction hypothesis, we have

$$|\operatorname{Iso}_{\theta_1}(E, E')| \leq [E : F[\alpha]]. \tag{23.7}$$

Hence

$$\begin{aligned}
|\operatorname{Iso}_\theta(E,E')| &= \sum_{\theta_1\in \operatorname{Emb}_\theta(F[\alpha],E')} |\operatorname{Iso}_{\theta_1}(E,E')| \\
&\le [E:F[\alpha]]|\operatorname{Emb}_\theta(F[\alpha],E')| && \text{(by (23.7))}\\
&\le [E:F[\alpha]][F[\alpha]:F]=[E:F]. && \text{(by (23.6))}
\end{aligned}$$

To prove the *moreover* part, we go back through the above argument and show the equalities hold. If α is a zero of f, then $m_{\alpha,F}$ is an irreducible factor of f in $F[x]$. Then, by hypothesis, $m_{\alpha,F}$ has distinct zeros in E. Hence by Proposition 18.3.4, $\gcd(m_{\alpha,F},m'_{\alpha,F})=1$. Thus $\gcd(\theta(m_{\alpha,F}),\theta(m_{\alpha,F})')=1$, and so by Proposition 18.3.4, $\theta(m_{\alpha,F})$ has distinct zeros in E'. Therefore by (23.6), we have

$$|\operatorname{Emb}_\theta(F[\alpha],E')|=[F[\alpha]:F]. \tag{23.8}$$

As in the above argument, we want to use the strong induction hypothesis to obtain that $|\operatorname{Iso}_{\theta_1}(E,E')|=[E:F[\alpha]]$ for every $\theta_1\in\operatorname{Emb}_\theta(F[\alpha],E')$. We have already pointed out that E is a splitting field of f over $F[\alpha]$ and E' is a splitting field of $\theta_1(f)$ over $F'[\theta_1(\alpha)]$. To use the strong induction hypothesis for θ_1, E, and E', it is enough to show that all the irreducible factors of f in $(F[\alpha])[x]$ do not have multiple zeros in E. Let $p(x)$ be a monic irreducible factor of f. Then there is $\beta\in E$ which is a zero of p. Hence by Theorem 8.2.5, $p(x)=m_{\beta,F[\alpha]}$. Hence by Lemma 23.2.1, $p(x)|m_{\beta,F}$ in $(F[\alpha])[x]$. Since $m_{\beta,F}$ is an irreducible factor of f in $F[x]$, by hypothesis it does not have multiple zeros in E. Hence its divisor p does not have multiple zeros in E, either. Therefore by the strong induction hypothesis, we have

$$|\operatorname{Iso}_{\theta_1}(E,E')|=[E:F[\alpha]]. \tag{23.9}$$

Hence

$$\begin{aligned}
|\operatorname{Iso}_\theta(E,E')| &= \sum_{\theta_1\in \operatorname{Emb}_\theta(F[\alpha],E')} |\operatorname{Iso}_{\theta_1}(E,E')| \\
&= [E:F[\alpha]]|\operatorname{Emb}_\theta(F[\alpha],E')| && \text{(by (23.9))}\\
&= [E:F[\alpha]][F[\alpha]:F]=[E:F]. && \text{(by (23.8))}
\end{aligned}$$

This completes the proof. □

Chapter 24

Lecture 24

24.1 Separable polynomials

To have a simpler formulation of Theorem 23.5.1, we define *separable polynomials* as follows.

Definition 24.1.1. *Suppose F is a field and $f \in F[x]$. We say f is* separable *(in $F[x]$) if its irreducible factors in $F[x]$ do not have multiple zeros in a splitting field of f over F.*

Let us make two remarks:

1. The way we defined *separability* of $f \in F[x]$ depends on both the polynomial f and the field F. For instance every polynomial $f \in F[x]$ is separable as an element of $E[x]$ where E is a splitting field of f over F (Notice that all the irreducible factors of f in $E[x]$ are of degree 1 and so they do not have multiple zeros). On the other hand, $x^p - t$ is irreducible in $\mathbb{F}_p(t)$ and it has multiple zeros in its splitting field. To show the latter you can use the fact that either the derivative of this polynomial is zero or $x^p - t = (x - \sqrt[p]{t})^p$.

