MATH 4140/MATH 5140: Abstract Algebra II

Farid Aliniaeifard

April 30, 2018

Contents

1 Rings and Isomorphism (See Chapter 3 of the textbook)

1.1 Definitions and examples

Definition. *A* **ring** *is a nonempty set R equipped with two operations (usually written as addition (+) and multiplication(.) and we denote the ring with its operations by (R,+,.)) that satisfy the following axioms. For all $a, b, c \in R$:*

(1) If $a \in R$ and $b \in R$, then $a + b \in R$. [Closure for addition]

(2) $a + (b + c) = (a + b) + c$. [Associative addition]

(3) $a + b = b + a$. [Commutative addition]

(4) There is an element 0_R in R such that $a + 0_R = a = 0_R + a$ for every $a \in R$. [Zero element]

(5) For every $a \in R$, there exists an element $b \in R$ such that $a+b = 0 = b+a$. [additive Inverse element]

(6) If $a \in R$ and $b \in R$, then $a.b \in R$. [Closed for multiplication]

(7) $a.(b.c) = (a.b).c$

(8) $a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$ [Distributive laws]

Remark. *Note that axioms $1, 2, 3, 4,$ and 5 shows that $(R, +)$ is an abelian group.*

Example 1.1. *$\mathbb{Z}$, $\mathbb{Z}_n$, and $M_2(\mathbb{R})$ are rings.*

Definition. *A* **commutative ring** *is a ring R that satisfies the axiom:*

(9) $a.b = b.a$ for all $a, b \in R$. [Commutative multiplication]

Definition. *A* **ring with identity** *is a ring R that contains an element 1_R satisfying this axiom:*

(10) $a.1_R = a = 1_R.a$ *for all* $a \in R$ *[Multiplicative identity]*

Definition. *An* **integral domain** *is a commutative ring R with identity $1_R \neq 0$ that satisfies this axiom:*

(11) whenever $a, b \in R$ *and* $a.b = 0$*, then* $a = 0_R$ *or* $b = 0_R$*.*

The end of the lecture 1

Lecture 2, January 19, 2018

A ring is a nonempty set R together with two operations $(+)$ and $(.)$ such that

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

(ii) for all $a, b \in R$, $a.b \in R$.

(iii) for all $a, b, c \in R$, $a.(b.c) = (a.b).c$.

(iv) for all $a, b, c \in R$, we have $a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$.

Then a ring is commutative if $a.b = b.a$ for all $a, b \in R$. It has an identity if there is an element $1 \in R$ such that $a.1 = 1.a = a$.

An integral domain is a commutative ring with identity 1 that satisfy the axiom: if $ab = 0$, then $a = 0$ or $b = 0$.

Example 1.2. $\mathbb{Z}, \mathbb{R}$, *and* $\mathbb{Q}$ *are integral domains.*

$\mathbb{Z}_6$ *is a ring but not an integral domain. The elements of* $\mathbb{Z}_6$ *are* $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. *In* $\mathbb{Z}_6$, *we have* $\overline{2} + \overline{3} = \overline{5}$, $\overline{5} + \overline{4} = \overline{3}$ *and* $\overline{5} + \overline{3} = \overline{2}$. *Also, if we compute*

$$\overline{2}.\overline{3} = \overline{0}$$

we see that $\mathbb{Z}_6$ *is not an integral domain.*

Example 1.3. *Let* $\mathbb{R}$ *be the ring of real numbers. Then* $\mathbb{R}[x]$ *is a ring with the following addition and multiplication: if*

$$f(x) = 1 + 3x + x^2 \in \mathbb{R}[x]$$

and

$$g(x) = -3x + x^3 \in \mathbb{R}[x],$$

then

$$f(x) + g(x) = 1 + x^2 + x^3$$

and

$$f(x)g(x) = -3x + x^3 - 9x^2 + 3x^4 - 3x^3 + x^5 = -3x - 9x^2 - 2x^3 + 3x^4 + x^5.$$

Also, the polynomial $e(x) = 1$ *is the identity element and* $0(x) = 0$ *is the zero element.*

Theorem 1.4. *Let* R *and* S *be rings. Define the following addition and multiplication on the Cartisian Product* $R \times S$ *by*

$$(r, s) + (r', s') = (r + r', s + s') \text{ and } (r, s).(r', s') = (r.r', s.s').$$

Then $R \times S$ *is a ring. If* R *and* S *are both commutative, so does* $R \times S$. *If both* $R \times S$ *have identity then so does* $R \times S$.

In the following proposition we will present some properties of the elements of a ring.

Proposition 1.5. *Let* R *be a ring and* $a, b \in R$. *Then*

(i) $0.a = a.0 = 0$.

(ii) $(-a).b = a.(-b) = -(a.b)$.

(iii) *if* R *has identity* 1*, then the identity is unique and* $(-a) = (-1).a$.

Proof. 1. (i)

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

2. (ii)

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

The rest left to the reader. □

Definition. *A subset* S *of a ring* R *is a* **subring** *of* R *if it is a ring with the same addition and multiplication as* R*. To show that a subset* S *of* R *is a subring of* R*, you only need to check that* S *is nonempty and*

(i) S *is closed under multiplication.*

(ii) S *is closed under subtraction, i.e., if* $a, b \in R$*, then* $a - b \in R$.

Example 1.6. *Define* $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ *is a subring of* $\mathbb{R}$.

Proof. Let $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and $c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + cb)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

and

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Therefore $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$. □

Definition. *A* **Field** *is a commutative ring* R *with identity* $1_R \neq 0$ *that satisfies this axiom:*

(12) *For each* $a \neq 0_R$ *in* R*, there is an element* $b \in R$ *such that* $ab = 1 = ba$*. The element* b *is called the* **inverse** *of* a *and is denoted by* a^{-1}.

Example 1.7. *(i)* $\mathbb{Q}$, $\mathbb{R}$ *and* $\mathbb{C}$ *are fields.*

(ii) $\mathbb{Z}_p$ *when* p *is a prime number is a field.*

Week 2, Lecture 1

1.2 Units and Zero-divisors

Definition. *An element a in a ring R with identity is called a* **unit** *if there exists $u \in R$ such that $au = 1_R = ua$.*

Example 1.8. *(i) Units of $\mathbb{Z}$ are 1 and -1.*

(ii) Units of $\mathbb{Z}_6$ are $\overline{1}$ and $\overline{5}$. In general the set of units of $\mathbb{Z}_n$ is $\{\overline{k} : \quad k$ and n are coprime $\}$.

(iii) Units of the rings of 2×2 matrices $M_2(\mathbb{R})$ are the invertible matrices.

Definition. *An element a in R is a* **zero-divisor** *provided that*

(i) $a \neq 0_R$.

(ii) There exists a nonzero element $c \in R$ such that $ac = 0_R$ or $ca = 0_R$.

Remark. *An integral domain contains no* **zero-divisors**.

Example 1.9. *(i) $\overline{2}$ and $\overline{3}$ are zero-divisors in $\mathbb{Z}_6$ since $\overline{2}.\overline{3} = \overline{0}$.*

(ii) zero-divisors of the rings of 2×2 matrices $M_2(\mathbb{R})$ are the non-invertible matrices. Because if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a non-invertible matrix we have $det(A) = ad - bc = 0$, and we multiply $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

A ring D with identity 1_D in which every non-zero element is a unit is called a **Division ring**. Note that any field is a commutative division ring.

1.3 Useful facts about fields and integral domains

Theorem 1.10. *Every finite field $\mathbb{F}$ is an integral domain.*

Proof. Every field is a commutative ring with identity, so it is enough to show that if $ab = 0$, then $a = 0$ or $b = 0$. Assume that $ab = 0$ but $a \neq 0$ and $b \neq 0$. Then

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

which is a contradiction. □

Theorem 1.11. *Every finite integral domain R is a field.*

Proof. As every integral domain is a commutative ring with identity, it is enough to show that every non-zero element in R has an inverse in R. Let $a_1, \dots, a_n$ be all of nonzero distinct elements of R. Let a be an arbitrary nonzero element in R. Then for any a_i we have $aa_i \neq 0$ otherwise since R is in integral domain we have $a = 0$ or $a_i = 0$ which is not possible. Therefore, $aa_1, \dots, aa_n$ are nonzero elements in R. Moreover, they are distinct because if for some distinct i and j, $aa_i = aa_j$, then

$$aa_i - aa_j = 0 \Rightarrow a(a_i - a_j) = 0.$$

Since R is an integral domain and $a \neq 0$, we must have $a_i - a_j = 0$, and so $a_i = a_j$, which is not possible. Therefore, for all distinct i and j we have $aa_i \neq aa_j$. So $aa_1, \ldots, aa_n$ are all of nonzero distinct elements of R. We can conclude that $\{a_1, \ldots, a_n\} = \{aa_1, \ldots, aa_n\}$. Since $1 \in \{a_1, \ldots, a_n\} = \{aa_1, \ldots, aa_n\}$. Thus for some i we have $aa_i = 1$, and so $a^{-1} = a_i$, i.e., a is invertible. It follows that every element of R has an inverse and so R is a field. $\square$

1.4 Homomorphism and isomorphism

Definition. *Let R and S be rings. A function $f : R \to S$ is said to be a* **homomorphism** *if $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.*

Definition. *A ring R is* **isomorphic** *to a ring S (in symbols, $R \cong S$) if there is a homomorphism $f : R \to S$ such that*

(i) f is injective;

(ii) f is surjective.

Week 2, Lecture 2

The **kernel** of a homomorphism of rings $f : R \to S$ is the set

$$\ker f = \{r \in R : f(r) = 0\}.$$

The **image** of f denoted by $\mathrm{Img} f$, is $\{s \in S : s = f(r) \text{ for some } r \in R\}$.

Theorem 1.12. *Let $f : R \to S$ be a homomorphism of rings. Then*

1. $f(0_R) = f(0_S)$.
2. $f(-a) = -f(a)$.
3. $f(a - b) = f(a) - f(b)$.

   If R is a ring with identity and f is surjective, then

4. *S is a ring with identity $f(1_R)$.*
5. *Whenever u is a unit in R, then $f(u)$ is a unit in S and $f(u)^{-1} = f(u^{-1})$.*

Proof. Refer to the book for (1), (2), and (3).
(4) We want to show that for any $s \in S$, we have $sf(1_R) = f(1_R)s = s$. Since f is surjective, there is an element $r \in R$ such that $f(r) = s$. Therefore,

$$sf(1_R) = f(r)f(1_R) = f(r1_R) = f(r) = s.$$

Similarly we have $f(1_R)s = s$.
(5) Since u is a unit in R, there is an element $v \in R$ such that $uv = vu = 1_R$. Therefore, $f(uv) = f(1_R)$. So, $f(u)f(v) = f(v)f(u) = f(1_R)$. Note that $f(1_R)$ is the identity of S, therefore, $f(u)$ is a unit in S. Now we want to show that $f(u)^{-1} = f(u^{-1})$. Note that $uu^{-1} = 1_R$, therefore, $f(u)f(u^{-1}) = f(1_R)$, which means that $f(u)^{-1} = f(u^{-1})$. $\square$

Example 1.13. *Let*

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

Show that R is a ring and is isomorphic to $\mathbb{C}$ the ring of complex numbers.

Proof. Define a function as follows

$$\begin{array}{cccc} f: & R & \to & \mathbb{C} \\ & \begin{bmatrix} a & b \\ -b & a \end{bmatrix} & \mapsto & a + ib \end{array}$$

Clearly this function is well-defined, surjective and one to one, so we only show that it is a ring homomorphism.

$$f(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}) = f(\begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix}) = (a+c)+i(c+d) = (a+ib)+(c+id)$$

$$= f(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}) + f(\begin{bmatrix} c & d \\ -d & c \end{bmatrix})$$

$$f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) = f\left(\begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix}\right) = (ac-bd)+(ad+bc)i = (a+ib)(c+id)$$

$$= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) f\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)$$

□

Corollary 1.14. *If $f : R \to S$ is a homomorphism, then the image of f is a subring of S.*

Proof. Note that $f(0_R) = 0_S$, so Img$f$ is nonempty. Let $s, s^{'} \in$ Img$f$. Then there are elements $r, r^{'} \in R$ such that $f(s) = r$ and $f(r^{'}) = s^{'}$. Now,

$$ss^{'} = f(r)f(r^{'}) = f(rr^{'}) \in \text{Img}f$$

and

$$s - s^{'} = f(r) - f(r^{'}) = f(r - r^{'}) \in \text{Img}f.$$

We conclude that Img$f$ is a subring of S. □

2 Polynomials Arithmetic and the Division algorithm

Let R be any ring. A **polynomial** with coefficients in R is an expression of the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

where n is a nonnegative integer and $a_i \in R$. Let $R[x]$ be the set of all polynomials in $R[x]$. Actually, $R[x]$ is a subring of another ring T (we do not discuss the structure of T in this course). The element x sometimes called an **indeterminate**.

Definition. *Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ such that $a_n \neq 0$. Then a_n is called the* **leading coefficient** *of $f(x)$. The* **degree** *of $f(x)$ is the integer n, and we write* deg$f(x) = n$. *We can consider elements of R as polynomials in $R[x]$, and they are called* **constant polynomials**. *The polynomials of degree 0 in $R[x]$ are precisely the constant polynomials. Note that 0_R does not have a degree.*

Theorem 2.1. *If R is an integral domain and $0 \neq f, g \in R[x]$, then*

$$\text{deg}f(x)g(x) = \text{deg}f(x) + \text{deg}g(x).$$

Proof. Suppose that $f(x) = a_0 + a_1x + \ldots + a_nx^n$ ($a_n \neq 0$) and $g(x) = b_0 + b_1x + \ldots + b_mx^m$ ($a_m \neq 0$). So deg$f(x) = n$ and deg$g(x) = m$. Then

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \ldots + a_nb_mx^{n+m}.$$

Since R is an integral domain and $a_n, b_m \neq 0$, we have that $a_nb_m \neq 0$, and so deg$f(x)g(x) = n + m =$ deg$f(x) +$ deg$g(x)$. □

Corollary 2.2. *If R is an integral domain, so is $R[x]$.*

Proof. We have that $R[x]$ is a commutative ring with identity. We will show that it does not have any nonzero zero-divisors. Let $0 \neq f(x), g(x) \in R[x]$. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ $(a_n \neq 0)$ and $g(x) = b_0 + b_1 x + \ldots + b_m x^m$ $(a_m \neq 0)$. Then

$$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \ldots + a_n b_m x^{n+m}.$$

If $f(x)g(x) = 0$, then $a_n b_m = 0$, which is impossible since R is an integral domain. Therefore, $R[x]$ is an integral domain. $\square$

Corollary 2.3. *Let R be a ring. If $f(x), g(x)$ and $f(x)g(x)$ are non-zero in $R[x]$, then* $\deg f(x)g(x) \leq \deg f(x) \deg g(x)$.

Week 2, Lecture 3

Corollary 2.4. *Let R be an integral domain and $f(x) \in R[x]$. Then $f(x)$ is a unit in $R[x]$ if and only if $f(x)$ is a constant polynomial that is a unit in R. In particular, $\mathbb{F}$ is a field, then units in $\mathbb{F}[x]$ are the nonzero constant in $\mathbb{F}$.*

Proof. Assume that $f(x)$ is a unit in $R[x]$, then there is a polynomial $g(x)$ such that $f(x)g(x) = 1$. Since R is an integral domain, we have $\deg f(x) + \deg g(x) = deg f(x)g(x) = deg\ 1 = 0$. Therefore, we must have both $f(x)$ and $g(x)$ are of degree 0, so they are constant, and actually they are units in R. $\square$

The theorem above is not true if R is not an integral domain, for example, $5x + 1 \in \mathbb{Z}_{25}[x]$ is not a constant, however, it is a unit since $(5x + 1)(20x + 1) = 1$.

Theorem 2.5. *Let $\mathbb{F}$ be a field and $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that*

$$f(x) = g(x)q(x) + r(x) \quad \textit{and either } r(x) = 0 \textit{ or } \deg r(x) < \deg g(x).$$

3 Ideals and Quotient Rings

An **ideal** of a ring R is a non-empty subset of R such that for all $a, b \in I$ and $r \in R$,

1. $a - b \in I$
2. $ra \in I$ and $ar \in I$

Example 3.1. *Let $T = \{f : R \to R : f \text{ is a function}\}$. Define the following addition and multiplication for T. For all $f, g \in T$ and $a \in R$,*

$$(f + g)(a) = f(a) + g(a) \qquad fg(a) = f(a)g(a).$$

Then T is a ring with the above addition and multiplication. Show that the following set is an ideal of T,

$$I = \{f : R \to R : f \textit{ is a funtion and } \ f(2) = 0\}.$$

Proof. The set I is nonempty since $0 : R \to R$ defined by $0(r) = 0$ for every $r \in R$, is in I. Moreover, for all $f, g \in I$ and $h \in I$, we have that

$$(f - g)(2) = f(2) - g(2) = 0 - 0 = 0$$

and

$$hf(2) = h(2)f(2) = h(2)0 = 0 \text{ and } fh(2) = f(2)h(2) = 0h(2) = 0.$$

Therefore, $f - g, fh, hf \in I$ and so I is an ideal. $\square$

Definition. *A nonempty subset of a ring R is a* **left (right) ideal** *if for all $a, b \in I$, and $r \in R$,*

$$a - b \in I \qquad \textit{and} \qquad ra \in I (ar \in I).$$

Remark. *Any ideal of R is a subring of R. Also, a left (right) ideal is a right (left) ideal in a commutative ring.*

3.1 Finitely Generated Ideals

Theorem 3.2. *Let R be a commutative ring with identity and let $c \in R$. Define*

$$I = \{rc : r \in R\}.$$

Then I is an ideal of R.

Proof. Note that $0 = 0c \in I$, so I is nonempty. Moreover, for all $r_1c, r_2c \in I$ and $r \in R$. Then

$$r_1c - r_2c = (r_1 - r_2)c \in I \text{ and } r(r_1c) = (rr_1)c \in I.$$

As R is commutative $(r_1c)r \in I$. Therefore, I is an ideal of the commutative ring R. $\square$

Definition. *The ideal I defined in the above theorem is called the* **principal ideal generated by** *c and is denoted by $\langle c \rangle$.*

Example 3.3. *Let*

$$I = \{\textit{All polynomials in } \mathbb{Z}[x] \textit{ with even constant term } \}.$$

Then I is an ideal of $\mathbb{Z}[x]$ but I is not principal.

Proof. First note that I is an ideal (show it). We now show that I is not principal, i.e., there is not any polynomial $p(x) \in \mathbb{Z}[x]$ such that

$$I = \langle p(x) \rangle = \{f(x)p(x) : f(x) \in \mathbb{Z}[x]\}.$$

On the contrary assume that $I = \langle p(x) \rangle$. Then since $2 \in I$, there is an polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(x)p(x) = 2$. Since $\mathbb{Z}$ is an integral domain, we have

$$\deg f(x) + \deg p(x) = \deg f(x)g(x) = \deg 2 = 0.$$

We can say that $\deg p(x) = 0$ and let $p(x) = c$. Since $c|2$, we have $c = 2$ or -2. Now, $x \in I$. Therefore, $f(x)c = x$ for some $f(x) \in \mathbb{Z}[x]$. By comparing the degrees, $\deg f(x) = 1$. So $f(x) = a + bx$ for some $a, b \in \mathbb{Z}$. Therefore, $(a + bx)c = x$, and so $ac + bcx = x$, which means that $bc = 1$. Thus c is invertible, which is a contradiction. $\square$

Week 3, Lecture 1

Theorem 3.4. *Let R be a commutative ring with identity, and $c_1, \ldots, c_n \in R$. Then the set*

$$I = \{r_1c_1 + r_2c_2 + \ldots + r_nc_n : r_1, r_2, \ldots, r_n \in R\}$$

is an ideal.

