

# MATH 4108: Abstract Algebra II

Frank Qiang  
Instructor: Jennifer Hom

Georgia Institute of Technology  
Spring 2024

# Contents

<b>1</b>	<b>Jan. 8 — Rings and Fields</b>	<b>3</b>
1.1	Lots of Definitions . . . . .	3
<b>2</b>	<b>Jan. 10 — Field of Fractions, Polynomials</b>	<b>6</b>
2.1	Isomorphisms . . . . .	6
2.2	Field of Fractions . . . . .	7
2.3	The Characteristic of a Field . . . . .	8
2.4	Polynomials . . . . .	9
<b>3</b>	<b>Jan. 17 — Irreducible Polynomials</b>	<b>10</b>
3.1	Principal Ideal Domains and Irreducible Polynomials . . . . .	10
3.2	Irreducible Polynomials over $\mathbb{C}$ , $\mathbb{R}$ , $\mathbb{Q}$ , and $\mathbb{Z}$ . . . . .	11
<b>4</b>	<b>Jan. 22 — Field Extensions</b>	<b>15</b>
4.1	More on Irreducibility . . . . .	15
4.2	Field Extensions . . . . .	16
<b>5</b>	<b>Jan. 24 — Algebraic Extensions</b>	<b>20</b>
5.1	Minimal Polynomials . . . . .	20
5.2	Algebraic Extensions . . . . .	21
<b>6</b>	<b>Jan. 29 — Geometric Constructions</b>	<b>23</b>
6.1	$K$ -Isomorphisms . . . . .	23
6.2	Applications to Geometric Constructions . . . . .	24
6.3	Classic Problems . . . . .	25
6.3.1	Duplicating the Cube . . . . .	25
6.3.2	Trisecting the Angle . . . . .	25
<b>7</b>	<b>Jan. 31 — Splitting Fields</b>	<b>27</b>
7.1	Review of Notation . . . . .	27
7.2	Splitting Fields . . . . .	27
7.3	Finite Fields . . . . .	29
<b>8</b>	<b>Feb. 5 — Finite Fields</b>	<b>30</b>
8.1	Last Time . . . . .	30
8.2	Finite Fields . . . . .	30
8.3	Automorphisms of Fields . . . . .	32
<b>9</b>	<b>Feb. 7 — The Galois Correspondence</b>	<b>34</b>
9.1	Automorphisms of Fields . . . . .	34
9.2	The Galois Correspondence . . . . .	34

9.3	Normal Extensions . . . . .	36
<b>10 Feb. 12</b>	<b>— Normal Closures</b>	<b>38</b>
10.1	Normal Closures . . . . .	38
10.2	Separable Extensions . . . . .	40
<b>11 Feb. 21</b>	<b>— Galois Extensions</b>	<b>42</b>
11.1	Example of an Inseparable Extension . . . . .	42
11.2	Galois Extensions . . . . .	42
<b>12 Feb. 26</b>	<b>— The Fundamental Theorem</b>	<b>44</b>
12.1	Normal Subgroups . . . . .	44
12.2	The Fundamental Theorem of Galois Theory . . . . .	44
<b>13 Feb. 28</b>	<b>— Join of Subgroups and Subfields</b>	<b>47</b>
13.1	Join of Subgroups . . . . .	47
<b>14 Mar. 4</b>	<b>— Solvable Groups</b>	<b>48</b>
14.1	Solvable Groups . . . . .	48
14.2	Solvable Polynomials . . . . .	50
<b>15 Mar. 6</b>	<b>— Cyclotomic Polynomials</b>	<b>52</b>
15.1	Cyclotomic Polynomials . . . . .	52
15.2	The Galois Groups of Cyclotomic Polynomials . . . . .	53
<b>16 Mar. 11</b>	<b>— Solvable Polynomials</b>	<b>56</b>
16.1	More on Cyclotomic Polynomials . . . . .	56
16.2	Solvable Polynomials . . . . .	56
16.3	Insolvability of the Quintic . . . . .	58
16.4	Finitely-Generated Extensions . . . . .	58
<b>17 Mar. 13</b>	<b>— Symmetric Polynomials</b>	<b>60</b>
17.1	Transcendental Extensions . . . . .	60
17.2	Symmetric Polynomials . . . . .	60
<b>18 Mar. 25</b>	<b>— Modules</b>	<b>64</b>
18.1	Introduction to Modules . . . . .	64
18.2	Submodules . . . . .	65
18.3	Module Homomorphisms . . . . .	65
18.4	Direct Sums of Modules . . . . .	66
<b>19 Mar. 27</b>	<b>— Multilinear Functions</b>	<b>69</b>
19.1	The Homomorphism Theorem . . . . .	69
19.2	Multilinear Functions . . . . .	70

# Lecture 1

## Jan. 8 — Rings and Fields

### 1.1 Lots of Definitions

Recall the definitions of a ring and a field:

**Definition 1.1** (Ring). A *ring*  $R = (R, +, \cdot)$  is a non-empty set  $R$  together with two binary operations  $+$  and  $\cdot$ , called addition and multiplication respectively, which satisfy:

(R1) *Associative law for addition*:  $(a + b) + c = a + (b + c)$  for all  $a, b, c \in R$ .

(R2) *Commutative law for addition*:  $a + b = b + a$  for all  $a, b \in R$ .

(R3) *Existence of zero*: There exists  $0 \in R$  such that  $a + 0 = a$  for all  $a \in R$ .

(R4) *Existence of additive inverses*: For all  $a \in R$ , there exists  $-a \in R$  such that  $a + (-a) = 0$ .<sup>1</sup>

(R5) *Associative law for multiplication*:  $(ab)c = a(bc)$  for all  $a, b, c \in R$ .