2. If $p \in F[x]$ is irreducible, then by Proposition 18.3.4, p is separable in $F[x]$ if and only if $\gcd(p, p') = 1$ in $F[x]$. Notice that if E is a field extension of F and $\gcd(p, p') = 1$ in $F[x]$, then $\gcd(p, p') = 1$ in $E[x]$ as well. Hence for an irreducible polynomial $p \in F[x]$, separability only depends on the polynomial.

By the special case of Theorem 23.5.1 for $F = F'$ and $\theta := \mathrm{id}_F$, we obtain the following:

Theorem 24.1.2. *If E is a finite normal extension of F, then $|\operatorname{Aut}_F(E)| \le [E : F]$.*

Theorem 24.1.3. *Suppose E is a splitting field of a separable polynomial $f \in F[x]$ over F. Then $|\operatorname{Aut}_F(E)| = [E : F]$.*

24.2 Separable and Galois extensions

We start by defining *separable field extensions*.

Definition 24.2.1. *Suppose E is an algebraic field extension of F. We say E is a separable extension of F if, for every $\alpha \in E$, $m_{\alpha,F}$ is a separable element of $F[x]$.*

Theorem 24.2.2. *Suppose E is a finite field extension of F. Then the following statements are equivalent.*

1. *E is a normal separable extension of F.*
2. *E is a splitting field of a separable $f \in F[x]$ over F.*
3. *$|\operatorname{Aut}_F(E)| = [E : F]$.*

Proof. (1) $\Rightarrow$ (2). Suppose $(\gamma_1, \ldots, \gamma_m)$ is an F-basis of E. Since E is a normal extension of F, there are $\gamma_{i,j} \in E$ such that $m_{\gamma_i,F}(x) = \prod_{j=1}^{n_i}(x - \gamma_{i,j})$. Let

$$f(x) := \prod_{i=1}^{m} m_{\gamma_i,F}(x) = \prod_{i,j}(x - \gamma_{i,j}).$$

We notice that $\gamma_i \in E$ is among $\{\gamma_{i,1}, \ldots, \gamma_{i,n_i}\}$. So

$$E \supseteq F[\gamma_{1,1}, \ldots, \gamma_{m,n_m}] \supseteq \operatorname{Span}_F(\gamma_1, \ldots, \gamma_m) = E.$$

Hence E is a splitting field of f over F. Since E is a separable extension of f, $m_{\gamma_i,F}$'s do not have multiple zeros in E. Hence f is separable in $F[x]$ (notice that that $m_{\gamma_i,F}(x)$'s are irreducible in $F[x]$).

(2) $\Rightarrow$ (3). It follows from Theorem 24.1.3.

(3) $\Rightarrow$ (1). For every $\alpha \in E$, we have

$$\begin{aligned}
|\operatorname{Aut}_F(E)| &= \sum_{\theta \in \operatorname{Emb}_F(F[\alpha],E)} |\operatorname{Iso}_\theta(E,E)| \\
\text{(By Theorem 23.5.1)} \quad &\leq [E : F[\alpha]] |\operatorname{Emb}_F(F[\alpha],E)| \\
\text{(By (23.4))} \quad &= [E : F[\alpha]] \cdot (\#\text{of distinct zeros of } m_{\alpha,F} \text{ in } E) \qquad (24.1)
\end{aligned}$$

On the other hand, by hypothesis and the Tower Rule, we have

$$|\operatorname{Aut}_F(E)| = [E : F] = [E : F[\alpha]][F[\alpha] : F]. \qquad (24.2)$$

Hence by (24.2), (24.1), and Proposition 20.1.2, we obtain that

$$\#\text{of distinct zeros of } m_{\alpha,F} \text{ in } E \geq [F[\alpha] : F] = \deg m_{\alpha,F}.$$

Therefore $m_{\alpha,F}$ has $\deg m_{\alpha,F}$ distinct zeros in E. Hence the following holds.

1. There are $\alpha_1, \ldots, \alpha_m \in E$ such that $m_{\alpha,F}(x) = \prod_{i=1}^{m}(x - \alpha_i)$.

2. $m_{\alpha,F}$ does not have multiple zeros in E. The first assertion implies that E is a normal extension of F, and form the second statement we deduce that E is a separable extension of F. This completes the proof.

□

Definition 24.2.3. *An algebraic field extension E of F is called a* Galois extension *if it is normal and separable.*

Galois extensions will be explored more later.