Definition. *The ideal in the above theorem is called the* **ideal generated** *by $c_1, \ldots, c_n$ and denoted by*

$$\langle c_1, \cdots, c_n\rangle.$$

Definition. *If an ideal can be generated by a finite number of elements in R, then I is a* **finitely generated** *ideal.*

3.2 Congruence

Definition. *Let I be an ideal in R and $a, b \in R$. Then a is* **congruent to b modulo I** *[written $a \equiv b (mod\ I)$] if $a - b \in I$.*

Example 3.5. *Let $f(x) = x^2 + 6$ and $g(x) = 5x$ in $I = \{f : R \to R : f$ is a funtion and $f(2) = 0\}$. Then $f(x) \equiv g(x)(mod\ I)$ because $f(x) - g(x) = (x^2 + 6) - 5x$, $(f - g)(2) = 0$, and so $f(x) - g(x) \in I$.*

3.3 Quotient Ring

- Fix an ideal I of R. The relation $\equiv (mod\ I)$ is reflexive, symmetric, and transitive. Therefore, it is an equivalence relation.
- The equivalence class containing $a \in R$, denoted by $a + I$, is the set

$$a + I = \{b \in R : b \equiv a(mod\ I)\}.$$

- The set $a + I$ is called a **(left) coset** of I in R.

Theorem 3.6. *Let R be a ring and I be an ideal of R. Then*

1. *$a + I = \{a + i : i \in I\}$.*
2. *Two cosets are either identical or disjoint, i.e., for two cosets $a + I$ and $b + I$ we have either $a + I = b + I$ or $a + I \cap b + I = \emptyset$.*

Proof. 1. We have

$$a + I = \{b \in R : b \equiv a(mod\ I)\} = \{b \in R : b - a \in I\}$$

$$= \{b \in R : b - a = i \text{ for some } i \in I\} = \{b \in R : b = a + i \text{ for some } i \in I\}$$

$$= \{a + i : i \in I\}.$$

2. Let $a+I$ and $b+I$ be two cosets of I in R. Assume that $a+I\cap b+I\neq\emptyset$ and $c\in a+I\cap b+I$. Then $c=a+i$ for some $i\in I$ and $c=b+j$ for some $j\in I$. So

$$a+i=b+j\Rightarrow a-b=j-i\in I.$$

Let $B\in b+I$. Then $B=b+k$ for some $k\in I$. Also,

$$a-(b+k)=j-i-k\in I,$$

and so $B=b+k\in a+I$. Therefore, $a+I\subseteq b+I$. Similarly, we can show that $b+I\subseteq a+I$, and so $a+I=b+I$.

□

Define

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

Theorem 3.7. *1. The set R/I is a ring with the following addition and multiplication.*

$$\begin{array}{cccc} +: & R/I\times R/I & \to & R/I \\ & (a+I,b+I) & \mapsto & (a+b)+I \end{array}$$

$$\begin{array}{cccc} .: & R/I\times R/I & \to & R/I \\ & (a+I,b+I) & \mapsto & (ab)+I \end{array}$$

Also, $0_{R/I}=I$. The ring R/I is called **quotient ring or factor ring** *of R by I.*

2. If R is commutative, then so is R/I.

3. If R has identity, then so is R/I.

Proof. 1. First we should show that the functions $+$ and $.$ are well-defined, and then other axioms are easy to check. Let $a+I,b+I,c+I,d+I\in R/I$. Assume that $(a+I,b+I)=(c+I,d+I)$. Then $a+I=c+I$ and $b+I=d+I$. Therefore, $a-c,b-d\in I$. Now,

$$(a+b)-(c+d)=(a-c)+(b-d)\in I.$$

Therefore,

$$(a+b)+I=(c+d)+I.$$

Also,

$$ab-cd=ab-cb+cb-cd=(a-c)b+c(b-d)\in I.$$

Therefore,

$$(ab)+I=(cd)+I.$$

We conclude that both $+$ and $.$ are well-defined.

2. Note that $(a+I)(b+I)=(ab)+I=(ba)+I=(b+I)(a+I)$.

3. If R has an identity 1_R, we have 1_R+I is the identity of R/I since

$$(1_R+I)(a+I)=(1_Ra)+I=a+I=(a1_R)+I=(a+I)(1_R+I).$$

□

Week 3, Lecture 2.

Theorem 3.8. *Let R be a ring.*

1. *Let S be a ring. If $f : R \to S$ is a homomorphism, then* $\ker f$ *is an ideal of R.*

2. *Every ideal of R is a kernel of a homomorphism $f : R \to S$.*

Proof.
1. We want to show that $\ker f$ is an ideal. Note that $\ker f$ is not empty since $f(0) = 0$, so $0 \in \ker f$. Let $t, s \in \ker f$ and $r \in R$. Then

$$f(s - t) = f(s) - f(t) = 0 - 0 = 0,$$

so $s - t \in \ker f$. Also,

$$f(rs) = f(r)f(s) = f(r)0 = 0 \quad \text{and} \quad f(sr) = f(s)f(r) = 0f(r) = 0,$$

so $rs, sr \in \ker f$.

2. Let I be an ideal then there is a homomorphism $\pi : R \to R/I$ defined by $\pi(r) = r + I$. Then

$$\ker\pi = \{r \in R : r + I = I\} = \{r \in R : r \in I\} = I.$$

□

Theorem 3.9. *Let $f : R \to S$ be a homomorphism. Then* $\ker f = \{0\}$ *if and only if f is injective.*

Proof. First assume that $\ker\, f = \{0\}$. Then if $f(a) = f(b)$, we have $f(a) - f(b) = 0$, and so $f(a - b) = 0$. Since kerf $= 0$, it follows that $a - b = 0$, i.e., $a = b$.

Conversely, let $a \in \ker\, f$, then we have $f(a) = 0 = f(0)$. As f is injective, we must have $a = 0$. □

Theorem 3.10 (First Isomorphism Theorem). *Let $f : R \to S$ be a homomorphism. Then*

$$R/\ker f \cong \mathrm{Img} f.$$

Proof. Define $\overline{f} : R/I \to \mathrm{Img}\, f$ such that $f(r + I) = f(r)$. We must show that f is a isomorphism, i.e, it is a one-to-one and surjective homomorphism. First we show that f is well-defined. Let $a + \ker\, f = b + \ker\, f$, then $a - b \in \ker\, f$, and so $f(a-b) = 0$. Therefore, $f(a) - f(b) = 0$, and this implies that $\overline{f}(a) = \overline{f}(b)$. It is clear that f is surjective since $\mathrm{Img}\, f = \mathrm{Img}\, \overline{f}$. To show that f is one-to-one, note that if $\overline{f}(a + \ker\, f) = 0$, then $f(a) = 0$, that is $a \in \ker\, f$ and so $a + \ker\, f = \ker\, f = 0_{R/\ker\, f}$. Therefore, by the previous theorem we have that f is one-to-one. Moreover,

$$\overline{f}((a + \ker\, f)(b + \ker\, f)) = \overline{f}(ab + \ker\, f) = f(ab) = f(a)f(b) = \overline{f}(a + \ker\, f)\overline{f}(b + \ker\, f).$$

Similarly, we can show that $\overline{f}((a + \ker\, f) + (b + \ker\, f)) = \overline{f}(a + \ker\, f) + \overline{f}(b + \ker\, f)$.

We can now conclude that f is an isomorphism. □

Theorem 3.11 (The Second Isomorphism Theorem). *Let I and J be ideals in a ring R. Then*

$$\frac{I}{I \cap J} \cong \frac{I + J}{J}.$$

Theorem 3.12 (The Third Isomorphism Theorem). *Let I and K be ideals of R such that $K \subseteq I$. Then $\frac{I}{K}$ is an ideal of R/K, also*

$$\frac{R/K}{I/K} \cong R/I.$$

Theorem 3.13 (The Forth Isomorphism Theorem). *If $f : R \to S$ is a surjective homomorphism of rings with kernel K, then there is a bijection from the set of all ideals of S to the set of all ideals of R that contains K. (Now ask yourself what are the ideals of R/I?)*

4 The Structure of R/I When I Is Prime or Maximal

An ideal P in a commutative ring R is said to be prime if $P \neq R$ and whenever $bc \in P$, then $b \in P$ or $c \in P$.

Theorem 4.1. *Let P be an ideal in a commutative ring with identity. Then P is a prime ideal if and only if the quotient ring R/P is an integral domain.*

Proof. Let P be a prime ideal. Note that $1_{R/P} \neq 0$, otherwise $1_R + P = 0 + P$, which implies that $1_R \in P$, and so $R = P$, a contradiction.Now we show that R does not have any zero-divisors. Assume on the contrary that $a + P$ and $b + P$ are both non-zero, but $(a + P)(b + P) = 0$, then $ab + P = P$, and so $ab \in P$. It follows that $a \in P$ or $b \in P$, which means $a \in P$ or $b \in P$.

Conversely, if R/P is an integral domain, then $1_R + P \neq P$, and so $P \neq R$. Assume that $ab \in P$ but $a \notin P$ and $b \notin P$, then $(a + P)(b + P) = (ab) + P = P = 0_{R/P}$, which means R/P has a zero-divisor, a contradiction. □

Definition. *An ideal M in a ring R is said to be maximal if $M \neq R$ and whenever J is an ideal such that $M \subseteq J \subseteq R$, then either $M = J$ or $J = R$.*

Theorem 4.2. *Let M be an ideal in a commutative ring with identity. Then M is a maximal ideal if and only if the quotient ring R/M is field.*

Proof. Let M be a maximal ideal. With the same argument as in the above theorem, we have that $1_{R/M} \neq 0_{R/M}$. Now we show that every non-zero element in R/M is a unit element. Let $a + M \in R/M$. We first show that the ideal $\langle a + M\rangle = R/M$. On the contrary assume that $\langle a+M\rangle \neq R/M$, By the forth isomorphism theorem we have $\langle a+M\rangle$ is equal to some ideal J/M of R/M. Note that J is an ideal that containing M. Since M is maximal we have to have $J = R$, which is equivalent to say that $\langle a + M\rangle = R/M$, and so there is an element $b + M$ such that $(b + M)(a + M) = 1 + M$. Therefore, every element in R/M has an inverse and so R/M is a field. Conversely, assume that R/M is a field. Since $1_{R/M} \neq 0 + M$ we have that $M \neq R$. Now assume that there is an ideal J such that $M \subset J$. Then J/M is an ideal of R/M (again by forth isomorphism theorem), but we have R/M is a field and every element is invertible so there is a nonzero and so an invertible element in $a + M \in J/M$. Therefore, $J/M = R/M$ and so $R = J$. Therefore, M is a maximal ideal. □

Corollary 4.3. *If M is a maximal ideal of R, then M is prime too.*

5 EPU

Definition. *Let R be a commutative ring with identity. Let a and b be in R.*

- *An element $a \in R$* **divides** *$b \in R$, written $a|b$, if $b = ac$ for some $c \in R$.*
- *Two elements a and b are said to be* **associate** *if $a|b$ and $b|a$.*
- *A nonzero nonunit element $p \in R$ is said to be* **prime** *if $p|ab$, then $p|a$ or $p|b$.*
- *A nonzero nonunit element $p \in R$ is said to be* **irreducible** *if $a = rs$, then r or s is a unit.*

Theorem 5.1. *Let a, b and u be elements of a commutative ring R with identity.*

1. *$a|b$ if and only if $\langle b \rangle \subseteq \langle a \rangle$.*
2. *a and b are associate if and only if $\langle a \rangle = \langle b \rangle$.*
3. *u is a unit if and only if $u|r$ for all $r \in R$.*
4. *u is a unit if and only if $\langle u \rangle = R$.*
5. *The relation "a is an associate of b" is an equivalence relation on R.*
6. *If $a = br$ with $r \in R$ a unit, then a and b are associates. If R is an integral domain, the converse is true.*

Note that 2 is a prime element in $\mathbb{Z}_6$ but it is not an irreducible element since $2 = 2.4$.

Definition. *An integral domain R is a* **unique factorization domain (UFO)** *provided that every nonzero, nonunit element of R is the product of irreducible elements, and this factorization is unique up to associates; that is, if*

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

with each p_i and q_j irreducible, then $r = s$ and, after reordering and relabeling if necessary,

$$p_i \text{ is an associate of } q_i \text{ for } i = 1, 2, \dots, r.$$

Definition. *A* **principal ideal ring** *is a ring in which every ideal is a principal ideal. A principal ideal ring which is also an integral domain is called a principal ideal domain.*

Definition. *An integral domain R is a* **Euclidean domain** *if there is a function δ from the nonzero elements of R to the nonnegative integers with these properties:*

- *If a and b are nonzero elements of R, then $\delta(a) \leq \delta(ab)$.*
- *If $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$.*

Example 5.2.

1. *Every field is an integral domain with the function δ given by $\delta(x) = 1$ for all x in the field.*
2. *$\mathbb{Z}$ is a Euclidean domain with the function δ given by $\delta(a) = |a|$.*

3. $\mathbb{F}[x]$ *the polynomials with coefficients in the field* $\mathbb{F}$ *is a Euclidean domain with the function* δ *given by* $\delta(f(x)) = \deg(f(x))$.

4. *The ring of Gaussian integers*

$$\mathbb{Z}[i] = \{s + ti : s, t \in \mathbb{Z}\}$$

   is a Euclidean domain with the function δ *given by* $\delta(s + ti) = s^2 + t^2$.

Week 4, Lecture 2.

Theorem 5.3. *Let p and c be non-zero elements in an integral domain R.*

1. *p is prime if and only if $\langle p\rangle$ is nonzero prime.*
2. *c is irreducible if and only if $\langle c\rangle$ is maximal in the set S of all proper principal ideals of R.*
3. *Every prime element of R is irreducible.*
4. *If R is a principal ideal domain, then p is prime if and only if p is irreducible.*
5. *Every associate of an irreducible (resp. prime) element of R is irreducible (resp. prime).*
6. *The only divisors of an irreducible element of R are its associates and the units of R.*

Proof. 1. Let p be a prime element and $ab \in \langle p\rangle$. Then for some $r \in R$, we have $pr = ab$, i.e., $p|ab$ and since p is a prime element, it follows that $p|a$ or $p|b$, that is $a \in \langle p\rangle$ or $b \in \langle p\rangle$.

Conversely, assume that $\langle p\rangle$ is a prime ideal and $p|ab$, then $ab \in \langle p\rangle$, and since $\langle p\rangle$ is a prime ideal, we have a or b is in $\langle p\rangle$. Therefore, $p|a$ or $p|b$.

2. Assume that c is an irreducible elements and there is a proper principle ideal $\langle d\rangle$ that contains $\langle c\rangle$, then $d|c$, and so $da = c$ for some $a \in R$, since c is an irreducible element we must have a is a unit and so $\langle c\rangle = \langle d\rangle$.

   Conversely, assume that $\langle c\rangle$ is maximal in the set S of all proper principal ideals of R. Then if $c = rs$ and none of r and s are units, we have $\langle c\rangle = \langle r\rangle$. Then there is a unit u such that $c = ru$. Therefore, $ru = rs$ and so $u = s$.

3. If p is a prime element and $p = rs$, then $p|r$ or $p|s$. Without loss of generality assume that $p|s$, then since $s|p$, we have $\langle p\rangle = \langle s\rangle$, and since they are elements of integral domain, same as previous part, we have r is a unit.

4. By (3) every prime is irreducible in an integral domain, so we only need to show that every irreducible is prime in a principal ideal domain. Let p be an irreducible element, then by (2) $\langle p\rangle$ is a maximal ideal in R, and so it is a prime ideal. Therefore, by (1) p is a prime element.

5. Let p be an irreducible element. Then if q is associate to p by previous theorem part (6), there is a unit u such that $p = qu$. Assume that q is not an irreducible element, then $q = ab$ for some nonzero nonunit elements a and b, and so $p = (ua)b$. Note that ua is not unit because otherwise a is a unit. Therefore, q is not an irreducible element, a contradiction.

6. If $r|p$ where p is an irreducible element, then we have $rs = p$ for some $s \in R$. Since p is irreducible, r or s is a unit, which means either r is a unit or r is an associate of p.

$\square$

Week 4, Lecture 3

Example 5.4. An example of a ring that is an integral domain and it has some irreducible elements that are not prime

Let R be the subring $\{a+b\sqrt{10} : a, b \in \mathbb{Z}\}$ of real numbers. Note that $2, 3, 4+\sqrt{10}, 4-\sqrt{10}$ are irreducible elements but not prime elements. Also, note that this subring also is not a UFD. Moreover, in this subring every element can be factored into irreducible elements but it is not unique.

Proposition 5.5. *Every irreducible element in a UFD is a prime element.*

Proof. Let p be an irreducible element in a UFD, say R. If $ab \in \langle p\rangle$ for some $a, b \in R$, then $pr = ab$. Now factor $r = r_1 \dots r_k$, $a = a_1 \dots a_t$, and $b = b_1 \dots b_t$ into irreducible elements. Then p must be equal to some a_i or b_j which means $p|a$ or $p|b$, and so $a \in \langle p\rangle$ or $b \in \langle p\rangle$. Therefore, $\langle p\rangle$ is a prime ideal and so p is a prime element. $\square$

Our goal now is to show that every PID is a UFD. In order to prove that we need the following lemma.

Lemma 5.6. *If R is a principal ideal domain and*

$$\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \dots$$

is a chain of ideals in R, then for some positive integer n, $\langle a_j\rangle = \langle a_n\rangle$ for all $j \geq n$.

Proof. Let

$$I = \bigcup_{i=1} \langle a_i\rangle.$$

Then note that I is an ideal of R. Since R is a principal ideal domain, there is an element $c \in R$ such that $I = \langle c\rangle$. Since $c \in I$, there is an $\langle a_n\rangle$ such that $c \in \langle a_n\rangle$. Therefore, we must have

$$\langle a_n\rangle = \langle c\rangle.$$

$\square$

Theorem 5.7. *Every PID is a UFD.*

Proof. Assume that in the PID R there is an element a that can not be written as the product of irreducible elements. So we can write $a = a_1 b_1$ such that a_1 and b_1 are not units and at least one of a_1 or b_1 can not be written as product of irreducible elements. WLOG assume that we can not write a_1 as a product of prime elements. Note that $\langle a\rangle \subsetneq \langle a_1\rangle$, because otherwise b_1 is a unit. Now we repeat the process for a_1. So, we can write $a_1 = a_2 b_2$ such that $\langle a_1\rangle \subsetneq \langle a_2\rangle$. If we continue this process we will have the following chain that never end

$$\langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \langle a_3\rangle \subsetneq \cdots$$

that is a contradiction since the previous theorem stated that any chain of ideal in a PID is stable.