(R6) *Distributive laws*:  $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$  for all  $a, b, c \in R$ .

**Definition 1.2** (Commutative ring). In this class, we will mostly be interested in *commutative rings*, which satisfy the following additional property for multiplication:

(R7) *Commutative law for multiplication*:  $ab = ba$  for all  $a, b \in R$ .

**Definition 1.3** (Ring with unity). A ring *with unity* satisfies the additional property that

(R8) *Existence of unity*: There exists  $1 \neq 0 \in R$  such that  $a1 = 1a = a$  for  $a \in R$ .

Note that a ring need not be commutative to have a unity.

**Definition 1.4** (Domain). A commutative ring with unity is called a (*integral*) *domain* if it has the following cancellation property:

(R9) *Cancellation*: For all  $a, b \in R$  and  $c \neq 0$ ,  $ca = cb$  implies  $a = b$ .

(R9') *No zero divisors*: For all  $a, b \in R$ ,  $ab = 0$  implies  $a = 0$  or  $b = 0$ .

The conditions (R9) and (R9') are equivalent.

**Definition 1.5** (Field). A commutative ring with unity is called a *field* if it has the following additional property for multiplicative inverses:

(R10) *Existence of multiplicative inverses*: For all  $a \neq 0 \in R$ , there exists  $a^{-1} \in R$  such that  $aa^{-1} = 1$ .

---

<sup>1</sup>Note that we'll usually write  $a - b$  in place of  $a + (-b)$ .

**Example 1.5.1.** Some examples of rings are  $\mathbb{Z}/2\mathbb{Z}$ , which also happens to be a field. The ring  $\mathbb{Z}$  is a domain. The set  $M_{2 \times 2}(\mathbb{R})$  is a non-commutative ring with unity, and has zero divisors. The ring  $\mathbb{Q}$  is a field.<sup>2</sup> The real polynomials in a single variable  $\mathbb{R}[x]$  form a ring, which is a domain but not a field. The complex numbers  $\mathbb{C}$  and the real numbers  $\mathbb{R}$  both form a field. The even integers  $2\mathbb{Z}$  form a commutative ring without unity. In general,  $\mathbb{Z}/n\mathbb{Z}$  is a commutative ring with unity, and is a field if and only if  $n$  is prime (and has zero divisors otherwise, if  $n$  is composite).

**Remark.** If  $(R, +, \cdot)$  is a ring, then  $(R, +)$  is an abelian group. If  $(K, +, \cdot)$  is a field, then  $(K^*, \cdot)$  is an abelian group, where  $K^* = K \setminus \{0\}$ .

**Definition 1.6** (Group of units). Let  $R$  be a commutative ring with unity. The *group of units* of  $R$  is

$$U = \{u \in R \mid \text{there exists } v \in R \text{ such that } uv = 1\}.$$

**Exercise 1.1.** Show that  $U$  is in fact a group under multiplication.

**Definition 1.7** (Associate). If  $a, b \in R$  such that  $a = ub$  for some  $u \in U$ , then  $a$  and  $b$  are called *associates*, denoted by  $a \sim b$ .

**Exercise 1.2.** Show that  $\sim$  is in fact an equivalence relation.

**Example 1.7.1.** The group of units of  $\mathbb{Z}$  is  $\{1, -1\}$ . The group of units of a field  $K$  is  $K^* = K \setminus \{0\}$ .

**Exercise 1.3.** Let  $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ . Check the following:

1.  $R$  is a commutative ring with unity.
2. The group of units of  $R$  is  $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}, |a^2 - 2b^2| = 1\}$ .

**Definition 1.8** (Divisor). Let  $D$  be an integral domain,  $a \in D \setminus \{0\}$ ,  $b \in D$ . Then  $a$  divides  $b$ , or  $a$  is a *divisor* or *factor* of  $b$ , denoted by  $a|b$ , if there exists  $z \in D$  such that  $az = b$ . We write  $a \nmid b$  if  $a$  does not divide  $b$ . We say that  $a$  is a *proper divisor* or that  $a$  *properly divides*  $b$  if  $z$  is not a unit.

**Remark.** Equivalently,  $a$  is a proper divisor of  $b$  if and only if  $a|b$  and  $b \nmid a$ .

**Definition 1.9** (Subring). A *subring*  $U$  of a ring  $R$  is a non-empty subset of  $R$  with the property that for all  $a, b \in R$ ,  $a, b \in U$  implies  $a + b \in U$  and  $ab \in U$ , and  $a \in U$  implies  $-a \in U$ .

**Remark.** Equivalently,  $U$  is a subring of  $R$  if and only if  $a, b \in U$  implies  $a - b \in U$  and  $ab \in U$ .

**Remark.** We automatically have  $0 \in U$  since we can pick any  $a \in U$ , and then  $0 = a - a \in U$ .

**Definition 1.10** (Subfield). A *subfield* of a field  $K$  is a subset  $E$  containing at least two elements such that  $a, b \in E$  implies  $a - b \in E$  and  $a \in E, b \in E \setminus \{0\}$  implies  $ab^{-1} \in E$ . If  $E$  is a subfield and  $E \neq K$ , then we say  $E$  is a *proper* subfield.

**Remark.** As before, we can replace the last condition with the equivalent statement that  $a, b \in E$  implies  $ab \in E$  and  $a \in E \setminus \{0\}$  implies  $a^{-1} \in E$ .

**Definition 1.11** (Ideal). An *ideal* of  $R$  is a non-empty subset  $I$  of  $R$  with the properties that  $a, b \in I$  implies  $a - b \in I$  and  $a \in I, r \in R$  implies  $ra \in I$ .