Now we will show that this factorization is unique up to associates and reordering. Let a be an arbitrary element and we write a as a product of irreducible elements in the following ways:

$$p_1 p_2 \cdots p_s = a = q_1 q_2 \cdots q_r.$$

Without loss of generality assume that $r \geq s$. Note that $p_1|q_1q_2\cdots q_r$. Therefore, Since in a PID every irreducible is a prime, we have that $p_1|q_i$ for some i. After rearranging and relabeling the q_i's if necessary, we may assume that $p_1|q_1$. Therefore, $p_1u_1 = q_1$ and as q_1 is an irreducible element we must have u_1 is a unit. Therefore, q_1 and p_1 are associate. So we can write

$$p_1p_2\cdots p_s = a = u_1p_1q_2\cdots q_r,$$

for some unit u_1. By the cancellation law we have

$$p_2\cdots p_s = (u_1q_2)\cdots q_r.$$

Note that u_1q_2 also is an irreducible element. Continue the same argument until there is no more p_i's left. So if $s \neq r$, we have $1 = u_1u_2\ldots u_sq_{s+1}\ldots q_{r-1}q_r$, and so q_r is a unit, a contradiction. Therefore, we must have $r = s$ and the factorization is unique up to associates. $\square$

Remark. *The converse is not true since $\mathbb{Z}[x]$ is a UFD but not a PID.*

Week 5, Lecture 1
Well-ordering Axiom: Every nonempty subset of the set of nonnegative integers contains a smallest element.

Theorem 5.8. *Every Euclidean domain is a PID.*

Proof. Let I be an ideal of the Euclidean domain R, and consider the set $\{\delta(a) : a \in I, a \neq 0\}$. By The well-ordering principal there is an element $b \in I$ such that $\delta(b)$ is minimal in the set $\{\delta(a) : a \in I, a \neq 0\}$. We claim that $\langle b \rangle = I$. So we must show that every $a \in I$ is in $\langle b \rangle$. Since R is a Euclidean domain, there are elements r and q in R such that $b = aq + r$ and either $r = 0$ or $\delta(r) < \delta(a)$. Note that $b - aq = r$, and also b and a are in I, therefore, $b - aq \in I$. So, $r \in I$. It is not possible to have $r \neq 0$, since $\delta(r) < \delta(a)$ and $\delta(a)$ is the smallest element in I. So we must have $r = 0$, and $b = aq$, i.e., $a \in \langle b \rangle$. $\square$

Definition.
1. *A* **Dedekind domain** *is an integral domain in which every nonzero proper ideal factors into a product of prime ideals.*
2.

Remark. *Let R be the following ring of the complex numbers:*

$$R = \{a + b(1 + \sqrt{19}i)/2 : a, b \in \mathbb{Z}\}.$$

Then R is a principal ideal domain that is not a Euclidean domain.

Definition. *Let A be a nonempty subset of a commutative ring R.An element d is a great common divisor of X provided:*

1. *$d|x$ for all $x \in X$.*
2. *if $c|x$ for all x in X, then $d|c$.*

Remark. *There are some commutative rings that a set X of its elements does not have a GCD, for example look at the ring $2\mathbb{Z}$ and the set $\{2, 4\}$.*

Definition. *Let $a_1, a_2, \ldots, a_n$ be some elements in a ring R with identity. Then if the GCD of $a_1, a_2, \ldots, a_n$ is 1, then $a_1, a_2, \ldots, a_n$ are said to be* **relatively prime**.

Theorem 5.9. *If R is a UFD, then there is a GCD of $a_1, a_2, \ldots, a_n$ in R.*

Proof. Factor each $a_i = u_i p_1^{m_{i1}} \ldots p_k^{m_{ik}}$ into irreducible elements, where all p_{ij} are distinct and $m_{ij} \geq 0$. Show that $d = p_1^{k_1} \ldots p_n^{k_n}$ is the greatest common multiple of $a_1, a_2, \ldots, a_n$, where $k_j = min\{m_{1j}, \ldots, m_{nj}\}$. $\square$

6 $\mathbb{Z}[\sqrt{d}]$, an integral domain which is not a UFD

An square-free element in $\mathbb{Z}$ is an element $d \neq 1$ such that $d = -1$ or $d = p_1 p_2 \ldots p_k$ for distinct prime numbers $p_1, p_2, \ldots, p_k$.

For a square-free number d define

$$\mathbb{Z}[\sqrt{d}] = \{a + b\mathbb{Z}[\sqrt{d}] : a, b \in \mathbb{Z}\}.$$

Definition. *The function* $N(s + t\sqrt{d}) = (s + t\sqrt{d})(s - t\sqrt{d}) = s^2 - dt^2$ *is called the* **norm**.

Theorem 6.1. *If d is a square-free integer, then for all $a, b \in \mathbb{Z}[\sqrt{d}]$*

1. $N(a) = 0$ *if and only if* $a = 0$.
2. $N(ab) = N(a)N(b)$.

Proof. The second part is a straight forward computation so we only proof the first part. Let $a = s + t\sqrt{d}$. If $d = -1$, then $N(a) = 0$ if and only if $s^2 - dt^2 = 0$ if and only if $s^2 = -t^2$. So we must have $s = t = 0$. Now assume that $d \neq -1$. Note that $s, t \neq \pm 1$. Then $N(a) = 0$ if and only if $s^2 = dt^2$. Factor s and t into primes. If p be a prime which appears in the factor of d into primes, then in the left hand side p has an even power while in the right hand side it has a odd power, which is impossible. Therefore, the only case we must have is that $a = 0$ and $b = 0$. $\square$

Week 5, Lecture 2

Theorem 6.2. *Let d be a square-free integer. Then $u \in \mathbb{Z}\sqrt{d}$ is a unit if and only if $N(u) = \pm 1$.*

Proof. Assume that u is a unit, then there is an element v such that $uv = 1$, then $\delta(uv) = 1$ and so $\delta(u)\delta(v) = 1$ by the previous theorem. Therefore, we must have $\delta(u) = 1$ or -1.

Conversely, assume that $u = a + b\sqrt{d}$ and $\delta(u) = 1$, thus $a^2 - db^2 = 1$. Now consider the element $v = a - b\sqrt{d}$, then $uv = a^2 - db^2 = 1$. □

Example 6.3. *Is $u = 3 + 2\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$? Yes because $\delta(u) = 3^2 - 2.2^2 = 1$.*

Corollary 6.4. *Let d be a square free integer. Then if $d > 1$, then $\mathbb{Z}[\sqrt{d}]$ has infinitely many units. If $d = -1$, then the units are $\pm 1, \pm i$. If $d < -1$, then the units are ± 1.*

Theorem 6.5. *Let d be a square-free integer. Then every nonzero, nonunit element in $\mathbb{Z}[\sqrt{d}]$ is a product of irreducible elements.*

Proof. Let S be the set of all elements in $\mathbb{Z}[\sqrt{d}]$ that cannot be written as the product of irreducible elements. We want to show that $S = \emptyset$. Assume otherwise, then by well-ordering axiom, the set $\{|N(t)| : t \in S\}$ has an element a such that for any $t \in S$, $|N(a)| \leq N(t)$. Since a is not irreducible, there are nonunits (because of non-irreduciblity of a) elements b, c such that $a = bc$ and b or c is in S. Without loss of generality assume that $b \in S$. Then $N(a) = N(bc) = N(b)N(c)$ by the previous theorem. Therefore, $|N(a)| = |N(b)||N(c)|$. If $N(b), N(c) = \pm 1$, otherwise they are units which is not possible. Therefore, $N(a) > N(b)$, a contradiction. □

Example 6.6. *Consider $\mathbb{Z}[-5]$. Then $2 = 2.3$ and also $2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.*

7 The field of quotients of an integral domain

Let R be an integral domain. Define a relation $\backsim$ on the set $S = \{(a, b) : a, b \in R, b \neq 0\}$ by

$$(a, b) \backsim (c, d) \text{ if and only if } ad = bc.$$

Theorem 7.1. *The relation $\backsim$ is an equivalence relation on S.*

Proof. Reflexive: it is easy to see that $(a, b) \backsim (a, b)$ since $ab = ba$.
Symmetric: if $(a, b) \backsim (c, d)$, then $ad = bc$, by commutativity $cb = da$, thus $(c, d) \backsim (a, b)$.
Transitivity: if $(a, b) \backsim (c, d) \backsim (e, f)$, then $ad = bc$ and $cf = de$. Multiplying $ad = bc$ by f we have

$$adf = bcf \to a(df) = b(cf) = b(de).$$

Therefore, $d(af) = d(be)$. By cancellation law, we have $af = be$ and so $(a, b) = (e, f)$. □

Denote the equivalence class of (a, b), i.e., $[(a, b)]$, by $\frac{a}{b}$. Therefore, $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.

Theorem 7.2. *Let R be an integral domain. Then the set*

$$F = \{\frac{a}{b}, a, b \in R, b \neq 0\}$$

is a field with the following addition and multiplication,

$$\frac{a}{b} + \frac{c}{d} = \frac{(ad+bc)}{(bd)} \qquad\qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Proof. First we showed show that the addition and multiplication are well-defined and then we check that F is a field.
• Addition is well-defined: Let $\frac{a}{b} = \frac{a^{'}}{b^{'}}$ and $\frac{c}{d} = \frac{c^{'}}{d^{'}}$. We want to show that $\frac{a}{b} + \frac{c}{d} = \frac{a^{'}}{b^{'}} + \frac{c^{'}}{d^{'}}$. Since $\frac{a}{b} = \frac{a^{'}}{b^{'}}$ and $\frac{c}{d} = \frac{c^{'}}{d^{'}}$, we have

$$ab^{'} = a^{'}b \qquad\qquad cd^{'} = c^{'}d.$$

Therefore,

$$ab^{'}dd^{'} = a^{'}bdd^{'} \qquad\qquad cd^{'}bb^{'} = c^{'}dbb^{'}.$$

So

$$ab^{'}dd^{'} + cd^{'}bb^{'} = a^{'}bdd^{'} + c^{'}dbb^{'}$$

Thus we have

$$\Rightarrow (ad+cd)b^{'}d^{'} = (a^{'}d^{'} + c^{'}b^{'})bd \Rightarrow \frac{(ad+bc)}{(bd)} = \frac{(a^{'}d^{'} + b^{'}c^{'})}{(b^{'}d^{'})}.$$

• Multiplication is well-defined: Let $\frac{a}{b} = \frac{a^{'}}{b^{'}}$ and $\frac{c}{d} = \frac{c^{'}}{d^{'}}$. We have

$$ab^{'} = a^{'}b \qquad\qquad cd^{'} = c^{'}d.$$

We want to show that $\frac{a}{b}\frac{c}{d} = \frac{a^{'}}{b^{'}}\frac{c^{'}}{d^{'}}$, i.e., $(ac)(b^{'}d^{'}) = bd(a^{'}c^{'})$. Note that

$$(ac)(b^{'}d^{'}) = (ab^{'})(cd^{'}) = (a^{'}b)(c^{'}d) = (bd)(a^{'}c^{'}).$$

Therefore, $\frac{a}{b}\frac{c}{d} = \frac{a^{'}}{b^{'}}\frac{c^{'}}{d^{'}}$.
Moreover, it is straight forward to check that

- $0_F = \frac{0}{b}$ for any $b \neq 0$.
- $\frac{a}{b} + \frac{-a}{b} = 0_F$.
- The identity element is $\frac{1}{1}$.
- The inverse of a nonzero element $\frac{a}{b}$ is $\frac{b}{a}$.
- We have

$$\frac{a}{b}(\frac{c}{d} + \frac{r}{s}) = \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{r}{s}.$$

□

Week 5, Lecture 3

8 If R is a UDF, so is $R[x]$

Definition. *Let R be a UFD. The polynomial $f(x) \in R[x]$ is called primitive if the only divisors of $f(x)$ of degree zero are units.*

Let R be a UFD.

1. The units of $R[x]$ are the units of R.
2. If p is irreducible in R, then it is irreducible in $R[x]$.
3. An irreducible polynomial is a primitive polynomial.
4. Every polynomial $f(x) \in R[x]$ factors as $f(x) = cg(x)$ where $c \in R$ and $g(x)$ is a primitive polynomial.
5. Every primitive polynomial of degree 1 is irreducible.

Theorem 8.1. *Let R be a UFD. Then every nonzero nonunit polynomial $f(x) \in R[x]$ is a product of irreducible elements.*

Proof. We prove this theorem by induction on the degree of $f(x)$.

If $deg(f(x)) = 0$, then $f(x)$ is an irreducible elements of R and since R is a UFD and every irreducible element of R is an irreducible element of $R[x]$, so we have that $f(x)$ is irreducible in $R[x]$.

If $deg(f(x)) = 1$, then we can write $f(x) = cg(x)$ where $c \in R$ and $g(x)$ is a primitive element of degree 1. Since c can be written as product of irreducible elements of R and $g(x)$ is an irreducible element, so $f(x)$ can be written as the product of irreducible elements.

Now, assume that $deg(f(x)) = r > 1$ and for every polynomial of degree less than r the theorem is true. If $f(x)$ is irreducible we are done, otherwise there is a primitive polynomial $g(x)$ such that $f(x) = cg(x)$ where $c \in R$. If $g(x)$ is irreducible then since c can be written as product of primes, $f(x) = cg(x)$ is a product of irreducible elements. If $g(x)$ is not an irreducible element then there are polynomials $h(x)$ and $g(x)$ such that non of them is of degree 0 and $g(x) = h(x)k(x)$. Note that $deg(f(x)) = deg(g(x)) > deg(h(x)), deg(k(x))$, thus $h(x)$ and $k(x)$ are product of irreducible elements. Therefore, $f(x) = ch(x)k(x)$ is a product of irreducible elements. □

Lemma 8.2. *Let p be an irreducible element in a UFD R. If $p|f(x)g(x)$ where $f(x), g(x) \in R[x]$, then $p|f(x)$ or $p|g(x)$.*

Corollary 8.3. *Let R be a UFD. The product of primitive polynomials in $R[x]$ is primitive.*

Proof. Let $f(x), g(x)$ be primitive polynomials in $R[x]$. Then if $c|f(x)g(x)$ and c is not a unit and nonzero, then $c = p_1 \dots p_k$, where each p_i is an irreducible elements. Thus $p_1|f(x)g(x)$ and so $p|f(x)$ or $p|g(x)$ which means $f(x)$ or $g(x)$ is not primitive. □

Theorem 8.4. *Let R be a UFD and r, s two nonzero elements of R. Let $f(x)$ and $g(x)$ be primitive elements in $R[x]$ such that $rf(x) = sg(x)$. Then r, s are associates in R and $f(x), g(x)$ are associates in $R[x]$.*

Proof. If r is a unit then $f(x) = r^{-1}sg(x)$, and since $f(x)$ is primitive, $r^{-1}s$ is a unit and so $f(x)$ and $g(x)$ are associates.

If r is not a unit, then it is a product of irreducible elements, so $r = p_1 \dots p_k$ where p_i's are irreducible. Therefore, $p_1 \dots p_k f(x) = sg(x)$. We have By lemma 8.2 that $p_1 | sg(x)$ so $p_1 | s$ or $p_1 | g(x)$. Note that $g(x)$ is a primitive element, therefore, $p_1 | s$. Let $s = p_1 t$. Then $p_1 p_2 \dots p_k f(x) = p_1 t g(x)$. By cancellation law, we have $p_2 \dots p_k f(x) = tg(x)$. Now $p_2 | tg(x)$, and similarly we have $p_2 | t$. Let $t = p_2 z$. Then $s = p_1 p_2 z$. Then $p_2 \dots p_k f(x) = p_2 z g(x)$. By cancellation we have $p_3 \dots p_k f(x) = zg(x)$. Repeat the argument k times, then we have $f(x) = wg(x)$ for some $w \in R$. Since $f(x)$ is primitive we must have w is a unit, and so $f(x)$ and $g(x)$ are associate. Moreover, we have $r = p_1 p_2 \dots p_k$ and $s = p_1 p_2 \dots p_k w$ for some unit $w \in R$. Therefore, r and s are associate in R. □

Corollary 8.5. *Let R be a UFD, F its field of quotients. Let $f(x)$ and $g(x)$ be primitive in $R[x]$. If $f(x)$ and $g(x)$ are associate in $F[x]$, then they are associate in $R[x]$.*

Proof. Since $f(x)$ and $g(x)$ are associate in $F[x]$, there is a unit $a/b, a, b \in R, b \neq 0$ such that $f(x) = a/bg(x)$, then we have $bf(x) = ag(x)$. By the previous theorem we have $f(x)$ and $g(x)$ are associate in $R[x]$. □

Corollary 8.6. *Let R be a UFD and F be its quotient field. If $f(x) \in R[x]$ has positive degree and is irreducible in $R[x]$, then $f(x)$ is irreducible in $F[x]$.*

Proof. Assume on the contrary that $f(x)$ is not irreducible in $F[x]$. Then there are polynomials $g(x) = b_0'/b_0 + b_1'/b_1 x + \dots + b_n'/b_n x^n$ and $h(x) = c_0'/c_0 + c_1'/c_1 x + \dots + c_n'/c_n x^n$ in $F[x]$ with positive degree such that $f(x) = g(x)h(x)$. Let $b = lcm(b_0, \dots, b_n)$. Then $bg(x)$ is in $R[x]$, so there is an element $a \in R$ and a primitive polynomial $g_1(x) \in R[x]$ such that $bg(x) = ag_1(x)$. Similarly, we have $ch(x) = dh_1(x)$ where $c, d \in R$ and $h_1(x) \in R[x]$ is a primitive polynomial. We have $bdf(x) = bdg(x)h(x) = abg_1(x)h_1(x)$. By Corollary 8.3, we have $g_1(x)h_1(x)$ is primitive and also $f(x)$ is primitive too. Therefore, bd and ab are associate in R, and so there is a unit u such that $ubd = ab$. We have $bdf(x) = ubdg(x)$. By cancellation we have $f(x) = ug_1(x)h_1(x)$, and so $f(x)$ is not irreducible in $R[x]$. □

Theorem 8.7. *If R is a UFD, so is $R[x]$.*

Proof. We already showed that every polynomial in $R[x]$ is a product of irreducible polynomials. So we must show that this factorization is unique up to reordering and association.

Assume that we factor a nonzero and nonunit polynomial into the following two factors

$$c_1 \cdots c_m p_1(x) \dots p_k(x) = d_1 \cdots d_n q_1(x) \dots q_t(x),$$

where c_i, d_j are irreducible in R and $p_i(x)$ and q_j are irreducible in $R[x]$. By Theorem 8.4 we have $c_1 \cdots c_m$ and $d_1 \cdots d_n$ are associate in R and also $p_1(x) \dots p_k(x)$ and $q_1(x) \dots q_t(x)$ are associates in $R[x]$. Since R is a UFD and we have $c_1 \cdots c_m = (ud_1) \cdots d_n$ for some unit $u \in R$. We have that $m = n$ and $c_i = u_i d_i$ for some units u_i and for all i.

Let F be the field of quotients of R. Then by Corollary 8.6, $p_i(x)$ and $q_j(x)$ are irreducible in $F[x]$. Since there is a unit $v \in R$ such that $p_1(x) \dots p_k(x) = vq_1(x) \dots q_t(x)$ and $F[x]$ is a UFD, we have $k = t$ and after reordering we have that $p_i(x)$ and $q_i(x)$ are associate in $F[x]$ which by Corollary 8.5 we have thery are associate in $R[x]$.

□

Method of proofs

Our goal is to prove a statement. Assume we have a statement P, note that P can be of form $A \Rightarrow B$ (i.e., an implication), for example: if x is odd, then $x+1$ is even, or just a proposition A, for example: $\sqrt{2}$ is irrational.

If we want to show that $A \Rightarrow B$ it is equivalent to show one of the following:
Contrapositive: $\neg B \Rightarrow \neg A$.
Contradiction: ($\neg B$ and A) $\Rightarrow C$, where C is obviously false.

If we want to show that a statement which is just a proposition A, is true, then we can not use contrapositive, and we only can directly prove it or use contradiction: $\neg A \Rightarrow C$, where C is obviously false.

9 Vector Spaces

Let F be a field. We call $(V, +, .)$ a **vector space over** F when $(V, +)$ is an abelian group, and

$$. : F \times V \to V$$

such that for all $a, a_1, a_2 \in F$ and $v, v_1, v_2 \in V$

1. $a(v_1 + v_2) = av_1 + av_2$;
2. $(a_1 + a_2)v = a_1v + a_2v$;
3. $a_1(a_2v) = (a_1a_2)v$;
4. $1_F v = v$.

Example 9.1. *If F and K are fields such that $F \subseteq K$, we say K is an* **extension field** *of F. Any extension field of F is a vector space over F with the same addition as field K, and the scalar multiplication is the multiplication of K.*

Let $v_1, \ldots, v_n$ be in the vector space V over F.

- We say vector w is a l**linear combination** of vectors $v_1, \ldots, v_n$ if there are scalars $c_1, \ldots, c_n \in F$ such that $w = c_1v_1 + \ldots, c_nv_n$.
- The set of all linear combination of vectors $v_1, \ldots, v_n$ is denoted by $Span\{v_1, \ldots, v_n\}$. i.e.,
$$Span\{v_1, \ldots, v_n\} = \{c_1v_1 + \cdots + c_nv_n : c_1, \ldots, c_n \in F\}.$$
- We say the set of vectors $\{v_1, \ldots, v_n\}$ spans V if $V = Span\{v_1, \ldots, v_n\}$.
- A subset $\{v_1, \ldots, v_n\}$ of V is said to be **linearly independent** provided that whenever
$$c_1v_1 + \ldots, c_nv_n = 0,$$
with each $c_i \in F$, then $c_1 = c_2 = \ldots, c_k = 0$.
- A subset $\{v_1, \ldots, v_n\}$ of V is said to be a **basis** for V if the set is linearly independent and also $Span\{v_1, \ldots, v_n\} = V$.

Theorem 9.2. *Let V be a vector space over a field F.*

1. *The subset $\{u_1, u_2, \ldots, u_n\}$ of V is linearly dependent over F if and only if some u_k is a linear combination of the preceding ones, $u_1, u_2, \ldots, u_{k-1}$.*

2. *All bases for V have the same size (cardinality).*

3. *If a basis for V has a finite number of vectors, then V is called* **finite dimensional**. *The number of elements in any basis of V is called* **dimension** *of V, is denoted by $[V : F]$. If V does not have a finite basis, then V is said to be* **infinite dimensional** *over F.*

4. *Let $\{v_1, v_2, \ldots, v_k\}$ be a basis for V. If a subset $\{u_1, u_2, \ldots, u_n\}$ spans V, then $n \geq k$. If a subset $\{w_1, w_2, \ldots, w_m\}$ is linearly independent, then $m \leq k$.*

5. *Let K and F be fields such that $F \subseteq K$. Then $[K : F] = 1$ if and only if $K = F$.*

Definition. *We say that K is a* **finite-dimensional extension** *of F if K, considered as a vector space over F, is finite dimensional over F.*

Let V and W be vector spaces on a field F. A **homomorphism** f form V to W is a map that for all $c \in F, v, w \in V$, $f(cv + w) = cf(v) + w$. An isomorphism form V to W is a homomorphism that is injective and surjective.

Theorem 9.3. 1. *Let F, K and L be fields with $F \subseteq K \subseteq L$. If $[K : F]$ and $[L : K]$ are finite, then L is a finite-dimensional extension of F and $[L : F] = [L : K][K : F]$.*

2. *Let K and L be finite dimensional extension fields of F and let $f : K \to L$ be an isomorphism such that $f(c) = c$ for every $c \in F$. Then $[K : F] = [L : F]$.*

10 Simple Extensions

Let K be an extension of the field F and $u \in K$. Let $F(u)$ be the intersection of all subfield of K containing F and u.

- $F(u)$ is a subfield of K. $F(u)$ is the smallest subfield of K containing F and u.
- $F(u)$ is called a simple extension of F.

Definition. *Let field K be an extension of field F and $u \in K$. Then u is said to* **algebraic** *over F if u is the root of some nonzero polynomial in $F[x]$. When u is not a root of some polynomial we say u is* **transcendental**.

Example 10.1. *$i \in \mathbb{C}$ is algebraic over $\mathbb{R}$.*
$\sqrt{2}$ is algebraic over $\mathbb{Q}$.

Theorem 10.2. *Let $u \in K$ be algebraic over F. Then there exists a unique monic irreducible polynomial $p(x)$ in $F[x]$ that has u as a root. Furthermore, if u is a root of $g(x) \in F[x]$, then $p(x)$ divides $g(x)$.*

Proof. Let S be the set of all nonzero polynomials in $F[x]$ that have u as a root. Since u is algebraic over F, at least there is a polynomial in $F[x]$ that has u as a root, so $S \neq \emptyset$. By the Axiom of Choice there is an element $p(x)$ in S with the smallest degree. We now show that $p(x)$ is irreducible. Assume $p(x) = f(x)g(x)$. If both $f(x)$ and $g(x)$ are not constant, then $p(u) = f(u)g(u) = 0$, and since F is an integral domain, we must have $f(u) = 0$ or $g(u) = 0$. Without loss of generality assume that $f(u) = 0$. However, $deg(f(x)) < deg(p(x))$, and $f(u) = 0$, this yields a contradiction since we chose $p(x)$ in a way that it has the smallest degree in S. If a polynomial has u as a root, all constant multiple of that polynomial has u as a root, we may assume that $p(x)$ is monic. Now we show if $g(u) = 0$ for some polynomial $g(x) \in F[x]$, then $p(x)|g(x)$. By division algorithm there are polynomials $f(x)$ and $r(x)$ such that $g(x) = p(x)f(x) + r(x)$ and degree of $r(x)$ is either zero or $deg(r(x)) < deg(p(x))$. Since $g(u) = 0$ and $f(u) = 0$ and we have $g(u) = p(u)f(u) + r(u)$, we have $r(u) = 0$. Note that $r(x)$ must be zero because we have chosen $p(x)$ in a way that has the smallest degree amongst all polynomials with u as a root. Thereofore, $p(x)|g(x)$. Now we prove that $p(x)$ is unique. Assume $p_1(x)$ is also a monic polynomial has u as a root and if u is a root of $g(x) \in F[x]$, then $p_1(x)$ divides $g(x)$. Therefore, $p_1(x)|p(x)$, and since they are irreducible we must have $p_1(x) = up(x)$ for some unit u. Since both polynomials are monic we conclude that $p(x) = p_1(x)$. □

Definition. *If K is an extension of field of F and $u \in K$ is algebraic over F, then the unique monic, irreducible polynomial $p(x)$ in the above thorem is called* **minimal polynomial** *of u over F.*

As an example $x^2 - 3$ is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}$.

Theorem 10.3. *Let K be an extension field of F and $u \in K$ be algebraic over F with minimal polynomial $p(x)$ of degree n. Then*

1. *$F(u) \cong F[x]/\langle p(x) \rangle$.*
2. *$\{1_F, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $F(u)$ over F.*
3. *$[F(u) : F] = n$.*

Proof. Proof of (1): Define a fucntion $\psi : F[x] \to F(u)$ such that $\psi(f(x)) = f(u)$. This function is a ring homomorphism. By the first isomorphism theorem we have

$$Img\psi \cong F(x)/ker(\psi).$$

So we only need to show that $ker(\psi) = \langle p(x) \rangle$ and $Img\psi = F(u)$. Note that $ker(\psi) = \{f(x) : f(u) = 0\}$ i.e., the set of all polynomials that have u as a root. By the previous theorem, if a polynomial has u as a root then $p(x)$ divides it, therefore, $ker(\psi) \subseteq \langle p(x) \rangle$, and it is clear that $\langle p(x) \rangle ker(\psi)$. Thus $\langle p(x) \rangle = ker(\psi)$. So $F[x]/\langle p(x) \rangle = Img\psi$. Moreover, since image of ψ is a field that contains both F and u it must be $F(u)$.

Proof of (2) and (3): We first show that $\{1_F, u, u^2, \ldots, u^{n-1}\}$ spans $F(u)$. Any element of $F(u)$ is of the form $f(u)$ for some polynomial $f(x) \in F(x)$. If $deg(p(x)) = n$, then by the devision algorithm we have $f(x) = p(x)q(x) + r(x)$, where $r(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$ for some $b_i \in F$. Then $f(u) = p(u)q(u) + r(u) = b_0 + b_1 u + \ldots + b_{n-1}u^{n-1}$.

Now we show that $\{1_F, u, u^2, \ldots, u^{n-1}\}$ is linearly independent. Assume on the contrary that the set is not linearly independent, then there are elements $a_0, a_1, \ldots, a_{n-1} \in F$ such that at leat one of them is not zero and $a_0 + a_1 u + \ldots + a_{n-1}u^{n-1} = 0$. Therefore the polynomial $g(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ has u as its root, but it is not possible sice $p(x)$ has the smallest degree amongst all polynomials that have u as a root. □

Example 10.4. *The set* $\{1, \sqrt{3}\}$ *is a basis for* $\mathbb{Q}[\sqrt{3}]$ *and moreover,* $\mathbb{Q}[\sqrt{3}] \cong Q[x]/\langle x^2 - 3 \rangle$.

Corollary 10.5. *If u and v have the same minimal polynomial $p(x)$ in $F[x]$, then $F(u) \cong F[v]$.*

Definition. *Let R, S be rings and Q and T be subring of R and S respectively. We say the isomorphism $\sigma : Q \to T$ extends to the isomorphism $f : R \to S$ if $f(r) = \sigma(r)$ for every $r \in Q$.*

Example 10.6. *If $\sigma : F \to E$ is an isomorphism of fields, then it extends to (by an abuse of notaiton)*

$$\begin{array}{cccc} \sigma : & F[x] & \to & E[x] \\ & a_0 + a_1 x + \ldots + a_n x^n & \mapsto & \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^n \end{array}$$

Corollary 10.7. *Let $\sigma : F \to E$ be an isomorphism of fields. Let u be an algebraic in some extension of F with minimal polynomial $p(x)$ and v be an algebraic element in some externison of E with minimal polynomial $\sigma(p(x))$. Then σ extends to an isomorphism of fields $\overline{\sigma} : F(u) \to F(v)$ such that $\overline{\sigma}(u) = v$ and also for every $c \in F$, we have $\overline{\sigma}(c) = \sigma(c)$.*

Proof. Note that by the previous theorem

$$\begin{array}{cccc} \overline{\tau} : & E[x]/\langle \sigma(p(x)) \rangle & \to & E(v) \\ & f(x) + \langle \sigma(p(x)) \rangle & \mapsto & f(v) \end{array}$$

is an isomorphism. Also define the surjective homomorphism

$$\begin{array}{cccc} \pi : & E[x] & \to & E[x]/\langle \sigma(p(x)) \rangle \\ & f(x)\rangle & \mapsto & f(x) + \langle \sigma(p(x)) \rangle \end{array}$$

Now consider the following map,

$$\begin{array}{cccccccc} \psi : & F[x] & \overset{\sigma}{\to} & E[x] & \overset{\pi}{\to} & E[x]/\langle \sigma(p(x)) \rangle & \overset{\overline{\tau}}{\to} & E(v) \\ & f(x) & \mapsto & \sigma(f(x)) & \mapsto & \sigma(f(x)) + \langle \sigma(p(x)) \rangle & \mapsto & \sigma(f(v)) \end{array}$$

We use the first isomorphism theorem and we have $F[x]/ker\psi \cong E(v)$ since all maps are surjective. We claim that $ker\psi = \langle p(x) \rangle$. If $f(x) \in ker\psi$, then $\sigma(f(v)) = 0$. As $\overline{\tau}$ is an isomorphism, we must have $\sigma(f(x)) \in \langle \sigma(p(x)) \rangle$, which is equivalent to say that $f(x) \in \langle p(x) \rangle$. Moreover, $\psi(p(x)) = \sigma(p(v)) = 0$. Therefore, $ker\psi = \langle p(x) \rangle$.

Then

$$\begin{array}{rrcl} \overline{\psi}: & F[x]/\langle p(x) \rangle & \rightarrow & E(v) \\ & f(x) + \langle p(x) \rangle & \mapsto & f(v) \end{array}$$

is an isomorphism. Also by the previous theorem we have the following isomorphism

$$\begin{array}{rrcl} \overline{\phi}^{-1}: & F[u] & \rightarrow & F[x]/\langle p(x) \rangle \\ & f(u) & \mapsto & f(x) + \langle p(x) \rangle \end{array}$$

Now define

$$\begin{array}{rrcl} \overline{\sigma} = \overline{\psi} \circ \overline{\phi}^{-1}: & F[u] & \rightarrow & F[v] \\ & f(u) & \mapsto & f(v) \end{array}$$

is an isomorphism such that $\overline{\sigma}(u) = v$ and also $\overline{\sigma}(c) = \sigma(c)$ for all $c \in F$. $\square$

11 Algebraic Extensions

Definition. *An extension field K of a field F is said to be an algebraic extension of F if every element of K is algebraic over F.*

Example 11.1. *The complex number $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$. Note that for every element $a+ib \in \mathbb{C}$ we have $(x-(a+bi))(x-((a-bi))) = x^2 - 2ax + (a^2+b^2) \in mathbbR[x]$. Therefore, $a+ib$ is a root of a polynomial in $\mathbb{R}[x]$.*

Theorem 11.2. *If K is a finite-dimensional extension of F, then K is an algebraic extension of F.*

Proof. Let $[K : F] = n$ and $u \in K$. We have either for some $0 \leq i < j$, $u^i = u^j$ or all different powers of u are distinct. In the former case, we have u is a root of $x^i - x^j \in F[x]$, and in the latter case the set $\{1_F, u, u^2, \ldots, u^n\}$ is liearly dependent since the set contains $n+1$ element, therefore, there are scalars $c_0, \ldots, c_n \in F$ such that at least one of them is nonzero and $c_0 + c_1 u + \ldots + c_n u^n = 0$. It follows that $c_0 + c_1 x + \ldots + c_n x^n \in F[x]$ has u as a root. □

• The inverse of the above theroem is false since there is an algebraic extension over $\mathbb{Q}$ with infinite dimestion. See Exercise 16 of Section 11.3.

Example 11.3. *When u is an algebraic element over F, the field $F(u)$ is algebraic over F since by the previous theorem it is finite dimensional over F.*

Definition.

1. *Let $F(u_1, \ldots, u_t)$ be the intersection of all fields that contains all u_i and also F.*
2. *$F(u_1, \ldots, u_t)$ is said to be a* **finitely generated extension of F, generated by $u_1, \ldots, u_t$.**

Example 11.4.

1. *The field $\mathbb{Q}(\sqrt{3}, i)$ is the smallest subfield of $\mathbb{C}$ contains $\mathbb{Q}$ and both $\sqrt{3}$ and i.*
2. *The finitely generated $\mathbb{Q}(i, -i)$ is the same as $\mathbb{Q}(i)$ and so it is a simple extension.*
3. *A finite dimensional extension K of a field F is also finitely genetrated since if $u_1, u_2, \ldots, u_k$ is a basis for the extension K, then $K = (u_1, u_2, \ldots, u_k)$.*

Remark. *Let u, v be two elements in an extension of F, then $F(u, v) = F(u)(v)$.*

Proof. $F(u, v)$ contains $F(u)$ since $F(u)$ is a subfield of any field containing both F and u. Moreover, $F(u)(v)$ is the subfiled of any field containing $F(u)$ and v, and so is a subfield of $F(u, v)$. Thus, $F(u)(v) \subseteq F(u, v)$.

Also, since $F(u, v)$ is the smallest subfield of containing u, v and F, it is a subfield of $F(u)(v)$.

$$F \subseteq F(u) \subseteq F(u, v) = F(u)(v)$$

□

Example 11.5. *Find the dimestion of $\mathbb{Q}(\sqrt{3}, i)$ over $\mathbb{Q}$.*

Proof. Note that the monimal polynomial of $\sqrt{3}$ over Q is $x^2 - 3$, therefore, $\mathbb{Q}(\sqrt{3})$ has dimension 2 over $\mathbb{Q}$. Moreover, the minimal polynomial of i over $\mathbb{Q}$ is $x^2 + 1$. Thus, $[\mathbb{Q}(i) : \mathbb{Q}(\sqrt{3})] = 2$. Therefore,

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(sqrt3), \mathbb{Q}] = 4.$$

$\square$

Theorem 11.6. *Let $K = F(u_1, \ldots, u_n)$ is a finitely generated extension of F and each u_i is algebraic over F, then K is finite dimensional algebraic extension of F.*

Proof. Note that we have

$$F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq F(u_1, \ldots, u_n)$$

Thus

$$[F(u_1, \ldots, u_n) : F] = [F(u_1, \ldots, u_n) : F(u_1, \ldots, u_{n-1})]$$
$$[F(u_1, \ldots, u_{n-1}) : F(u_1, \ldots, u_{n-2})] \ldots [F(u_1, u_2) : F(u_1)][F(u_1) : F]$$

For each i, $[F(u_1, \ldots, u_{i-1}) : F(u_1, \ldots, u_i)]$ is the same as $[F(u_1, \ldots, u_{i-1})(u_i) : F(u_1, \ldots, u_{i-1})]$, and since u_i is algebraic over F, it is also algebraic over $F(u_1, \ldots, u_{i-1})$, therefore, by a theorem $[F(u_1, \ldots, u_{i-1}) : F(u_1, \ldots, u_i)]$ is finite and so $[F(u_1, \ldots, u_n) : F]$ is finite, and since any finite-dimensional extension is algebraic, we conclude that $K = F(u_1, \ldots, u_n)$ is finite dimensional algebraic extension of F. $\square$

Corollary 11.7. *If L is an algebraic extension of K and K is an algebraic extension of F, then L is an algebraic extension of F.*

Proof. Let u be an element of L, we should show that there is a polynomial in $F[x]$ that has u as a root. As L is an algebraic extension of K there is a polynomial $a_0 + a_1x + \ldots + a_nx^n$ such that $a_0 + a_1u + \ldots + a_nu^n = 0$. Note that u is algebraic over $F(a_0, \ldots, a_n)$. Also, note that $F(a_0, \ldots, a_n, u)$ is finite dimensional over F. Therefore, $F(a_0, \ldots, a_n, u)$ is an algebraic extension of F and so there is a polynomial in $F[x]$ that has u as a root. $\square$

Corollary 11.8. *Let K be an extension field of F and let E be the set of all elements of K that are algebraic over F. Then E is a subfield of K and an algebraic extension field of F.*

Proof. It is clear that if E is a field, it is an algebraic extension of F, so we only need to show that it is a subfield of K. If $u, v \in E$, then $F(u, v)$ is a subset of E since all elements of $F(u, v)$ are algebraic over F. Therefore, we have $u+v, -v, uv \in F(u, v) \subseteq E$, and moreover, $u^{-1} \in F(u, v)$ if u is not zero. Therefore, E is a field. $\square$

Definition. *The set of all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$ is called the field of algebraic numbers.*

12 Splitting Fields

Any polynomial of degree n over a field has at most n roots.