**Remark.** All ideals are subrings, but the converse is not true in general.

**Example 1.11.1.** The integers  $\mathbb{Z}$  form a subring of  $\mathbb{R}$  but not an ideal.

---

<sup>2</sup>In fact,  $\mathbb{Q}$  is somehow the smallest field containing  $\mathbb{Z}$ .

**Remark.** We trivially have that  $\{0\}$  and  $R$  are both ideals of  $R$ . An ideal  $I$  is called *proper* if  $\{0\} \subsetneq I \subsetneq R$ .

**Theorem 1.1.** Let  $A = \{a_1, \dots, a_n\}$  be a finite subset of a commutative ring  $R$ . Then the set

$$Ra_1 + \dots + Ra_n = \{x_1a_1 + \dots + x_na_n \mid x_i \in R\}$$

is the smallest ideal of  $R$  containing  $A$ .

*Proof.* See Howie. Check this is indeed an ideal and is contained in any other ideal containing  $A$ .  $\square$

**Definition 1.12** (Ideals generated by elements of a ring). The set  $Ra_1 + \dots + Ra_n$  is the *ideal generated* by  $a_1, \dots, a_n$ , denoted by  $\langle a_1, \dots, a_n \rangle$ . If the ideal is generated by a single element  $a \in R$ , then we say that  $Ra = \langle a \rangle$  is a *principal ideal*.

**Example 1.12.1.** In  $\mathbb{Z}$ , the ideal  $\langle 2 \rangle = 2\mathbb{Z}$  are the even numbers. We have  $\langle 2, 3 \rangle = \mathbb{Z}$ , but  $\langle 6, 8 \rangle = \langle 2 \rangle$ .

**Theorem 1.2.** Let  $D$  be an integral domain with group of units  $U$  and let  $a, b \in D \setminus \{0\}$ . Then

1.  $\langle a \rangle \subseteq \langle b \rangle$  if and only if  $b|a$ ,
2.  $\langle a \rangle = \langle b \rangle$  if and only if  $a \sim b$ ,
3.  $\langle a \rangle = D$  if and only if  $a \in U$ .

*Proof.* See Howie.  $\square$

**Definition 1.13** (Homomorphism of rings). A *homomorphism* from a ring  $R$  to a ring  $S$  is a mapping  $\varphi : R \rightarrow S$  such that  $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$  and  $\varphi(ab) = \varphi(a)\varphi(b)$  for all  $a, b \in R$ .

**Example 1.13.1.** The zero mapping  $\varphi(a) = 0$  is always a homomorphism. The inclusion map  $\iota : 2\mathbb{Z} \rightarrow \mathbb{Z}$  or  $\iota : \mathbb{Z} \rightarrow \mathbb{Q}$  is a homomorphism.

**Theorem 1.3.** Let  $R, S$  be rings and  $\varphi : R \rightarrow S$  a homomorphism. Then

1.  $\varphi(0_R) = 0_S$ ,
2.  $\varphi(-r) = -\varphi(r)$  for all  $r \in R$ ,
3. the image  $\varphi(R)$  is a subring of  $S$ .

*Proof.* See Howie.  $\square$

**Definition 1.14** (Monomorphism). Let  $\varphi : R \rightarrow S$  be a homomorphism. If  $\varphi$  is injective, we say that  $\varphi$  is a *monomorphism* or an *embedding*.

**Example 1.14.1.** The inclusion map  $\varphi : \mathbb{Z} \rightarrow \mathbb{R}$  given by  $\varphi(n) = n$  is an embedding.

# Lecture 2

## Jan. 10 — Field of Fractions, Polynomials

### 2.1 Isomorphisms

**Definition 2.1** (Isomorphism). If a homomorphism  $\varphi : R \rightarrow S$  is both one-to-one and onto, then  $\varphi$  is an *isomorphism* and we say  $R$  and  $S$  are *isomorphic*, denoted  $R \cong S$ .

**Definition 2.2** (Automorphism). An isomorphism  $\varphi : R \rightarrow R$  is called an *automorphism*.

**Example 2.2.1.** For any ring  $R$ , the identity map  $\varphi : R \rightarrow R$  with  $\varphi = \text{id}$  is an automorphism.

**Exercise 2.1.** The complex conjugation  $\varphi : \mathbb{C} \rightarrow \mathbb{C}$  with  $\varphi(z) = \bar{z}$  is an automorphism.

**Definition 2.3** (Kernel). Let  $\varphi : R \rightarrow S$  be a homomorphism. The *kernel* of  $\varphi$  is

$$\ker \varphi = \phi^{-1}(0_S) = \{a \in R : \varphi(a) = 0_S\}.$$

**Exercise 2.2.** For any homomorphism  $\varphi$ ,  $\ker \varphi$  is an ideal.

**Definition 2.4** (Residue class). Let  $I$  be an ideal of a ring  $R$  and  $a \in R$ . The set

$$a + I = \{a + x \mid x \in I\}$$

is the *residue class* of  $a$  modulo  $I$ .

**Exercise 2.3.** The set  $R/I$  of residue classes modulo  $I$  forms a ring with respect to the operations

$$(a + I) + (b + I) = (a + b) + I \quad \text{and} \quad (a + I)(b + I) = ab + I.$$

**Exercise 2.4.** The map  $\theta_I : R \rightarrow R/I$  with  $\theta_I(a) = a + I$  is a surjective homomorphism onto  $R/I$  with kernel  $I$ . This map  $\theta_I$  is called the *natural homomorphism* from  $R$  to  $R/I$ .

**Example 2.4.1.** Consider  $\mathbb{Z}$  and  $I = \langle n \rangle = n\mathbb{Z}$ . Then  $\theta_I : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  with  $\theta_I(a) = a + \langle n \rangle$  is the natural homomorphism. There are  $n$  residue classes, which are

$$\langle n \rangle, \quad 1 + \langle n \rangle, \quad \dots, \quad (n-1) + \langle n \rangle.$$

**Theorem 2.1.** Let  $n \in \mathbb{Z}_{>0}$ . Then  $\mathbb{Z}/n\mathbb{Z}$  is a field if and only if  $n$  is prime.