Definition. *We say that $f(x)$ split over the field K if $f(x)$ factors in $K[x]$ as*

$$f(x) = c(x - u_1) \dots (x - u_n).$$

Definition. *If F is a field and $f(x) \in F[x]$, then an extension field K of F is said to be* **splitting field** *(or* **root field***) of $f(x)$ over F provided that*

1. *$f(x)$ splits over K, say $f(x) = c(x - u_1) \dots (x - u_n)$.*

2. *$K = F(u_1, \dots, u_n)$.*

Example 12.1. *The splitting field of $x^2 + 1$ over $\mathbb{R}$ is $\mathbb{R}(i, -i) = \mathbb{R}(i) = \mathbb{C}$.*

Lemma 12.2. *Let $f(x) \in F[x]$ where F is a field. Then there is an extension field of F that contains a root of $f(x)$.*

Proof. As $F[x]$ is a UFD, then $f(x)$ factors into irreducible polynomials. So assume that $f(x) = cp(x)p_1(x) \dots p_k(x)$ where all $p_i(x)$ are irreducible and $p(x) = a_0 + a_1 x + \dots + x^n$ is a monic irreducible polynomial. So if we show that there is an extension of F that contains a root of $p(x)$, then it is also contains a root of $f(x)$. Note that $K = F[x]/\langle p(x) \rangle$ is an extension of F. Moreover, consider $x + \langle p(x) \rangle$. Then

$$p(x + \langle p(x) \rangle) = a_0 + a_1(x + \langle p(x) \rangle) + \dots + (x + \langle p(x) \rangle)^n = a_0 + a_1 x + \dots + a_n x^n =$$

$$p(x) + \langle p(x) \rangle) = 0_K.$$

□

Theorem 12.3. *Let F be a field and $f(x)$ a nonconstant polynomial of degree n in $F[x]$. Then there exists a splitting field K of $f(x)$ over F such that $[K : F] \leq n!$.*

Proof. We proceed the proof by induction on degree of $f(x)$. If degree of $f(x)$ is one then F is a splitting field for $f(x)$ and so $[F, F] = 1 \leq 1!$. Now assume that for every polynomial of degree $n - 1$ the theorem is true, i.e., any nonconctant polynomial over any field of degree $n - 1$ has a splitting field. By previous lemma there is an extension field K that contains a root, say u, of $f(x)$. Therefore, $f(x) = c(x - u)g(x)$ where $g(x) \in F(u)[x]$. By induction hypothesis, there is a splitting field K of $g(x)$ over $F(u)$ such that $[K : F(u)] \leq (n - 1)!$. We have also that K is splitting field of $f(x)$ over F, and $[K : F] = [K : F(u)][F(u) : F] \leq (n - 1)! deg(f(x)) \leq n!$. □

Any two splitting field of a polynomial in $F[x]$ are isomorphic.

Theorem 12.4. *Let $\sigma : F \to E$ be an isomorphism of fields. Assume that $f(x) \in F[x]$ is nonconstant. Let*

$$\begin{array}{rccc} \sigma : & F[x] & \to & E[x] \\ & f(x) & \mapsto & \sigma(f(x)) \end{array}$$

- *K a splitting field of $f(x)$ over F*

- *L a splitting field of $\sigma(f(x))$*

Then σ extends to an isomorphism between K and L.

Proof. We proceed the proof by induction on $deg(f(x))$. If $deg(f(x)) = 1$, then $f(x) = c(x-b)$ where c and b are elements of F. Therefore, the splitting field of $f(x)$ is itself. Also $\sigma(c(x-b) = \sigma(c)x + \sigma(cb) = \sigma(c)(x - \sigma(b))$, since $\sigma(c), \sigma(b) \in E$, we have that splitting field of $\sigma(f(x))$ is E, and we already have that $F \cong E$.

Assume that the theorem is true for any polynomial of degree $n-1$ and $deg(f(x)) = n$. Assume that $u \in K$ is a root of $f(x)$ and $p(x)$ is the minimal polynomial of u. Consider that $f(x) \in F(u)[x]$. Use division algorithm to divide $f(x)$ by $x-u$ in $F(u)[x]$. Then we have $f(x) = (x-u)g(x)$ for some $g(x) \in F(u)[x]$.

Consider that $\sigma(p(x))$ is a monic irreducible polynomial. Let v ve a root of $\sigma(P(x))$. So $\sigma(P(x))$ is the minimal polynomial of v. By a theorem we have the isomorphism $\sigma : F \to E$ extends to an isomorphism from $F(u)$ to $E(v)$. Now we have

$$\begin{array}{ccc} K & & L \\ \cup\!\!| & & \cup\!\!| \\ F(u) & \overset{\cong}{\to} & E(v) \\ \cup\!\!| & & \cup\!\!| \\ F & \overset{\sigma}{\to} & E \end{array}$$

If $f(x) = (x-u)(x-u_1)\ldots(x-u_k)$ then $g(x) = (x-u_1)\ldots(x-u_k)$. Note that $g(x) \in F(u)[x]$ has splitting field K, moreover,

$$\sigma(f(x)) = \sigma((x-u)g(x)) = (x-\sigma(u))\sigma(g(x)) = (x-v)\sigma(g(x)).$$

So the splitting field of $\sigma(g(x)) \in E(v)$ is also L. Therefore, by induction hypothesis the isomorphism between $F(u)$ and $E(v)$ extends to an isomorphism between K and L.

□

Definition. *An algebraic extension field K of F is* **normal** *provided that whenever an irreducible polynomial in $F[x]$ has one root in K, then it splits over K.*

Theorem 12.5. *The field K is a splitting field over the field F of some polynomial in $F[x]$ if and only if K is finite dimensional, normal extension of F.*

Proof. As K is a splitting filed of some polynomial $f(x) \in F[x]$, we have $K = F(u_1, \ldots, u_n)$ where u_i are roots of $f(x)$. Since each u_i is algebraic over F, we have from a theorem that K is finite dimensional extension of F.

Now we show that K is normal extension of F. Let $p(x)$ be an irreducible polynomial in $F[x]$ with a root u in K. We want to show that if w is a root of $p(x)$ other than u, then $w \in K$. Consider the field extension $F(w)$. Since w and u has the same minimal polynomial we have that $F(u) \cong F(w)$. So we have

$$\begin{array}{ccc} K & & K(w) \\ \cup\!\!| & & \cup\!\!| \\ F(u) & \cong & F(w) \\ \cup\!\!| & & \cup\!\!| \\ F & = & F \end{array}$$

Since K is splitting field of $f(x) \in F(u)[x]$ and also $K(w)$ is also a splitting field of $f(x) \in F(w)[x]$ and moreover $F(u) \cong F(w)$, by the last theorem we have $K \cong K(w)$, in such a way that this isomorphism takes u to w and any element of F maps to itself. By a theorem in linear algebra (Let K and L be finite dimensional extension fields of F and let $f : K \to L$ be an isomorphism such that $f(c) = c$ for every $c \in F$. Then $[K : F] = [L : F]$.) we have $[K : F] = [K(w) : F]$, so K is a subspace of $K(w)$ with the same dimension, and so $K(w) = K$. Therefore, $w \in K$.

Conversely, assume that K is a finite-dimensional normal extension of F, we want to show that there is a polynomial $f(x)$ such that K is its splitting field. Since K is finite dimensional, then K has a basis $\{u_1, \ldots, u_k\}$ over F, so we can write $K = F(u_1, \ldots, u_k)$. Note that by the theorem [If K is a finite-dimensional extension field of F, then K is an algebraic extension of F], each u_i has a minimal polynomial over F, say $p_i(x)$. Since $p_i(x)$ has one root, u_i, in K and K is normal we conclude that all roots of $p_i(x)$ are in K. Therefore, K is the splitting field of $f(x)$, a polynomial over F.

$\square$

Example 12.6. *Fact:* $z = 2^{2/3}(\frac{-1+\sqrt{3}i}{2})$ *is a root of* $x^3 - 2$ *in* $\mathbb{C}$.
Use the above fact to show that $\mathbb{Q}(\sqrt[3]{2})$ *is not a normal extension of* $\mathbb{Q}$.
Answer: Note that if $\mathbb{Q}(\sqrt[3]{2})$ *is a normal extension of* $\mathbb{Q}$, *then if it has one root of some polynomial of* $\mathbb{Q}[x]$, *it must contains all of other roots of the polynomial. But* $x^3 - 2$ *is in* $\mathbb{Q}[x]$ *with a root* z *which is not in* $\mathbb{Q}(\sqrt[3]{2})$

Definition. 1. *A field over which every non-constant polynomial splits is said to be* **algebraically closed**. *For example,* $\mathbb{C}$ *is algebraically closed.*

2. *If* K *is an algebraic extension of* F *and* K *is algebraically closed, then* K *is said to be* **algebraic closure** *of* F.

13 Separability

Definition. 1. *Let F be a field. A polynomial $f(x) \in F[x]$ of degree n is said to be* **separable** *if it has n distinct roots in some splitting field. Equivalently, $f(x)$ is* **separable** *if it has no repeated roots in any splitting field.*

2. *If K is an extension field of F, then an element $u \in K$ is said to be* **separable** *over F if u is algebraic over F and its minimal polynomial $p(x) \in F[x]$ is separable.*

3. *The extension field K is said to be a* **separable extension** *if every element of K is separable over F.*

Derivative of polynomial: The **derivative** of $f(x) = c_0+c_1x+c_2x^2+\ldots+c_nx^n \in F[x]$ is defined to be the polynomial

$$f^{'}(x) = c_1 + 2c_2x + \ldots + nc_nx^{n-1}. \in F[x].$$

If you check we have

$$(f+g)^{'}(x) = f^{'}(x) + g^{'}(x) \quad (fg)^{'}(x) = f(x)g^{'}(x) + f^{'}(x)g(x).$$

Lemma 13.1. *Let F be a field and $f(x) \in F[x]$. If $f(x)$ and $f^{'}(x)$ are relatively prime in $F[x]$, then $f(x)$ is separable.*

Proof. Two polynomials are relatively prime if the only factor of both of them is 1. Assume on the contrary that $f(x)$ is not separable, so in the splitting field of $f(x)$ we must have $f(x) = (x-u)^2g(x)$. So, $f^{'}(x) = 2(x-u)g(x) + (x-u)^2g^{'}(x)$. Therefore, we can see that $(x-u)$ divides both $f(x)$ and $f^{'}(x)$, and so they are not relatively prime. □

Definition. *Let F be a field. Then F has* **characteristic** *0 if $n1_F \neq 0_F$ for every positive integer n, and also F has characteristic k if k is the smallest integer such that $k.1 = 0$.*

Proposition 13.2. *If F is a filed then either it has characteristic 0 or p where p is a prime number.*

Proof. Let F be a filed with nonzero characteristic. Let $n.1 = 0$ where n is the smallest positive integer with this property. If n is not a prime then we can write $n = mk$, so $mk1 = 0$, which means $(m.1)(k.1) = 0$, and so $m.1 = 0$ or $k.1 = 0$ which is a contradiction since m and k are smaller than m. □

Theorem 13.3. *Let F be a field of characteristic* 0*. Then every irreducible polynomial in $F[x]$ is separable, and every algebraic extension of F is a separable extension.*

Proof. Let $p(x)$ be an irreducible polynomial in $F[x]$. So $p(x)$ is nonconstant and it is of the form

$$p(x) = cx^n + \textit{ lower terms}$$

and also $p^{'}(x) = (nc)x^{n-1} +$ lower terms. Therefore, $p^{'}(x)$ has a smaller degree than $p(x)$ so they are relatively prime and so $p(x)$ is separable. In particular, the minimal polynomial of each $u \in K$ is separable and so K is a separable extension. □

Lemma 13.4. *Let $K = F(v, w)$ be a separable extension of F and F is an infinite field, then there is $u \in K$ such that $F(u) = K$.*

Proof. Let $p(x)$ be the minimal polynomial of v over F and $q(x)$ be the minimal polynomial of w over F. Let L be the splitting field of the polynomial $p(x)q(x)$. Let $v, v_1, \ldots, v_n$ be the roots of $p(x)$ and $w, w_1, \ldots, w_m$ be the roots of $q(x)$. Since $F(u, v)$ is a separable extension of F and $w \in F(u, v)$, so the minimal polynomial of $q(x)$ is separable and so all $w, w_1, \ldots, w_m$ are distinct.. As F is infinite, there is an element $c \in F$ such that

$$c \neq 0 \text{ and } c \neq \frac{v_i - v}{w - w_j} \; 1 \leq i \leq n, 1 \leq j \leq m.$$

Let $u = v + cw$ ($v = u - cw$). We claim that $F(u) = K$. Define $h(x) = p(u - cx) \in F(u)[x]$. Note that $h(w) = p(u - cw) = p(v) = 0$. So w is a root of $h(x)$. We show that the only common root of $h(x)$ and $q(x)$ is w. Assume otherwise, then for some w_j we have $p(u - cw_j) = 0$, and so $u - cw_j = v_i$. Therefore, $v + cw = u = v_i + cw_j$ which means

$$c = \frac{v_i - v}{w - w_j}.$$

A contradiction, thus we must have $h(x) \in F(u)[x]$ and $q(x) \in F(u)[x]$ has one root w in common.

Let $r(x)$ be the minimal polynomial of w over $F(u)$. Then $r(x)|h(x)$ and $r(x)|q(x)$, and so it must be of degree 1 because otherwise, $h(x)$ and $q(x)$ have more than one common roots. So $r(x) = a(x - w)$ such that $a \in F(u)$ and $w \in F(u)$. Since $w \in F(u)$ and $u = v - cw$ we have that $v \in F(u)$. And so $F(v, w) = F(u)$. □

Theorem 13.5. *If K is a finitely generated separable extension field of F, then $K = F(u)$ for some $u \in K$.*

Proof. As K is finitely generated we have $K = F(u_1, \ldots, u_n)$ for some $u_i \in K$. We proceed by induction on n. If $n = 1$, so nothing to prove. Assume $n \geq 2$ and the theorem is true for $n - 1$. So $F(u_1, \ldots, u_n) = F(u_1, \ldots, u_{n-1})u_n)$. By induction hypothesis we have there is some $v \in F(u_1, \ldots, u_{n-1})$ such that $F(u_1, \ldots, u_{n-1}) = F(v)$. Therefore, $F(u_1, \ldots, u_n) = F(u_1, \ldots, u_{n-1})u_n) = F(v, u_n)$, and so by previous lemma, there is an element u such that $F(v, u_n) = F(u)$. □

14 Finite Fields

Let R be a ring with identity. We say R has characteristic 0 if there is not a positive integer m such that $m.1 = 0$ and we say it has characteristic n if n is the smallest positive integer such that $n.1 = 0$.

Theorem 14.1. *If R is an integral domain the characteristic of R is either infinity or a prime number.*

Lemma 14.2. *Let R be a ring with identity of characteristic $n > 0$. Then $k.1 = 0$ if and only if $n|k$.*

Proof. We can write $k = mn + r$, we have $0 = k.1 = (mn + r)1 = mn1 + r1 = 0 + r1$, so if r is not zero, then $r1 = 0$ and $r < n$ a contradiction. Therefore, we must have $r = 0$ and $n|k$. $\square$

Theorem 14.3. *Let R be a ring with identity. Then*

1. *The set $P = \{k1_R | k \in \mathbb{Z}\}$ is a subring of R.*
2. *If R has characteristic 0, then $P \cong \mathbb{Z}$.*
3. *If R has characteristic $n > 0$, $P \cong \mathbb{Z}_n$.*

Proof. It is easy to check that P is closed under subtraction and also multiplication. Therefore, it is a subring. To prove (2) and (3), define $f : \mathbb{Z} \to P$ given by $f(k) = k.1$. It is clear that f is a surjective homomorphism. If char(R) = 0, then the kernel of f is trivial and so $\mathbb{Z} \cong P$, if char(R) $= n$, then kernel of f is equal to $\{k.1 = 0 : k \in \mathbb{Z}\}$. Since if any element k with $k.1 = 0$ divides n, we have $ker f = n\mathbb{Z}$ and so be first isomorphism theorem $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong P$. $\square$

Corollary 14.4. *Every field of characteristic p has $\mathbb{Z}_p$ as a subfield.*

Theorem 14.5. *Every finite field K has order p^n, where p is the characteristic of K and $[K : \mathbb{Z}_p] = n$.*

Proof. Any finite field has characteristic > 0, therefore, it contains $\mathbb{Z}_p$ by previous theorem. So it is a vector space over $\mathbb{Z}_p$. By linear algebra, when K is finite, we have the dimension of a vector space K over $\mathbb{Z}_p$ is $|K|/|\mathbb{Z}_p| = n$. $\square$

Theorem 14.6. *(Freshman's Dream) Let p be a prime and R be a commutative ring with identity of characteristic p. Then for every $a, b \in R$ and every positive integer n,*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Proof. We proceed the theorem by induction on n. If $n = 1$, then by the Binomial Theorem,

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{r} a^{p-r}b^r + \cdots + \binom{p}{p-1} ab^{p-1} + b^p.$$

The prime p divides each of the coefficients $\binom{p}{r}$, so the term $\binom{p}{r}a^{p-r}b^r = 0$. Therefore, $(a + b)^p = a^p + b^p$. Assume that the theorem is true for $n = k$. Now by induction hypothesis and first step we have

$$(a + b)^{p^{n+1}} = (a + b)^{p^n p} = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

$\square$

Theorem 14.7. *Let K be an extension field of $\mathbb{Z}_p$ and n a positive integer. Then K has order p^n if and only if K is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.*

Proof. $\Leftarrow$) As K is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$, it contains all of its roots. We show that $x^{p^n} - x$ has p^n distinct roots, and the set all of these distinct roots is precisely K.

Let E be the subset of K containing all of the roots of $x^{p^n} - x$. Note that if $f(x) = x^{p^n} - x$, then $f'(x) = p^n x^{p^n - 1} - 1 = -1$. Therefore, $f(x)$ and $f'(x)$ are relatively prime. And so $x^{p^n} - x$ is separable. So E has p^n distinct elements. If we show that E is a field, then since E also spitting field of $x^{p^n} - x$ we conclude that $K = E$, and so it has p^n elements.