*Proof.* See Howie. □

**Remark.** If  $n = 0$ , then  $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ .

**Theorem 2.2.** Let  $\varphi : R \rightarrow S$  be a surjective homomorphism with kernel  $K$ . Then there is an isomorphism  $\alpha : R/K \rightarrow S$  such that the following diagram commutes (i.e.  $\varphi = \alpha \circ \theta_K$ ):

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \theta_K \downarrow & \nearrow \alpha & \\ R/K & & \end{array}$$

*Proof.* See Howie. But the general idea is to define  $\alpha : R/K \rightarrow S$  by  $\alpha(a + K) = \varphi(a)$ . Then need to check that  $\alpha$  is well-defined and an isomorphism.  $\square$

## 2.2 Field of Fractions

The motivating question is: How do we get from  $\mathbb{Z}$  to  $\mathbb{Q}$ ? Recall that

$$\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\},$$

where  $a/c = b/d$  if  $ad = bc$ . We add and multiply fractions by

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

How do we do this more generally (construct a field out of an arbitrary integral domain)?

**Definition 2.5** (Field of fractions of a domain). Let  $D$  be an integral domain and

$$P = D \times (D \setminus \{0\}) = \{(a, b) \mid a, b \in D, b \neq 0\}$$

Define an equivalence relation  $\equiv$  on  $P$  by  $(a, b) \equiv (a', b')$  if  $ab' = a'b$ . Then the *field of fractions* of  $D$  is

$$Q(D) = P/\equiv.$$

We denote the equivalence class  $[a, b]$  by  $a/b$ , i.e.  $a/b = c/d$  if  $ad = bc$ . We define addition and multiplication on  $Q(D)$  by

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

**Exercise 2.5.** Do the following:

1. Check that  $\equiv$  is an equivalence relation.
2. Check that these operations are well-defined.
3. Check that  $Q(D)$  is a commutative ring with unity.
  - The zero element is  $0/b$  for  $b \neq 0$ .
  - The unity element is  $a/a$  for  $a \neq 0$ .
  - The negative of  $a/b$  is  $(-a)/b$  or equivalently  $a/(-b)$ .
  - The multiplicative inverse of  $a/b$  is  $b/a$  for  $a, b \neq 0$ .
4. Complete the previous exercise and check that  $Q(D)$  is a field.



**Exercise 2.6.** The map  $\varphi : D \rightarrow Q(D)$  defined by  $\varphi(a) = a/1$  is a monomorphism. In particular, the field of fractions  $Q(D)$  contains  $D$  as a subring and  $Q(D)$  is the smallest field containing  $D$ , in the sense that if  $K$  is a field with the property that there exists a monomorphism  $\theta : D \rightarrow K$ , then there exists a monomorphism  $\psi : Q(D) \rightarrow K$  such that the following diagram commutes:

$$\begin{array}{ccc} D & \xrightarrow{\theta} & K \\ \varphi \downarrow & \nearrow \psi & \\ Q(D) & & \end{array}$$

## 2.3 The Characteristic of a Field

Note that for  $a \in R$ , we might write  $a + a$  as  $2a$  and  $a + a + \cdots + a$  ( $n$  times) as  $na$ . Furthermore,  $0a = 0_R$  and  $(-n)a = n(-a)$  for  $n \in \mathbb{Z}_{>0}$ . Thus  $na$  has meaning for all  $n \in \mathbb{Z}$ .<sup>1</sup>

**Exercise 2.7.** For  $a, b \in R$  and  $m, n \in \mathbb{Z}$ , we have  $(ma)(nb) = (mn)(ab)$ .

**Definition 2.6** (Characteristic of a ring). For an arbitrary ring  $R$ , there are two possibilities:

1.  $m1_R$  for  $m \in \mathbb{Z}$  are all distinct. In this case, we say that  $R$  has *characteristic 0*.
2. There exists  $m, n \in \mathbb{N}$  such that  $m1_R = (m+n)1_R$ . In this case, we say that  $R$  has *characteristic  $n$* , where  $n$  is the least positive  $n$  for which this property holds.

We denote the characteristic of  $R$  by  $\text{char } R$ . If  $\text{char } R = n$ , then  $na = 0_R$  for all  $a \in R$  since

$$na = (n1_R)a = 0a = 0.$$

**Example 2.6.1.** We have  $\text{char } \mathbb{Z}/n\mathbb{Z} = n$ .

**Theorem 2.3.** The characteristic of a field is either 0 or a prime.

*Proof.* Let  $K$  be a field and suppose  $\text{char } K = n \neq 0$  and  $n$  is not prime. Then we can write  $n = rs$  where  $1 < r, s < n$ . The minimal property of  $n$  implies that  $r1_K \neq 0$  and  $s1_K \neq 0$ . But then

$$r1_K \cdot s1_K = rs1_K = n1_K = 0,$$

which is impossible since  $K$  is a field and thus has no zero divisors. □

**Remark.** Note the following:

1. If  $K$  is a field with  $\text{char } K = 0$ , then  $K$  has a subring isomorphic to  $\mathbb{Z}$ , i.e. elements of the form  $n1_K$  for  $n \in \mathbb{Z}$ , and  $K$  has a subfield isomorphic to  $\mathbb{Q}$ , i.e.

$$P(K) = \{m1_K/n1_K \mid m, n \in \mathbb{Z}, n \neq 0\}.$$

This is the *prime subfield* of  $K$ , and any subfield of  $K$  must contain  $P(K)$ .