Let $a, b \in E$ and $a \neq 0$. Then

$$(a - b)^{p^n} - (a - b) = (a + (-b))^{p^n} - (a + (-b)).$$

By Freshman's dream

$$(a + (-b))^{p^n} - (a + (-b)) = a^{p^n} + (-b)^{p^n} - (a + (-b)) = (a + (-b)) - (a + (-b)) = 0.$$

So $a - b \in E$. Moreover,

$$(ba^{-1})^{p^n} - ba^{-1} = b^{p^n}(a^{-1})^{p^n}) - ba^{-1}.$$

Since $a, b \in E$, we have $a^{p^n} - a = 0$ and so $a^{p^n} = a$ and similarly, $b^{p^n} = b$. Therefore,

$$b^{p^n}(a^{-1})^{p^n}) - ba^{-1} = ba^{-1} - ba^{-1} = 0,$$

so $ba^{-1} \in E$. We can now say that E is a field.

Assume that K is a field of order p^n. It is enough to show that every element $c \in K = \{0, c_1, \ldots, c_{p^n-1}\}$ is a root of $x^{p^n} - x$. If c is zero, then it is a root of $x^{p^n} - x$. If $c \neq 0$, then $cc_1, \ldots, cc_{p^n-1}$ are also the list of all nonzero elements of K. Therefore, $u = cc_1, \cdots, cc_{p^n-1} = c_1 \ldots c_{p^n-1}$. Also

$$u = cc_1, \cdots, cc_{p^n-1} = c^{p^{n-1}} c_1 \ldots c_n = c^{p^n-1} u.$$

Therefore, $c^{p^n-1} = 1$ which means that $c^{p^n} = c \Rightarrow c^{p^n-1} - c = 0$, i.e., c is a root of $x^{p^n} - x$. $\square$

Corollary 14.8. *For each positive prime p and positive integer n, there exists a field of order p.*

Proof. We previously showed that the splitting field of any polynomial exists, and so the splitting field of $x^{p^n} - x$ exists and by previous theorem has order p^n. $\square$

Corollary 14.9. *Two finite fields of the same order are isomorphic.*

Proof. Let K and L be two field of order p^n. Then they are splitting field of $x^{p^n} - x$, and by Theorem 12.4, they are isomorphic. $\square$

So there is a unique field, up to isomorphism, of order p^n, and we call it **Galois field of order p^n**.

Theorem 14.10. *Let K be a finite field and F a subfield. Then K is a simple extension of F.*

Proof. Note that $K \setminus \{0\}$ is a multiplicative group, and by a theorem the multiplicative group of any field is cyclic. So, there is an element $u \in K$ such that $K = \{1, u, \ldots, u^{p^n-1}\}$. Therefore, $K = F(u)$. $\square$

Corollary 14.11. *Let p be a positive prime. For each positive integer n, there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.*

Proof. There is a field K of order p^n, and also K has a copy of $\mathbb{Z}_p$. By the previous theorem there is an element $u \in K$ such that $K = \mathbb{Z}_p(u)$ so the minimal polynomial of u has degree n. $\square$

15 The Galois Group

Definition. *Let K be an extension of F. An F-***automorphism** *σ of K is an isomorphism $\sigma : K \to K$ such that for every $c \in F$, $\sigma(c) = c$. The set of all F-automorphism is denoted by $Gal_F K$ and is called the Galois group of K over F.*

Theorem 15.1. *If K is an extension field of F, then $Gal_F K$ is a group under the operation of composition of functions.*

Proof. If $\sigma, \tau \in Gal_F K$, then $\sigma \circ \tau$ is an isomorphism and also $\sigma \circ \tau(c) = \sigma(\tau(c)) = \sigma(c) = c$. Therefore, $\sigma \circ \tau \in Gal_F K$. Moreover,

1. Identity map is in $Gal_F K$.
2. If $\sigma \in Gal_F K$, then σ^{-1} is an isomorphism such that $\sigma^{-1}(c) = c$ because σ is one-to-one and $\sigma(c) = c$.
3. Compositions of functions is associative.

Therefore, $Gal_F K$ is a group. □

Theorem 15.2. *Let K be an extension field of F and $f(x) \in F[x]$. If $u \in K$ is a root of $f(x)$ and $\sigma \in Gal_F K$, then $\sigma(u)$ is also a root of $f(x)$.*

Proof. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$. Assume that $u \in K$ is a root of f. Then

$$f(\sigma(u)) = a_0 + a_1\sigma(u) + a_2\sigma(u)^2 + \ldots + a_n\sigma(u)^n.$$

Note that for every i, $\sigma(u)^i = \sigma(u)\ldots\sigma(u) = \sigma(u^n)$. Therefore,

$$f(\sigma(u)) = a_0 + a_1\sigma(u) + a_2\sigma(u^2) + \ldots + a_n\sigma(u^n) =$$

$$\sigma(a_0)+\sigma(a_1)\sigma(u)+\sigma(a_2)\sigma(u^2)+\ldots+\sigma(a_n)\sigma(u^n) = \sigma(a_0+a_1u+a_2u^2+\ldots+a_nu^n) = \sigma(0) = 0.$$

□

Remark. *Let $p(x)$ be an irreducible polynomial in $F[x]$ and K be the splitting field of $p(x)$. The above theorem is stating that if u is a root the image of u by any element of $Gal_F K$ also is a root of f. The converse is true by the following theorem, i.e., the set of all roots of $p(x)$ is $\{\sigma(u) : \sigma \in Gal_F K\}$ for any root u of $p(x)$.*

Theorem 15.3. *Let K be the splitting field of some polynomial over F and $u, v \in K$. Then there exists $\sigma \in Gal_F K$ such that $\sigma(u) = v$ if and only if u and v have the same minimal polynomial in $F[x]$.*

Proof. $\Leftarrow$) Let u and v have the same minimal polynomial $p(x)$, we previously had there is an isomorphism $\sigma : F(u) \to F(v)$ such that $\sigma_1(u) = v$ and σ_1 is fixed over F. Consider that K is splitting field of some polynomial in $F(u)[x]$ and $F(v)[x]$. Now, by Theorem 12.4, σ_1 extends to an isomorphism σ of K which is the same as σ_1 on $F(u)$, i.e., $\sigma(u) = \sigma_1(u) = v$. Therefore, $\sigma \in Gal_F K$ and $\sigma(u) = v$.

Converse is merely a result of previous theorem. □

Example 15.4. *Show that $Gal_{\mathbb{R}}\mathbb{C}$ is isomorphic to $\mathbb{Z}_2$.*

Proof. Note that x^2+1 is an irreducible polynomial in $\mathbb{R}[x]$ with roots i and $-i$. For every $\tau \in Gal_{\mathbb{R}}\mathbb{C}$, therefore, we have either $\tau(i)=i$ or $\tau(i)=-i$. Therefore,

$$\tau(a+ib)=\tau(a)+\tau(i)\tau(b)=a+\tau(i)b.$$

Which means τ only can be one of the following automorphisms

$$\tau(a+ib)=a+ib \qquad\qquad \tau(a+ib)=a-ib.$$

$\square$

Remark. *The example above shows that any $\mathbb{R}$-automorphism of $\mathbb{C}=\mathbb{R}(i)$ is determined by its action on i. This argument is true in general by the following theorem.*

Theorem 15.5. *Let $K=F(u_1,\dots,u_n)$ be an algebraic extension field of F. If $\sigma,\tau \in Gal_FK$ and $\sigma(u_i)=\tau(u_i)$ for each $i=1,2,\dots,n$, then $\sigma=\tau$.*

Proof. To show that $\sigma=\tau$, it is enough to show that $\tau^{-1}\circ\sigma=id$. We show this by induction on n. Let $n=1$. Then $K=F(u_1)$, and any element w in K is of the form $w=c_0+c_1u_1+\ldots+c_ku_1^k$, where each c_i is in F. Now $\tau^{-1}\circ\sigma(w)=\tau^{-1}\circ\sigma(c_0+c_1u_1+\ldots+c_ku_1^k)=c_0+c_1\tau^{-1}\circ\sigma(u_1)+\ldots+c_k(\tau^{-1}\circ\sigma(u_1))^k=c_0+c_1u_1+\ldots+c_ku_1^k=w$.

Now assume that for any element in $F(u_1,\dots,u_{n-1})$, we have $\tau^{-1}\circ\sigma=id$.

Now consider that $K=F(u_1,\dots,u_n)=F(u_1,\dots,u_{n-1})(u_n)$ so any element of K is of the form $w=a_0+a_1u_n+\ldots+a_ku_n$, and so $\tau^{-1}\circ\sigma(w)=\tau^{-1}\circ\sigma(a_0+a_1u_n+\ldots+a_ku_n^k)$. By induction hypothesis we have

$$\begin{aligned}\tau^{-1}\circ\sigma(a_0+a_1u_n+\ldots+a_ku_n^k)&=a_0+a_1\tau^{-1}\circ\sigma(u_n)+\ldots+(\tau^{-1}\circ\sigma(u_n))^k\\&=a_0+a_1u_n+\ldots+a_ku_n^k=w.\end{aligned}$$

$\square$

Example 15.6. *By Using the above Theorem we want to find $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{3},\sqrt{5})$.*

Note that x^2-3 and x^2-5 are the minimal polynomial of $\sqrt{3}$ and $\sqrt{5}$ over $\mathbb{Q}$, respectively. By Theorem 15.3, for any $\sigma\in Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{3},\sqrt{5})$, $\sigma(\sqrt{3})$ and $\sigma\sqrt{5}$ are roots of x^2-3 and x^2-5. Therefore, we have the following possibles situations if $\sigma\in Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{3},\sqrt{5})$.

$$\begin{cases}\sigma(\sqrt{3})=\sqrt{3}\\ \sigma(-\sqrt{3})=-\sqrt{3}\\ \sigma(\sqrt{5})=\sqrt{5}\\ \sigma(-\sqrt{5})=-\sqrt{5}\end{cases}\quad \begin{cases}\sigma(\sqrt{3})=-\sqrt{3}\\ \sigma(-\sqrt{3})=\sqrt{3}\\ \sigma(\sqrt{5})=\sqrt{5}\\ \sigma(-\sqrt{5})=-\sqrt{5}\end{cases}\quad \begin{cases}\sigma(\sqrt{3})=\sqrt{3}\\ \sigma(-\sqrt{3})=-\sqrt{3}\\ \sigma(\sqrt{5})=-\sqrt{5}\\ \sigma(-\sqrt{5})=\sqrt{5}\end{cases}\quad \begin{cases}\sigma(\sqrt{3})=-\sqrt{3}\\ \sigma(-\sqrt{3})=\sqrt{3}\\ \sigma(\sqrt{5})=-\sqrt{5}\\ \sigma(-\sqrt{5})=\sqrt{5}\end{cases}$$

Now if we show that each of this situations yields an isomorphism from $\mathbb{Q}(\sqrt{3},\sqrt{5})$ to $\mathbb{Q}(\sqrt{3},\sqrt{5})$, and also the order of each one is at most 2, then $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{3},\sqrt{5})\cong\mathbb{Z}_2\times\mathbb{Z}_2$. For instance we only show that the last one is in $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{3},\sqrt{5})$. Let $\iota:\mathbb{Q}\to\mathbb{Q}$ be identity map. Then since $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(-\sqrt{3})$ are the splitting fields of x^2-3 over $\mathbb{Q}$, so ι can be extend to an isomorphism σ_1 form $\mathbb{Q}(\sqrt{3})$ to $\mathbb{Q}(-\sqrt{3})$ such that $\sigma_1(\sqrt{3})=-\sqrt{3}$, and so $\sigma_1(-\sqrt{3})=\sqrt{3}$. Similarly, since $\mathbb{Q}(\sqrt{3})(\sqrt{5})$ and $\mathbb{Q}(\sqrt{3})(\sqrt{5})$ are the splitting fields of x^2-5 over $\mathbb{Q}(\sqrt{3})$, so σ_1 extends to an isomorphism σ from $\mathbb{Q}(\sqrt{3})(\sqrt{5})$ to $\mathbb{Q}(\sqrt{3})(\sqrt{5})$ such that

$$\begin{cases}\sigma(\sqrt{3})=-\sqrt{3}\\ \sigma(-\sqrt{3})=\sqrt{3}\\ \sigma(\sqrt{5})=-\sqrt{5}\\ \sigma(-\sqrt{5})=\sqrt{5}\end{cases}$$

Also it is easy to check that $\sigma^2 = id$. Similarly we can show others also are isomorphisms, and it is easy to check the order of each one is at most 2.

Definition. *A field E such that $F \subseteq E \subseteq K$ is called an intermediate field of the extension. Note that $Gal_E K \subseteq Gal_F K$.*

Theorem 15.7. *Let K be an extension field of F. Let H be a subgroup of $Gal_F K$, and let*

$$E_H = \{k \in K : \sigma(k) = k \text{ for every } \sigma \in H\}.$$

Then E_H is an intermediate field of the extension.

Proof. It is enough to show that for every elements $a, b \in E_H$, $b \neq 0$, $ab^{-1} \in E_H$ and also $a - b \in E_H$. If we want to show that $ab^{-1} \in E_H$ we must show that $\sigma(ab^{-1}) = ab^{-1}$. Note that for every $\sigma \in H$,

$$\sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1}$$

and

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

□

Definition. *The field E_H is called the fixed field of the subgroup H.*

Example 15.8. *Consider $Gal_{\mathbb{R}}\mathbb{C}$ and let $H = Gal_{\mathbb{R}}\mathbb{C}$, find E_H.*

Proof. Remember, $E_H = \{k \in \mathbb{C} : \sigma(k) = k$ for every $\sigma \in H\}$. We previously showed that $Gal_{\mathbb{R}}\mathbb{C} = \{id, \tau\}$. Note that id fixes all elements, and τ only fixes the real part of each complex number, therefore, $E_H = \mathbb{R}$. □

Example 15.9. *Consider $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$ and let $H = Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$, find E_H.*

Proof. Let $\sigma \in H$, then note that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Note that $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ and the roots of this polynomial are $\sqrt[3]{2}$, $\sqrt[3]{2}w$, $\sqrt[3]{2}w^2$ where $w = (-1 + \sqrt{3}i)/2$. Note that the only real root of $x^3 - 2$ is $\sqrt[3]{2}$. Also, $\mathbb{Q}(\sqrt[3]{2})$ is only contains real numbers, so since any $\sigma \in H$ has an image in real numbers, and $\sigma(\sqrt[3]{2})$ is also a root of $x^3 - 2$, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Therefore, $E_H = \mathbb{Q}(\sqrt[3]{2})$. □

16 The Fundamental Theorem of Galois Theory

Throughout this section let K be a finite dimensional extension field of F. Let

$$S = \{E : F \subseteq E \subseteq K\} \qquad T = \{H : H \subseteq Gal_F K\}.$$

The main goal of this section is to show that for Galois extension K of F,

$$\begin{array}{rccc} \varphi: & S & \to & T \\ & E & \mapsto & Gal_E K \end{array}$$

is a bijection. Note that $\varphi(F) = Gal_F K$ and $\varphi(K) = Gal_K K = id$.

Lemma 16.1. *Let K be a finite dimensional extension field of F. If $H \subseteq Gal_F K$, then K is a simple, normal, separable extension of E_H (fix field of H), for simplicity we denote E_H by E.*

Proof. We had a theorem that ant finite dimensional extension field is algebraic so K is algebraic extension of F, and since $F \subseteq E$, K is algebraic extension of E too.

We now want to show that K is a separable extension of E. Let $u \in K$ and $p(x) \in E[x]$ be the minimal polynomial of u. Then consider that $\{\sigma(u) : \sigma \in H\}$ is a root of $p(x)$, and therefore, this set if a finite set, so let

$$\{\sigma(u) : \sigma \in H\} = \{u_1, u_2, \ldots, u_t\}.$$

Also for every $\sigma \in H$, $\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_t)$ are distinct roots of $p(x)$ because σ is one-to-one. Therefore,

$$\{u_1, u_2, \ldots, u_t\} = \{\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_t)\}.$$

Every $\sigma \in Gal_F K$ extends to an isomorphism from $K[x]$ to $K[x]$ which by abuse of notation was dented by σ.

Now, let

$$f(x) = (x - u_1)(x - u_2) \ldots (x - u_t).$$

We show that $f(x) \in E[x]$. Note that for every $\sigma \in H$, we have

$$f(x) = (x - u_1)(x - u_2) \ldots (x - u_t) = (x - \sigma(u_1))(x - \sigma(u_2)) \ldots (x - \sigma(u_t)) = \sigma(f(x)).$$

Consider that we can write $f(x) = a_0 + a_1 x + \ldots + a_t x^t \in K[x]$. Since for every $\sigma \in H$, $\sigma(f(x)) = f(x)$, we have that for each $\sigma \in H$ and a_i, $\sigma(a_i) = a_i$. Therefore, all $a_i \in E$, and so $f(x) \in E$. So we showed that for any arbitrary element $u \in K$, it is a root of a separable polynomial over E, so K is a separable extension of E. Moreover, any finitely generated separable extension is simple so $K = E(u)$ for some $u \in K$ (see theorem 13.5).

Also since K is splitting field of $f(x) \in E[x]$, then as a result of Theorem 12.5, K is a normal extension of E. □

Theorem 16.2. *Let K be a finite dimensional extension field of F. If $H \subseteq Gal_F K$, then $H = Gal_{E_H} K$ and $[K : E] = |H|$.*

Proof. We first show that $H \subseteq Gal_{E_H} K$. Let $\sigma \in H$, then by the definition of the fixed field E_H, for every $k \in E_H$, $\sigma(k) = k$, therefore, $\sigma \in Gal_{E_H} K$. We can say that $H \subseteq Gal_{E_H} K$.

Now, since $Gal_{E_H} K$ is finite, if we show that $|H| \geq |Gal_{E_H} K|$, then $H = Gal_{E_H} K$. By the previous theorem we have that $K = E_H(u)$ for some $u \in K$. Let $p(x)$ be the minimal polynomial of u over $E_H(x)$. Let

$$f(x) = (x - u)(x - u_1) \ldots (x - u_t),$$

where $\{\sigma(u) : \sigma \in H\} = \{u, u_1, \ldots, u_t\}$. If we show that

$$|H| \geq deg(f(x)) \geq \overset{[K:E_H]=}{deg(p(x))} \geq |Gal_{E_H} K| \geq |H|$$

then $H = Gal_{E_H} K$ and $[K : E_H] = |H|$.

For the first inequality, it is clear that $|H| \geq |\{\sigma(u) : \sigma \in H\}| = |\{u, u_1, \ldots, u_t\}| = deg(f(x))$.

For the second inequality, same as the previous theorem $f(x) \in E_H[x]$, and moreover, it has u as a root, so $p(x)|f(x)$, and it follows that $deg(f(x)) \geq deg(p(x)) = [K : E_H]$.

For the third inequality, note that $p(x)$ is separable, and also for every $\sigma \in Gal_{E_H}K$, $\sigma(u)$ is a root of $p(x)$. Note that $\{\sigma(u) : \sigma \in Gal_{E_H}K\}$ contains exactly $|Gal_{E_H}K|$ elements, because if $\sigma_1(u) = \sigma_2(u)$, then for every element in $K = E_H(u)$, $\sigma_1 = \sigma_2$. Therefore,

$$deg(p(x)) \geq |Gal_{E_H}K|.$$

$\square$

Example 16.3. *Previously we showed that $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}) = \langle \iota \rangle$. Here we have two intermediate fields $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2})$, but $\varphi(\mathbb{Q}) = \langle \iota \rangle = \varphi(\mathbb{Q}(\sqrt[3]{2}))$. In this case, φ is not injective, so we need more condition on K as an extension of F.*

16.1 Galois Extensions

Definition. *If K be a finite-dimensional, normal, separable (FDNS) extension field of the field F, we say that K is* **Galois extension** *of F, or that K is* **Galois over** *F*

Theorem 16.4. *Let K be a Galois extension of F and E an intermediate field. Then E is the fixed field of the subgroup $Gal_E K$, i.e., $E_{Gal_E K} = E$.*

Proof. Note that $E_{Gal_E K} = \{k \in K : \sigma(k) = k, \forall \sigma \in Gal_E K\}$, therefore, since for every $k \in E$ and $\sigma \in Gal_E K$, $\sigma(k) = k$, we must have $E \subseteq E_{Gal_E K}$. So we only need to show that $E_{Gal_E K} \subseteq E$. We proceed the proof by contradiction. Assume that there is $u \in E_{Gal_E K} \setminus E$. Since K is a separable extension of F, there is an irreducible separable polynomial $p(x) \in F(x)$ which has u as a root. Moreover, let $q(x)$ be the minimal polynomial of u over $E[x]$. Note that $q(x)|p(x)$ and since $p(x) \in F[x]$ is separable, we have that $q(x)$ is separable. Moreover, K is normal extension of F and so all of the roots of $p(x)$ and so $q(x)$ are in K. Since K is finite dimensional over E, it is splitting field of some polynomial over E. So by Theorem 15.3, $\{\sigma(u) : \sigma \in Gal_E K\}$ is the set of all roots of $q(x)$. Note that $q(x)$ has degree more than one since a root of it, i.e., u is not in E. Assume that v is another root of $p(x)$, then there is a $\sigma \in Gal_E K$ such that $\sigma(u) = v$, which means that $u \notin E_{Gal_E K}$, a contradiction. $\square$

By the previous two theorems for a Galois extension K of F, $F \subseteq E \subseteq K$, and $H \subseteq Gal_F K$, we have $$E_{Gal_E K} = E \qquad H = Gal_{E_H} K.$$

Corollary 16.5. *Let K be a Galois extension of F. Let*

$$S = \{E : F \subseteq E \subseteq K\} \qquad T = \{H : H \subseteq Gal_F K\}.$$

Then

$$\begin{array}{rccc} \varphi : & S & \to & T \\ & E & \mapsto & Gal_E K \end{array}$$

is a bijection.

Proof. Since a Galois extension is finite dimensional, by Theorem 16.2, for any $H \subseteq Gal_F K$, we have $H = Gal_{E_H} K$, and so ψ is surjective. Moreover, by the previous theorem if $GalE_1K = \varphi(E_1) = \varphi(E_2) = GalE_2K$, then

$$E_1 = E_{Gal_{E_1}K} = E_{Gal_{E_2}K} = E_2.$$

Therefore, φ is injective. $\square$

Corollary 16.6. *Let K be a finite-dimensional extension of F. Then K is Galois over F if and only if $F = E_{Gal_F K}$, i.e., F is the fixed field of the Galois group $Gal_F K$.*

Proof. If K is Galois over F again by the previous theorem we have $F = E_{Gal_F K}$. Conversely, if $F = E_{Gal_F K}$, then by Theorem 16.1, K is a normal, simple, separable extension of F and so it is a Galois extension. $\square$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{3},\sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{5}) \arrow[d, dash] & \mathbb{Q}(\sqrt{15}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \langle \iota \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{\iota,\alpha\} \arrow[dr, dash] & \{\iota,\tau\} \arrow[d, dash] & \{\iota,\beta\} \arrow[dl, dash] \\
 & \{\iota,\tau,\alpha,\beta\} &
\end{tikzcd}$$

Theorem 16.7. (The Fundamental Theorem of Galois Theory) *If K is a Galois extension of F, then*

1. *φ is a bijection. Furthermore,*

$$[K : E] = |Gal_E K| \qquad \textit{and} \qquad [E : F] = [Gal_F K : Gal_E K].$$

2. *An intermediate field E is a normal extension of F if and only if $Gal_E K \lhd Gal_F K$, and in this case*

$$Gal_F E \cong Gal_F K / Gal_E K.$$

Proof. (1) We have already showed in Corollary 16.5 that φ is a bijection. Note that by Theorem 16.4 $E_{Gal_E K} = E$, therefore, by Theorem 16.2,

$$[K : E] = [K : E_{Gal_E K}] = |Gal_E K|.$$

Consider that $Gal_E K \leq Gal_F K$, so by group theory we have $[Gal_F K : Gal_E K] = |Gal_F K| / |Gal_E K|$, and so

$$|Gal_E K| [Gal_F K : Gal_E K] = |Gal_F K|.$$

Note that by what we just proved $|Gal_F K| = [K : F]$. Therefore,

$$|Gal_E K| [Gal_F K : Gal_E K] = |Gal_F K| = [K : F] = [K : E][E : F].$$

Since $[K : E] = |Gal_E K|$, we must have

$$[E : F] = [Gal_F K : Gal_E K].$$

Before proving the second part we need a lemma.

Lemma 16.8. *Let K be a finite-dimensional normal extension field of F and E an intermediate field, which is normal over F, Then there is a surjective homomorphism of groups $\theta : Gal_F K \to Gal_F E$ whose kernel is $Gal_E K$. Moreover, $Gal_F K/Gal_F E \cong Gal_E K$.*

Proof. Define

$$\begin{array}{rccc} \theta : & Gal_F K & \to & Gal_F E \\ & \sigma & \mapsto & \sigma|_E \end{array}$$

We first show that θ is well-defined. We only need to show that $\sigma|_E(u) \subseteq E$ and $\sigma|_E$ is surjective. Note that E is an algebraic extension of F. Let $u \in E$ and $p(x)$ be its minimal polynomial over F. Since E is a normal extension of F, so all the roots of $p(x)$ are in E, and since $\sigma(u)$ is a root of $p(x)$, we conclude that $\sigma(u) \subseteq E$. Therefore, $\sigma|_E \subseteq E$. Moreover, since $ker\sigma|E \subseteq ker\sigma = \{0\}$, we must have $\sigma(E) \cong E$. So $\sigma(E)$ is a subspace of E isomorphic to E, and so $\sigma(E) = E$. Therefore, $\sigma|_E$ is in $Gal_F E$, and thus θ is well-defined. Now, we show that θ is surjective. Note that K is finite dimensional over F and also it is a normal extension of F, so it is splitting field of some polynomial (see Theorem 12.5). Since K is also a splitting field of some polynomial over E, then by Theorem 12.4, τ will be extended to an automorphism σ of K. Therefore, $\theta(\sigma) = \sigma|_E = \tau$, and so τ is in the image of θ.

Finally, we show that the kernel of θ is $Gal_E K$. If $\sigma \in Gal_E K$, then $\sigma|_E = id$, so $\sigma \in ker\theta$. If $\sigma \in ker\theta$, then $\sigma|_E = id$, and so $\sigma \in Gal_E K$. Therefore, $ker\theta = GAL_E K$, and $Gal_F K/Gal_F E \cong Gal_E K$. □

(2) Assume that $Gal_E K \lhd Gal_F K$, we want to show that E is a normal extension of F. We must show that if $p(x)$ is an irreducible polynomial in $F[x]$ with a root $u \in E$, then all of the roots of $p(x)$ are in E. Since K is a normal extension of F, all of the roots of $p(x)$ are in K. We may assume that $p(x)$ has degree bigger than 1, because otherwise the root of $p(x)$ is only $u \in E$. Let v be a root of $p(x)$ distinct from u. Then by Theorem 15.3, there is a $\sigma \in Gal_F K$ such that $\sigma(u) = v$. Since $Gal_E K \lhd Gal_F K$, for any $\tau \in Gal_E K$, $\tau\sigma = \sigma\tau_1$ for some $\tau_1 \in Gal_E K$. Note that

$$\tau(v) = \tau(\sigma(u)) = \sigma\tau_1(u) = \sigma(u) = v.$$

Therefore, for any $\tau \in Gal_E K$, we have $\tau(u) = u$, and so $u \in E_{Gal_E K} = E$. As a result, $p(x)$ splits over E.

Converse is just the previous lemma. □

Remark. *The Galois correspondence φ is inclusion-reversing, i.e., if $E \subseteq L$, then $\varphi(L) = Gal_L K \subseteq Gal_E K = \varphi(E)$.*

Let K be the splitting field of $x^3 - 2$. We want to find $Gal_F K$. Note that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, and we have that $\mathbb{Q}(\sqrt[3]{2}) \subset K$ since other roots of $x^3 - 2$ are not in $\mathbb{Q}(\sqrt[3]{2})$. By a theorem, $Gal_F K \subseteq S_3$. Since $|Gal_F K| < |S_3| = 6$ and $|Gal_F K| = [K : \mathbb{Q}] > [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, we must have $[K : F] = 6$ and $Gal_F K = S_3$.

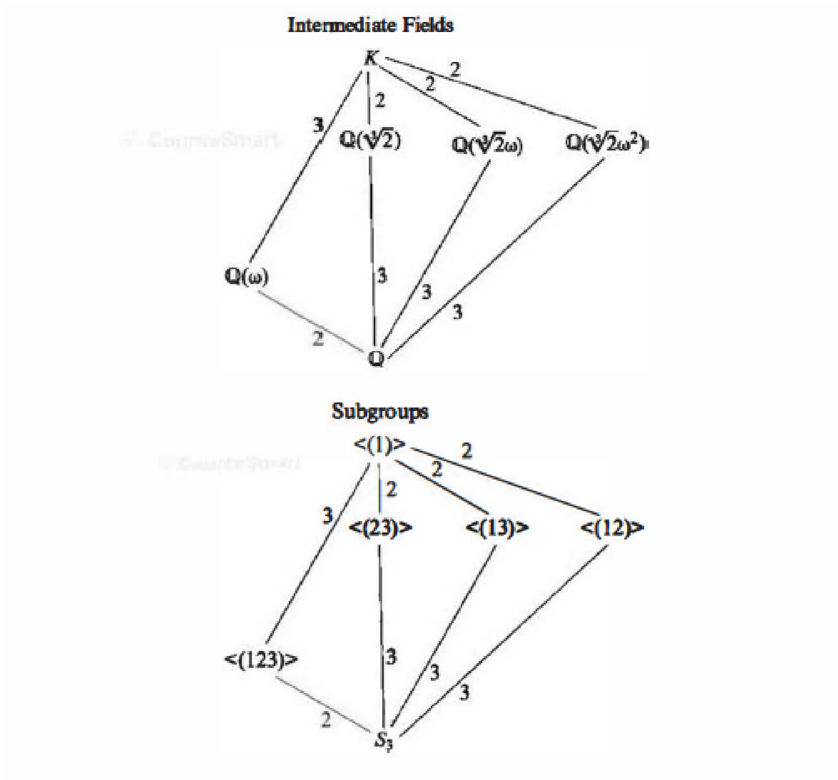
Intermediate Fields
K
2
2
2
3
Q(∛2)
Q(∛2ω)
Q(∛2ω²)
Q(ω)
3
3
3
2
Q
Subgroups
<(1)>
2
2
2
3
<(23)>
<(13)>
<(12)>
<(123)>
3
3
3
2
S₃

Figure 1:

17 Solvability by Radicals

Definition. *A field K is said to be a* **radical extension** *of a field F if there is a chain of fields*

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_t = K$$

such that for each $i = 1, 2, \ldots, t$,

$$F_i = F_{i-1}(u_i) \text{ and some powers of } u_i \text{ is in } F_{i-1}.$$

Definition. *Let $f(x) \in F[x]$. The equation $f(x) = 0_F$ is said to be* **solvable by radicals** *if there is a radical extension of F that contains a splitting field of $f(x)$.*

Remark. *When we say $f(x) = 0$ is not solvable by radicals, it means there is no formula (including only field operations and extraction of roots) for the solution of $f(x) = 0$.*

17.1 Solvable groups

A group is said to be **solvable** if it has a chain of subgroups

$$G = G_0 \subseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n = \langle e \rangle$$

such that each G_i is a normal subgroup of the preceding group G_{i-1} and the quotient group G_{i-1}/G_i is abelian.

Theorem 17.1.

1. *For $n \geq 5$, the group S_n is not solvable.*
2. *Every homeomorphic image of a solvable group G is solvable.*

Definition. *If $f(x) \in F[x]$, then* **Galois group of the polynomial** *$f(x)$ is $Gal_F K$, where K is a splitting field of $f(x)$ over F.*

We state Galois Criteria without proof.

Theorem 17.2. (Galois' Criteria) *Let F be a field of characteristic 0 and $f(x) \in F[x]$. Then $f(x) = 0_F$ is solvable by radicals if and only if the Galois group of $f(x)$ is solvable.*

Example 17.3. *Since S_5 is not solvable and Galois group of $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$ is S_5, therefore, $f(x) = 0$ is not solvable by radicals.*

18 Roots of Unity

Proposition 18.1. *Let K be the splitting field of $x^n - 1$. Then the set of all roots of $x^n - 1$ is a multiplicative subgroup of K, moreover, it is cyclic.*

Proof. Assume that ζ, τ are roots of $x^n - 1$, then $(\zeta\tau)^n - 1 = 0$, and so the set of all roots of $x^n - 1$ is closed under multiplication. Moreover, if ζ is a root of $x^n - 1$, so is ζ^{-1}, thus the set of all roots of $x^n - 1$ produce a multiplicative subgroup of K. It is known in group theory that any finite multiplicative subgroup of a field is cyclic, and so the set of all roots of $x^n - 1$ is a cyclic group. $\square$

Any root of $x^n - 1$ is called an nth root of unity. The above proposition states that the set of all nth roots of unity is a cyclic group. Any generator of this cyclic group is called a primitive nth root of unity.

Lemma 18.2. *Let F be a filed and ζ a primitive nth root of unity in F. Then F contains a primitive dth root of unity for every positive divisor d of n.*

Proof. Let $n = dt$. Note that $(\zeta^t)^d = 1$, moreover if $(\zeta^t)^i = (\zeta^t)^j$, $1 \leq i < j \leq d$, then $(\zeta^t)^{j-i} = 1$, and so $\zeta^{t(j-i)} = 1$, which is a contradiction since $t(j - i) < n$. Therefore,

$$(\zeta^t), (\zeta^t)^2, \ldots, (\zeta^t)^{d-1}$$

are distinct, and so they are the roots of $x^d - 1$, and (ζ^t) is a primitive dth roots of unity. $\square$

Theorem 18.3. *Let F be a field of characteristic 0 and ζ a primitive nth root of unity in some extension field of F. Then $K = F(\zeta)$ is a normal extension of F, and $Gal_F K$ is abelian.*

Proof. Consider that all roots of $x^n - 1$ are in $K = F(\zeta)$, so K is splitting field field of $x^n - 1$, therefore by Theorem 12.5, K is a normal extension of F. Let $\sigma, \tau \in Gal_F K$, then as $\sigma(\zeta), \tau(\zeta)$ are the roots of $x^n - 1$, and the roots of $x^n - 1$ are the powers of ζ, we conclude that $\sigma(\zeta) = \zeta^t$ and $\tau(\zeta) = \zeta^s$. So

$$\sigma \circ (\tau(\zeta)) = \sigma(\zeta^s) = \zeta^{st} \quad \textit{and} \quad \tau \circ (\sigma(\zeta)) = \tau(\zeta^t) = \zeta^{ts}$$

Therefore, $\sigma \circ \tau = \tau \circ \sigma$. $\square$

Theorem 18.4. *Let F be a field of characteristic 0 that contains a primitive nth root of unity. If u is a root of $x^n - c \in F[x]$ in some extension field of F, then $K = F(u)$ is a normal extension of F, and $Gal_F K$ is abelian.*

Proof. If u is a root of $x^n - c$ and ζ is a primitive nth roots, then $\zeta^i u$ for every $1 \leq i \leq n$ is a root of $x^n - c$ since $((\zeta^i u)^n - c = (\zeta^i)^n u^n - c = u^n - c = 0$. Moreover,

$$1, \zeta u, \zeta^2 u, \ldots, \zeta^{n-1} u$$

are distinct because if $\zeta^i u = \zeta^j u$, then $\zeta^i = \zeta^j$, which is contradiction. Therefore, the set of all roots of $x^n - c$ is $\{1, \zeta u, \zeta^2 u, \ldots, \zeta^{n-1} u\}$. Consider that $F(u)$ is splitting field of $x^n - c$ and so $F(u)$ is a normal extension of F. With the same argument as the previous theorem we have that $Gal_F K$ is abelian. $\square$

19 Representation Theory

A representation can be thought of as a way to model a group with a concrete group of matrices. After giving the precise definition, we look at some examples. The general linear group of degree d, $GL_d(\mathbb{C})$ is the set of all $d \times d$ invertible matrices over $\mathbb{C}$.

Definition. *A representation of a group G is a group homomorphism*

$$X : G \to GL_d(\mathbb{C}).$$

Equivalently, to each $g \in G$ is assigned $X(g) \in GL_d(\mathbb{C})$ such that

1. *$X(1) = Id$ the identity matrix in $GL_d(\mathbb{C})$, and*
2. *$X(gh) = X(g)X(h)$ for all $g, h \in G$.*

The parameter d is called the degree, or dimension, of the representation.

In the remainder of this course , we only say a matrix representation without mentioning the group G, if it is clear that we are using G.

Example 19.1. *All groups have the trivial representation, which is the one sending every $g \in G$ to the matrix (1). This is clearly a representation because $X(1) = (1)$ and $X(gh) = (1) = (1)(1) = X(g)X(h)$ for all $g, h \in G$. We often use the notation* **1** *to stand for the trivial representation of G.*

Example 19.2. *Let $G = C_n$ the cyclic group of order n. Let g be a generator for C_n, i.e.,*

$$C_n = \{1, g, g^2, \ldots, g^{n-1}\}.$$

We aim to find all one-dimensional representations of C_n. To identify a group homomorphism form C_n to $GL_d(C)$, it is enough to give $X(g)$. Assume that $X(g) = (c)$ be a one-dimensional representation. Then $X(1) = X(g^n) = X(g)^n = (c)^n = (c^n) = 1$. Therefore, c must be a nth root of unity, and it is clear that for every root of unity we have a one-dimensional representation.

Example 19.3. *One of the important representation for S_n is* **defining representation** *of S_n, which is of degree n. If $\pi \in S_n$, then we let $X(\pi) = (x_{i,j})_{n \times n}$, where*

$$x_{i,j} = \begin{cases} 1 & \textit{if } \pi(j) = i \\ 0 & \textit{otherwise.} \end{cases}$$

Let V be a vector space of dimension n over $\mathbb{C}$ with a fixed basis $\{v_1, \ldots, v_n\}$. Let $GL(V)$ be the set of all invertible linear transformation of V. Note that for every $A = (a_{i,j}) \in GL_n(\mathbb{C})$ and $c = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \in \mathbb{C}^n$, we have $(Ac)_{i,1} = a_{i1}c_1 + \ldots + a_{in}c_n$

Theorem 19.4. *Let V be a vector space of dimension n over $\mathbb{C}$ with a fix basis $\{v_1, \ldots, v_n\}$. Then $GL_n(\mathbb{C}) \cong GL(V)$.*

Proof. Define α as follows,

$$\begin{array}{rccc}\alpha: & GL_n(C) & \to & GL(V) \\ & A & \mapsto & T_A,\end{array}$$

where if $v = c_1v_1 + \ldots + c_nv_n$, then

$$T_A(c_1v_1 + \ldots + c_nv_n) = (A\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix})_{1,1}v_1 + \ldots + (A\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix})_{n,1}v_n.$$

□

19.1 G-modules and Group algebras

Definition. *(1) Let V be a vector space and G be a group. Then V is a G-module if there is a group homomorphism*

$$\rho : G \to GL(V).$$

Definition. *(2) The vector space V is a G-module if there is a multiplication, $g.v$, of elements of V by elements of G such that*

1. $g.v \in V$,
2. $g.(cv + dw) = c(g.v) + d(g.w)$,
3. $g.(h.v) = (gh).v$,
4. $e.v = v$ *for all* $g, h \in G$, $v, w \in V$, *and scalars* $c, d \in \mathbb{C}$.