2. If  $K$  is a field with  $\text{char } K = p$ , then the prime subfield of  $K$  is

$$P(K) = \{1_K, 2 \cdot 1_K, \dots, (p-1) \cdot 1_K\},$$

which is isomorphic to  $\mathbb{Z}/p\mathbb{Z}$ .

---

<sup>1</sup>This is saying that any abelian group is naturally a *module* over the integers  $\mathbb{Z}$ .

**Remark.** In other words, every field of characteristic 0 is an *extension* of  $\mathbb{Q}$  (contains  $\mathbb{Q}$  as a subfield), and every field of characteristic  $p$  is an *extension* of  $\mathbb{Z}/p\mathbb{Z}$  (contains  $\mathbb{Z}/p\mathbb{Z}$  as a subfield).

**Remark.** If  $\text{char } K = 0$ , then writing  $a/n1_K$  as  $a/n$  is fine. But if  $\text{char } K = p$ , then  $a/n$  does not make sense when  $p|n$  (since  $p \cdot 1_K = 0$ ).

**Theorem 2.4.** *If  $K$  is a field with  $\text{char } K = p$ , then for all  $x, y \in K$ ,  $(x + y)^p = x^p + y^p$ .*

*Proof.* See Howie. Uses the binomial theorem. □

## 2.4 Polynomials

Let  $R$  be a ring, then we have the polynomial ring over  $R$

$$R[X] = \{a_0 + a_1X + \cdots + a_nX^n \mid a_i \in R, n \in \mathbb{N}\}.$$

If  $f \in R[X]$ , then it has *degree*  $n$  if the last nonzero element in the sequence  $\{a_0, a_1, \dots\}$  is  $a_n$ , denoted  $\partial f = n$ . By convention, the zero polynomial has degree  $-\infty$ . The coefficient  $a_n$  is called the *leading coefficient*, and if  $a_n = 1$ , then  $f$  is *monic*. Addition and multiplication work as expected:

$$(a_0 + a_1X + \cdots + a_mX^m) + (b_0 + b_1X + \cdots + b_nX^n) = (a_0 + b_0) + (a_1 + b_1)X + \dots$$

and

$$(a_0 + a_1X + \cdots + a_mX^m)(b_0 + b_1X + \cdots + b_nX^n) = c_0 + c_1X + \dots$$

where

$$c_k = \sum_{i+j=k}^k a_i b_j.$$

The ground ring  $R$  sits inside of the polynomial ring  $R[X]$ . Take the monomorphism  $\theta : R \rightarrow R[X]$  by  $\theta(a) = a$ , i.e. an element  $a$  maps to the constant polynomial  $a$ .

**Theorem 2.5.** *Let  $D$  be an integral domain. Then*

1.  $D[X]$  is an integral domain.
2. If  $p, q \in D[X]$ , then  $\partial(p + q) \leq \max(\partial p, \partial q)$ .
3. If  $p, q \in D[X]$ , then  $\partial(pq) = \partial p + \partial q$ .
4. The group of units of  $D[X]$  coincides with the group of units of  $D$ .

*Proof.* Statements (2) and (3) are left as exercises.

(1) We need to show that  $D[X]$  has no zero divisors. For this, suppose that  $p, q$  are nonzero polynomials with leading coefficients  $a_m$  and  $b_n$  respectively. Then the leading coefficient of  $pq$  is  $a_m b_n$ , which is nonzero since  $D$  is an integral domain and thus has no zero divisors. So  $pq$  is nonzero.

(4) Let  $p, q \in D[X]$  and suppose  $pq = 1$ . Since  $\partial(pq) = \partial(1) = 0$ , we must have  $\partial p = \partial q = 0$ . Thus  $p, q \in D$  and  $pq = 1$  if and only if  $p$  and  $q$  are in the group of units of  $D$ . □

Since  $D[X]$  is a domain, we can consider polynomials in the variable  $Y$  with coefficients in  $D[X]$ :

$$D[X, Y] = (D[X])[Y].$$

We can repeat this to get polynomials in  $n$  variables:  $D[X_1, X_2, \dots, X_n]$ , which is an integral domain.

# Lecture 3

## Jan. 17 — Irreducible Polynomials

### 3.1 Principal Ideal Domains and Irreducible Polynomials

**Definition 3.1.** The field of fractions of  $D[X]$  consists of *rational forms*

$$\frac{a_0 + a_1X + \cdots + a_mX^m}{b_0 + b_1X + \cdots + b_nX^n}$$

where  $b_0 + b_1X + \cdots + b_nX^n \neq 0$ , denoted by  $D(X)$ .

**Definition 3.2.** A domain  $D$  is a *principal ideal domain* (PID) if all of its ideals are principal.<sup>1</sup>

**Example 3.2.1.** The integers  $\mathbb{Z}$  is a PID, since every ideal is of the form  $\langle n \rangle$ .

**Definition 3.3.** A non-zero, non-unit element  $p$  in a domain  $D$  is *irreducible* if it has no proper factors.

**Definition 3.4.** A domain  $D$  is a *unique factorization domain* (UFD) if every non-unit  $a \neq 0$  in  $D$  has an essentially unique<sup>2</sup> factorization into irreducible elements.

**Example 3.4.1.** Again  $\mathbb{Z}$  is a UFD, e.g.  $12 = 2 \cdot 2 \cdot 3 = (-2) \cdot 2 \cdot (-3)$ .

**Theorem 3.1.** *Every PID is a UFD.*

*Proof.* See Howie. □

**Theorem 3.2.** *If  $K$  is a field, then  $K[X]$  is a PID.*

*Proof.* See Howie. □

**Theorem 3.3.** *Let  $p$  be an element in a PID  $D$ . Then the following are equivalent:*

1.  $p$  is irreducible.
2.  $\langle p \rangle$  is maximal.
3.  $D/\langle p \rangle$  is a field.