Why the two definitions are equivalent? Assume that there is a group homomorphism

$$\rho : G \to GL(V).$$

Denote the homomorphism $\rho(g)$ by ρ_g. Then we can define a multiplication as follows $g.v = \rho_g(v)$. It is easy to check that this multiplication has all desired properties.

Now if we have a vector space with the properties in the second definition, then

$$\begin{array}{rccc}\rho: & G & \to & GL(V), \\ & g & \to & \rho_g,\end{array}$$

where $\rho_g(v) = g.v$.

19.2 Action of a group on a set yields a G-module

Before we start, let produce a matrix out of a linear transformation form V to V. Let V be a vector space with $\mathcal{B} = \{v_1, \ldots, v_n\}$ as a basis, and let T be a linear transformation from V to V, then

$$[T]_{\mathcal{B}} = [[T(v_1)]_{\mathcal{B}} \ldots [T(v_n)]_{\mathcal{B}}]$$

is an $n \times n$ matrix. Moreover, we have

$$GL(V) \cong GL_n(\mathbb{C})$$

in which the image of T is $[T]_{\mathcal{B}}$.

Definition. *We say a group G acts on a set S if there is a multiplication*

$$\begin{array}{rccc} .: & G \times S & \to & S \\ & (g,s) & \mapsto & g.s \end{array}$$

such that

1. $1.s = s$
2. $(gh).s = g.(h.s)$

for all $g, h \in G$ and $s \in S$.

Now assume that G acts on $S = \{s_1, \ldots, s_n\}$. Let

$$\mathbb{C}S = \mathbb{C}\{s_1, \ldots, s_n\} = \{c_1 s_1 + \ldots + c_n s_n : c_i \in \mathbb{C}\}$$

consists of all formal linear combination of the elements in S

- $\mathbb{C}S$ is a vector space with the following addition and scalar multiplication,

$$\begin{array}{rccc} + : & \mathbb{C}S \times \mathbb{C}S & \to & \mathbb{C}S \\ & (c_1 s_1 + \ldots + c_n s_n, d_1 s_1 + \ldots + d_n s_n) & \mapsto & (c_1 + d_1) s_1 + \ldots + (c_n + d_n) s_n \end{array}$$

$$c(c_1 s_1 + \ldots + c_n s_n) = (cc_1) s_1 + \ldots + (cc_n) s_n.$$

Note that the set S is a basis for $\mathbb{C}S$ as a $\mathbb{C}$-vector space and so the dimension of $\mathbb{C}S$ is $|S|$.

- Now we have that $\mathbb{C}S$ is a G-module with the following group homomorphism,

$$\begin{array}{rccc} \rho : & G & \to & GL(\mathbb{C}S) \\ & g & \mapsto & \rho_g, \end{array}$$

where

$$\rho_g(c_1 s_1 + \ldots + c_n s_n) = c_1(g.s_1) + \ldots + c_n(g.s_n).$$

$$\left(\begin{array}{c} \text{or equivalently we can define a multiplication as follows,} \\ \begin{array}{rccc} .: & G \times \mathbb{C}S & \to & \mathbb{C}S \\ & (g, c_1 s_1 + \ldots + c_n s_n) & \mapsto & c_1(g.s_1) + \ldots + c_n(g.s_n) \end{array} \end{array} \right)$$

Moreover, any this G-module produce a representation

$$\begin{array}{rccccc} X : & G & \xrightarrow{\rho} & GL(\mathbb{C}S) & \to & GL_n(\mathbb{C}) \\ & g & \mapsto & \rho_g & \mapsto & [\rho_g]_S \end{array}$$

Definition. *If G acts on a set S, then the G-module $\mathbb{C}S$ as defined above is called permutation representation associated with S.*

Example 19.5. *Consider that S_n acts on $S = \{1, 2, \ldots, n\}$ as follows,*

$$\begin{array}{rccc} .: & S_n \times S & \to & S \\ & (\sigma, i) & \mapsto & \sigma(i) \end{array}$$

Therefore, we can consider $\mathbb{C}S = \{c_1\mathbf{1} + c_2\mathbf{2} + \ldots + c_n\mathbf{n} : c_i \in \mathbb{C}\}$ as a S_n module with the homomorphism

$$\begin{array}{rccc} \rho: & S_n & \to & GL(\mathbb{C}S) \\ & \sigma & \mapsto & \rho_\sigma, \end{array}$$

where

$$\rho_\sigma(c_1\mathbf{1} + \ldots + c_n\mathbf{n}) = c_1(\sigma.\mathbf{1}) + \ldots + c_n(\sigma.\mathbf{n}).$$

And for example, if $S = \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$, then

$$X((1,2)) = [\rho_{(1,2)}]_S = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Example 19.6. *(Regular representation) Let $G = \{g_1, \ldots, g_n\}$ be a group, then as G always acts on G as follows,*

$$\begin{array}{rccc} .: & G \times G & \to & G \\ & (g,h) & \mapsto & gh \end{array}$$

So the corresponding G-module is

$$\mathbb{C}G = \{c_1g_1 + \ldots + c_ng_n : c_i \in \mathbb{C}\}$$

which has the following homomorphism

$$\begin{array}{rccc} \rho: & G & \to & GL(\mathbb{C}[G]) \\ & g & \mapsto & \rho_g \end{array}$$

where

$$\rho_g(c_1g_1 + \ldots + c_ng_n) = c_1(gg_1) + \ldots + c_n(gg_n).$$

As an example if $G = C_4 = \{e, g, g^2, g^3\}$, then

$$\mathbb{C}[C_4] = \{c_1e + c_2g + c_3g^2 + c_4g^3 : c_i \in \mathbb{C}\}.$$

Moreover,

$$X(g^2) = [\rho_{g^2}]_{C_4} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Example 19.7. *(Coset representation of G with respect to H) Let H be a subgroup of G, then $G = g_1H \sqcup \ldots \sqcup g_kH$, and $g_1, g_2, \ldots, g_k$ are called transversal for H. Let*

$$\mathcal{H} = \{g_1H, g_2H, \ldots, g_kH\}.$$

Then there is an action of G on $\mathcal{H}$ as follows,

$$\begin{array}{rccc} .: & G \times \mathcal{H} & \to & \mathcal{H} \\ & (g, g_iH) & \mapsto & (gg_i)H \end{array}$$

So the corresponding G-module is

$$\mathbb{C}\mathcal{H} = \{c_1(g_1H) + \ldots + c_k(g_kH) : c_i \in \mathbb{C}\}.$$

And also for example if $H = \{e, (2,3)\}$, then $\mathcal{H} = \{H, (1,2)H, (2,3)H\}$.

$$X((1,2)) = \rho_{(1,2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

20 Reducibility

Definition. *Let V be a G-module. A submodule of V is a subspace W that is closed under the action of G, i.e.,*

$$w \in W, g \in G \Rightarrow g.w \in W.$$

In this situation we also say W is G-invariant. (It is equivalent to say if ρ is the group homomorphism of the G-module V, then W is a subspace of V if $\rho|_W \in GL(W)$).

Example 20.1. *Every G-module V has two trivial submodules $W = \{0\}$ and $W = V$.*

Example 20.2. *Consider the $\mathbb{C}\{\mathbf{1}, \ldots, \mathbf{n}\}$ as a S_n module. Note that*

$$W = \mathbb{C}\{\mathbf{1} + \ldots + \mathbf{n}\}$$

is a subspace of V since for every $\sigma \in S_n$ and $w = c(\mathbf{1} + \ldots + \mathbf{n}) \in W$, we have $\sigma.w = c(\sigma(\mathbf{1}) + \ldots + \sigma(\mathbf{n})) \in W$.

Example 20.3. *Let $G = \{g_1, \ldots, g_n\}$ with group algebra $V = \mathbb{C}[G]$. Let*

$$W = \mathbb{C}[\mathbf{g}_1 + \ldots + \mathbf{g}_n].$$

Note that W is a G-module since for every $g \in G$ and $c(g_1 + \ldots + g_n)$,

$$g.(c(\mathbf{g}_1 + \ldots + \mathbf{g}_n)) = c(gg_1 + g\mathbf{g}_2 + \ldots + g\mathbf{g}_n) = c(\mathbf{g}_1 + \ldots + \mathbf{g}_n) \in W.$$

Example 20.4. *Consider $\mathbb{C}[S_n]$ and $W = \mathbb{C}[\sum_{\sigma \in S_n} sgn(\sigma)\sigma]$. Then for every $\pi \in S_n$ and $c\sum_{\sigma \in S_n} sgn(\sigma)\sigma$, we have*

$$\pi.c\sum_{\sigma \in S_n} sgn(\sigma)\sigma = c(\sum_{\sigma \in S_n} sgn(\sigma)\pi \circ \sigma) = c(\sum_{\pi^{-1}\sigma \in S_n} sgn(\pi^{-1} \circ \tau)\tau) =$$

$$\pm c(\sum_{\pi^{-1}\sigma \in S_n} sgn(\pi^{-1} \circ \tau)\tau) = \pm c\sum_{\sigma \in S_n} sgn(\sigma)\sigma.$$

Negative sign is when $sgn(\pi) = -1$.

Definition. *A nonzero G-module V is reducible if it contains a nontrivial submodule W. Otherwise, V is said to be irreducible. Equivalently, V is reducible if it has a basis $\mathcal{B}$ in which every $g \in G$ is assigned a block matrix of the form*

$$X(g) = \left(\begin{array}{c|c} A(g) & B(g) \\ \hline 0 & C(g) \end{array}\right)$$

where $A(g)$ are square matrices, all of the same size, and 0 is a nonempty matrix of zeros.

Example 20.5. *Let $V = \mathbb{C}\{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$ and $W = \mathbb{C}\{\mathbf{1} + \mathbf{2} + \mathbf{3}\}$. Note that $\{\mathbf{1} + \mathbf{2} + \mathbf{3}\}$ is a basis for W and $\mathbb{B} = \{\mathbf{1} + \mathbf{2} + \mathbf{3}, \mathbf{2}, \mathbf{3}\}$ is a basis for V. Consider that W is a submodule of V. We want to find corresponding representation,*

$$\begin{array}{rccccc} X: & G & \rightarrow & GL(V) & \rightarrow & GL_3(\mathbb{C}) \\ & g & \mapsto & \rho_g & \mapsto & [\rho_g]_{\mathcal{B}} \end{array}$$

Thus, $X((1,2)) = [[\rho_{(1,2)}(\mathbf{1}+\mathbf{2}+\mathbf{3})]_{\mathcal{B}} \ \ [\rho_{(1,2)}(\mathbf{2})]_{\mathcal{B}} \ \ [\rho_{(1,2)}(\mathbf{3})]_{\mathcal{B}}]$. *We have*

$$\rho_{(1,2)}(\mathbf{1}+\mathbf{2}+\mathbf{3}) = \mathbf{1}+\mathbf{2}+\mathbf{3},$$

$$\rho_{(1,2)}(\mathbf{2}) = \mathbf{1} = \mathbf{1}+\mathbf{2}+\mathbf{3}-\mathbf{2}-\mathbf{3}$$

$$\rho_{(1,2)}(\mathbf{3}) = \mathbf{3} = \mathbf{3}.$$

Therefore,

$$X((1,2)) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$$

If you check for any $\sigma \in S_3$, *you will see*

$$X(g) = \left(\begin{array}{c|cc} * & * & * \\ \hline 0 & * & * \\ 0 & * & * \end{array}\right)$$

21 Inner product space

Definition. *An* **inner product** *on a vector space* V *is a function*

$$\langle .,. \rangle : V \times V \longrightarrow \mathbb{C}$$

satisfying the following axioms:

1. $\langle u, v \rangle = \langle v, u \rangle$
2. $\langle u+v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
3. $\langle cu, v \rangle = c\langle u, v \rangle$
4. $\langle u, u \rangle \geq 0$ *and* $\langle u, u \rangle = 0$ *if and only if* $u = 0$.

A vector space with an inner product is called an **inner product space**. *Moreover, it is clear from the definition any subspace of an inner product space is an inner product space.*

Definition. *Two vectors* $v, w \in V$ *are orthogonal if* $\langle v, w \rangle = 0$.

Definition. *Let* $y \in V$ *where* V *is an inner product space. Let* $\{v_1, \ldots, v_p\}$ *be an orthogonal basis for* W. *Then the orthogonal projection of* y *onto a subspace* W *of* V *is*

$$\mathbf{proj}_W y = \frac{\langle y, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 + \frac{\langle y, v_2 \rangle}{\langle v_2, v_2 \rangle} v_2 + \ldots + \frac{\langle y, v_p \rangle}{\langle v_p, v_p \rangle} v_p.$$

Note that $\mathbf{proj}_W y \in W$, $y - \mathbf{proj}_W y \in W^{\perp}$.

Theorem 21.1. *(The Gram-Schmidt process for an inner product space) Given a basis* $\{x_1, \ldots, x_p\}$ *for non-zero subspace* W *of an inner product space* V, *define*

$v_1 = x_1$

$v_2 = x_2 - \frac{\langle x_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1$

$v_3 = x_3 - \frac{\langle x_3, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 - \frac{\langle x_3, v_2 \rangle}{\langle v_2, v_2 \rangle} v_2$

$\vdots$

$v_p = x_p - \frac{\langle x_p, v_1\rangle}{\langle v_1, v_1\rangle} v_1 - \frac{\langle x_p, v_2\rangle}{\langle v_2, v_2\rangle} v_2 - \ldots - \frac{\langle x_p, v_{p-1}\rangle}{\langle v_{p-1}, v_{p-1}\rangle} v_{p-1}$

Then $\{v_1, \ldots, v_p\}$ is an orthogonal basis for W. In addition $span\{v_1, \ldots, v_k\} = span\{x_1, \ldots, x_k\}$ for $1 \leq k \leq p$.

Theorem 21.2. *Let W be a subspace of an inner product space V. Then*

$$W^\perp = \{v \in V : \langle v, w\rangle = 0, \text{ for all } w \in W\},$$

the orthogonal complement of W, is also an inner product spaces.

Proof. We show that $W^\perp$ is a subspace, i.e., if $s, z \in W^\perp$, then $cz + s$ for $c \in \mathbb{C}$, is in $W^\perp$. Note that for any $w \in W$,

$$\langle cz + s, w\rangle = c\langle z, w\rangle + \langle s, w\rangle = 0,$$

and so $cz + s \in W$. □

Definition. *Let V be a vector space with subspaces U and W. Then V is (internal) direct sum of U and W, written $V = U \oplus W$ if $U \cap W = \{0\}$ and every element $v \in V$ can be written as $v = u + w$ where $u \in U$ and $w \in W$. If V, U and W are G-modules we say U and W are complement of each other.*

Theorem 21.3. *Let V be an inner product space and W be a subspace of V. Then $V = W \oplus W^\perp$.*

Proof. If $w \in W \cap W^\perp$, then for every $v \in W$, we must have $\langle w, v\rangle = 0$, so $\langle w, w\rangle = 0$, and it implies $w = 0$.

Moreover, any element $v \in V$, can be written as $v = \mathbf{proj}_W v + (v - \mathbf{proj}_W v)$, where $\mathbf{proj}_W v \in W$ and $(v - \mathbf{proj}_W v) \in W^\perp$. □

22 Maschke's Theorem

Remark. *When $V = W \oplus U$, then there is a basis for V such that the corresponding homomorphism is of the from*

$$X(g) = \left(\begin{array}{c|c} A(g) & 0 \\ \hline 0 & B(g) \end{array}\right).$$

Definition. *If X is a matrix, we say X is the direct sum of A and B, written $X = A \oplus B$, if*

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right).$$

Definition. *Let V be a G-module with an orthogonal basis $\{v_1, \ldots, v_n\}$. Then if $v = c_1 v_1 + \ldots + c_n v_n$, and $w = d_1 v_1 + \ldots + d_n v_n$, define*

$$\langle v, w\rangle = \sum_{i=1}^{n} c_i d_j \delta_{v_i, v_j},$$

where

$$\delta_{v_i,v_j} = \begin{cases} 1 & i = j \\ 0 & otherwise. \end{cases}$$

Now define,

$$\langle v, w\rangle' = \sum_{g\in G} \langle gv, gw\rangle.$$

Theorem 22.1. *Let V be a G-module. Then V is an inner product space with $\langle ., .\rangle'$ and moreover, if W is a G-submodule of V, then $W^\perp$ is also a G-module.*

Proof. It is easy to check that V is an inner product space with the inner product. We only show that $W^\perp$ is a G-submodule of V. Let $g \in G$ and $z \in W^\perp$, then we should show that $h.z \in W^\perp$, i.e., $\langle hz, w\rangle' = 0$ for every $w \in W$. Note that

$$\langle hz, w\rangle' = \sum_{g\in G} \langle ghz, gw\rangle.$$

$$\langle z, h^{-1}w\rangle' = \sum_{g\in G} \langle gz, gh^{-1}w\rangle.$$

Let $t = gh^{-1}$, then $g = th$. So,

$$0 = \langle z, h^{-1}w\rangle' = \sum_{th\in G} \langle thz, tw\rangle = \sum_{t\in G} \langle thz, tw\rangle = \sum_{g\in G} \langle ghz, gw\rangle = \langle hz, w\rangle'.$$

Therefore, $hz \in W^\perp$ and so $W^\perp$ is a G-module. □

Theorem 22.2. *(Mascheke's Theorem) Let G be a finite group and let V be a nonzero G-module. Then*

$$V = W^{(1)} \oplus \cdots \oplus W^{(k)}$$

where each $W^{(i)}$ is an irreducible G-module of V.

Proof. Let $dimV = d$, we prove the theorem by induction. Let $dimV = 1$, then V must be an irreducible module. Now assume that the theorem is true for any positive integer less than d and $dimV = d > 1$. If V is an irreducible module we are done, otherwise it has a nontrivial submodule W and by the previous theorem $V = W \oplus W^\perp$. Notice that $dimW$ and $dimW^\perp$ are less than d, so by induction hypothesis they decompose to irreducible submodules and so does V. □

Corollary 22.3. *Let G be a group and X be a matrix representation of G of dimension $d > 0$. Then there is a fixed matrix T such that every matrix $X(g)$, $g \in G$, is of the form*

$$TX(gT^{-1}) = \begin{pmatrix} X^{(1)}(g) & 0 & \dots & 0 \\ 0 & X^{(2)}(g) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & X^{(k)}(g) \end{pmatrix}$$