*In particular if  $f \in K[X]$ , then  $K[X]/\langle f \rangle$  is a field if and only if  $f$  is irreducible.*

*Proof.* See Howie. □

---

<sup>1</sup>Recall that a principal ideal is one generated by a single element.

<sup>2</sup>As in, unique up to use of associates or adding in units.

**Definition 3.5.** Let  $D$  be a domain and  $\alpha \in D$ . Let  $\sigma_\alpha : D[X] \rightarrow D$  defined by

$$\sigma_\alpha(a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

Note that we often write  $\sigma_\alpha(f)$  as  $f(\alpha)$ . If  $f(\alpha) = 0$ , we say  $\alpha$  is a *root* of  $f$ , or a *zero*.

**Exercise 3.1.** Check that  $\sigma_\alpha$  is a homomorphism.

**Theorem 3.4.** Let  $K$  be a field,  $\beta \in K$  and  $f$  a non-zero polynomial in  $K[X]$ . Then  $\beta$  is a root of  $f$  if and only if  $X - \beta \mid f$ .

*Proof.* See Howie. □

**Example 3.5.1.** We have  $X^2 + 1$  in  $\mathbb{R}[X]$  is irreducible, so  $\mathbb{R}[X]/\langle X^2 + 1 \rangle$  is a field. In fact this field is isomorphic to the complex numbers  $\mathbb{C}$ .

**Exercise 3.2.** Do the following:

1. Show that  $\varphi : \mathbb{R}[X] \rightarrow \mathbb{C}$  given by

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1i + \cdots + a_ni^n$$

is a surjective homomorphism.<sup>3</sup>

2. Show that  $\ker \varphi = \langle X^2 + 1 \rangle$ .

So by the first isomorphism theorem we can conclude that  $\mathbb{R}[X]/\langle X^2 + 1 \rangle = \mathbb{R}/\ker \varphi \cong \varphi(\mathbb{R}[X]) = \mathbb{C}$ .

**Theorem 3.5.** Let  $K$  be a field and  $g \in K[X]$  an irreducible polynomial. Then  $K[X]/\langle g \rangle$  is a field containing  $K$  up to isomorphism.

*Proof.* Since  $g$  is irreducible,  $K[X]/\langle g \rangle$  is a field. Now define  $\varphi : K \rightarrow K[X]/\langle g \rangle$  by

$$\varphi(a) = a + \langle g \rangle.$$

(Left as an exercise to check that  $\varphi$  is a homomorphism.) We need to show that  $\varphi$  is injective. For this, take  $a, b \in K$ . If  $a + \langle g \rangle = b + \langle g \rangle$ , then  $a - b \in \langle g \rangle$ . But  $K$  is a field, so this happens precisely when  $a = b$ . Thus  $\varphi$  embeds  $K$  into  $K[X]/\langle g \rangle$ , as desired. □

## 3.2 Irreducible Polynomials over $\mathbb{C}$ , $\mathbb{R}$ , $\mathbb{Q}$ , and $\mathbb{Z}$

Our goal now is to study irreducible polynomials. Note that linear polynomials are irreducible, and recall that every polynomial in  $\mathbb{C}$  factorizes, essentially uniquely, into linear factors. Furthermore, complex roots of real polynomials come in conjugate pairs, hence

$$g = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{R}[X]$$

factors as

$$g = a_n(X - \beta_1) \cdots (X - \beta_r)(X - \gamma_1)(X - \bar{\gamma}_1) \cdots (X - \gamma_s)(X - \bar{\gamma}_s)$$

---

<sup>3</sup>Note that there's some technicality about this  $\varphi$  not being a  $\sigma_\alpha$  since we defined  $\sigma_\alpha$  for  $\alpha$  in the base domain, and  $i$  is kind of somewhere else.

in  $\mathbb{C}[X]$ , where  $\beta_1, \dots, \beta_r \in \mathbb{R}$  and  $\gamma_1, \dots, \gamma_s \in \mathbb{C} \setminus \mathbb{R}$  and  $r + 2s = n$ . Thus over  $\mathbb{R}[X]$ ,  $g$  factors as

$$g = a_n(X - \beta_1) \dots (X - \beta_r)(X^2 - (\gamma_1 + \bar{\gamma}_1)X + \gamma_1\bar{\gamma}_1) \dots (X^2 - (\gamma_s + \bar{\gamma}_s)X + \gamma_s\bar{\gamma}_s)$$

in  $\mathbb{R}[X]$ , where the quadratic factors are irreducible in  $\mathbb{R}[X]$ .

**Exercise 3.3.** A quadratic  $aX^2 + bX + c \in \mathbb{R}[X]$  is irreducible if and only if its discriminant  $b^2 - 4ac < 0$ .

Now we have pretty much characterized irreducible polynomials in  $\mathbb{R}[X]$ . But what about  $\mathbb{Q}[X]$ ?

**Theorem 3.6.** Let  $g = a_0 + a_1X + a_2X^2 \in \mathbb{Q}[X]$ . Then

1. If  $g$  is irreducible over  $\mathbb{R}$ , then it is irreducible over  $\mathbb{Q}$ .
2. If  $g = a_2(X - \beta_1)(X - \beta_2)$  with  $\beta_1, \beta_2 \in \mathbb{R}$ , then  $g$  is irreducible in  $\mathbb{Q}[X]$  if and only if  $\beta_1$  and  $\beta_2$  are irrational.

*Proof.* (1) We show the contrapositive. If  $g$  factors as

$$g = a_2(X - q_1)(X - q_2) \in \mathbb{Q}[X],$$

then  $g$  also factors in  $\mathbb{R}[X]$ .

(2) If  $\beta_1$  and  $\beta_2$  are rational, then  $g$  factors in  $\mathbb{Q}[X]$  and is thus not irreducible. For the other direction, if  $\beta_1$  and  $\beta_2$  are irrational, then  $g = a_2(X - \beta_1)(X - \beta_2)$  is the only factorization in  $\mathbb{R}[X]$  since  $\mathbb{R}[X]$  is a UFD, so there is no factorization in  $\mathbb{Q}[X]$  into linear factors.  $\square$

**Example 3.5.2.** Are the following polynomials irreducible in  $\mathbb{R}[X]$ ? In  $\mathbb{Q}[X]$ ?

1.  $X^2 + X + 1$  is irreducible over  $\mathbb{R}$  and  $\mathbb{Q}$  since  $b^2 - 4ac = -3$ .
2.  $X^2 - X - 1$  has roots  $(-1 \pm \sqrt{5})/2$ , so it factors over  $\mathbb{R}$  but is irreducible over  $\mathbb{Q}$ .
3.  $X^2 + X - 2$  factors as  $(X + 2)(X - 1)$  over  $\mathbb{R}$  and  $\mathbb{Q}$ .

Now that we have studied irreducible polynomials in  $\mathbb{R}[X]$  and  $\mathbb{Q}[X]$ , can a polynomial in  $\mathbb{Z}[X]$  be irreducible over  $\mathbb{Z}$  but not  $\mathbb{Q}$ ? The answer is no!

**Theorem 3.7** (Gauss's lemma). Let  $f$  be a polynomial in  $\mathbb{Z}[X]$ , irreducible over  $\mathbb{Z}$ . Then  $f$  is irreducible over  $\mathbb{Q}$ .

*Proof.* For sake of contradiction, suppose  $f = gh$  with  $g, h \in \mathbb{Q}[X]$  and  $\partial g, \partial h < \partial f$ . Then there exists  $n \in \mathbb{Z}_{>0}$  such that  $nf = g'h'$  where  $g', h' \in \mathbb{Z}[X]$ . Let  $n$  be the smallest positive integer with this property. Let

$$\begin{aligned} g' &= a_0 + a_1X + \dots + a_kX^k \\ h' &= b_0 + b_1X + \dots + b_lX^l. \end{aligned}$$

If  $n = 1$ , then  $g' = g$  and  $h' = h$ , a contradiction. Now  $n \geq 1$ , so let  $p$  be a prime factor of  $n$ .<sup>4</sup> Without loss of generality, assume  $p$  divides  $g'$ , i.e.  $g' = pg''$  where  $g'' \in \mathbb{Z}[X]$ . Then

$$\frac{n}{p}f = g''h',$$

contradicting the minimality of  $n$ . Hence  $f$  cannot be factored over  $\mathbb{Q}$ .  $\square$

<sup>4</sup>Lemma: Either  $p$  divides all the coefficients of  $g'$  or  $p$  divides all the coefficients of  $h'$ . Proof left as an exercise.

**Example 3.5.3.** Show that  $g = X^3 + 2X^2 + 4X - 6$  is irreducible over  $\mathbb{Q}$ .

*Proof.* If  $g$  factors over  $\mathbb{Q}$ , it factors over  $\mathbb{Z}$  and at least one factor must be linear, i.e.

$$g = X^3 + 2X^2 + 4X - 6 = (X - a)(X^2 + bX + c)$$

where  $a, b, c \in \mathbb{Z}$ . We must have  $ac = 6$ , so  $a \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$  and  $g(a) = 0$ . We can check this:

$a$	1	-1	2	-2	3	-3	-6	6
$g(a)$	1	-9	1	-10	51	-27	306	-174

Hence  $g$  is irreducible over  $\mathbb{Z}$  and thus also irreducible over  $\mathbb{Q}$ . □

We could do this trick since the degree was 3, forcing a linear factor. What about degrees higher than 3?

**Theorem 3.8** (Eisenstein's criterion). *Let  $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ . Suppose there exists a prime  $p$  such that*

1.  $p \nmid a_n$ ,
2.  $p \mid a_i$  for  $i = 0, \dots, n-1$ ,
3.  $p^2 \nmid a_0$ .

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

*Proof.* By Gauss's lemma, it suffices to show that  $f$  is irreducible over  $\mathbb{Z}$ . Suppose for sake of contradiction that  $f = gh$  for

$$g = b_0 + b_1X + \cdots + b_rX^r \quad \text{and} \quad h = c_0 + c_1X + \cdots + c_sX^s,$$

$r, s < n$ , and  $r + s = n$ . Note that  $a_0 = b_0c_0$ , so  $p \mid a_0$  from (2) implies that  $p \mid b_0$  or  $p \mid c_0$ . Since  $p^2 \nmid a_0$ , it cannot be both. Without loss of generality, assume  $p \mid b_0$  and  $p \nmid c_0$ . Now suppose inductively that  $p$  divides  $b_0, \dots, b_{k-1}$  where  $1 \leq k \leq r$ . Then

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$$

and since  $p$  divides  $a_k, b_0c_k, b_1c_{k-1}, \dots, b_{k-1}c_1$ , it follows that  $p \mid b_kc_0$ . Since  $p \nmid c_0$  by assumption, we must have  $p \mid b_k$ . Thus  $p \mid b_r$  and since  $a_n = b_rc_s$ , we have  $p \mid a_n$ , contradicting (1). Hence  $f$  is irreducible. □

**Example 3.5.4.** The polynomial

$$X^5 + 2X^3 + \frac{8}{7}X^2 - \frac{4}{7}X + \frac{2}{7}$$

is irreducible over  $\mathbb{Q}$ .

*Proof.* Multiply by 7 and take the integer polynomial  $7X^5 + 14X^3 + 8X^2 - 4X + 2$ . Taking  $p = 2$  satisfies Eisenstein's criterion, so this polynomial is irreducible over  $\mathbb{Z}$  and thus also irreducible over  $\mathbb{Q}$ . □

**Example 3.5.5.** If  $p > 2$  is prime, then show that

$$f = 1 + X + X^2 + \cdots + X^{p-1}$$

is irreducible over  $\mathbb{Q}$ .

*Proof.* First observe that

$$f = \frac{X^p - 1}{X - 1}.$$

Let  $g(X) = f(X + 1)$ . Then

$$\begin{aligned} g(X) &= \frac{(X + 1)^p - 1}{(X + 1) - 1} = \frac{1}{X}((X + 1)^p - 1) = \frac{1}{X} \sum_{i=0}^p \binom{p}{i} X^{p-i} - 1 \\ &= \frac{1}{X} \sum_{i=0}^{p-1} \binom{p}{i} X^{p-i} = \sum_{i=0}^{p-1} \binom{p}{i} X^{p-i-1}. \end{aligned}$$

Note that  $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$  are all divisible by  $p$ , so  $g$  is irreducible by Eisenstein's criterion. Now if  $f$  factors as  $f = uv$ , then  $g(X) = u(X + 1)v(X + 1)$ , which is a contradiction since  $g$  is irreducible.  $\square$

# Lecture 4

## Jan. 22 — Field Extensions

### 4.1 More on Irreducibility

The following excerpt is from Howie:

Another device for determining irreducibility over  $\mathbb{Z}$  (and consequently over  $\mathbb{Q}$ ) is to map the polynomial onto  $\mathbb{Z}_p[X]$  for some suitably chosen prime  $p$ . Let  $g = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ , and let  $p$  be a prime not dividing  $a_n$ . For each  $i$  in  $\{0, 1, \dots, n\}$ , let  $\bar{a}_i$  denote the residue class  $a_i + \langle p \rangle$  in the field  $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$ , and write the polynomial  $\bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_nX^n$  as  $\bar{g}$ . Our choice of  $p$  ensures that  $\partial \bar{g} = n$ . Suppose that  $g = uv$ , with  $\partial u, \partial v < \partial g$  and  $\partial u + \partial v = \partial g$ . Then  $\bar{g} = \bar{u}\bar{v}$ . If we can show that  $\bar{g}$  is irreducible in  $\mathbb{Z}_p[X]$ , then we have a contradiction, and we deduce that  $g$  is irreducible. The advantage of transferring the problem from  $\mathbb{Z}[X]$  to  $\mathbb{Z}_p[X]$  is that  $\mathbb{Z}_p$  is finite, and the verification of irreducibility is a matter of checking a finite number of cases.

**Example 4.0.1.** Show that

$$g = 7X^4 + 10X^3 - 2X^2 + 4X - 5$$

is irreducible over  $\mathbb{Q}$ .

*Proof.* Let  $p = 3$  and

$$\bar{g} = X^4 + X^3 + X^2 + 1$$

This has no linear factors since

$$\bar{g}(0) = 1, \quad \bar{g}(1) = 2, \quad \bar{g}(-1) = 1.$$

So suppose

$$\bar{g} = X^4 + X^3 + X^2 + X + 1 = (X^2 + aX + b)(X^2 + cX + d)$$

in  $\mathbb{Z}_3[x]$ . Then for some  $a, b, c, d \in \mathbb{Z}_3 = \{-1, 0, 1\}$ , we have

$$\begin{cases} X^3 & a + c = 1 \\ X^2 & b + ac + d = 1 \\ X & ad + bc = 1 \\ 1 & bd = 1 \end{cases}$$

The first case is if  $b = d = 1$ , but this implies  $ac = -1$ , so  $a = \pm 1$  and  $c = \mp 1$ . But  $a + c = 1$ , so this cannot happen. The second case is if  $b = d = -1$ . This implies that  $ac = 0$  and  $a + c = 1$ . So if  $a = 0$ , then  $c = 1$ , so  $1 = ad + bc = b$ , which is a contradiction with  $b = -1$ . If  $c = 0$ , then  $1 = ad + bc = d$ ,



which is a contradiction with  $d = -1$ . Thus  $\bar{g}$  is irreducible in  $\mathbb{Z}_3[x]$ , so  $g$  is irreducible in  $\mathbb{Z}[x]$ , and by Gauss's lemma,  $g$  is irreducible in  $\mathbb{Q}[x]$ .  $\square$

**Remark.** If we had tried  $p = 2$ , then we have  $\bar{g} = x^4 + 1 \in \mathbb{Z}_2[x]$ , which is not in fact irreducible since

$$\bar{g} = x^4 + 1 = (x + 1)^4 \in \mathbb{Z}_2[x].$$

## 4.2 Field Extensions

**Definition 4.1.** Let  $K, L$  be fields and  $\varphi : K \rightarrow L$  an injective homomorphism. Then  $L$  is a *field extension* of  $K$ , denoted  $L : K$ .

**Example 4.1.1.** We have  $\mathbb{C} : \mathbb{R}$  is a field extension.

**Definition 4.2.** Recall that  $V$  is a  $K$ -vector space if

1.  $V$  is an abelian group under  $+$ ,
2. For  $a, b \in K$  and  $x, y \in V$ , we have

$$(i). a(x + y) = ax + ay, \quad (ii). (a + b)x = ax + bx, \quad (iii). (ab)x = a(bx), \quad (iv). 1x = x.$$

**Remark.** If  $L : K$  is a field extension, then  $L$  is a vector space over  $K$ .

**Definition 4.3.** A *basis* for a vector space is a linearly independent spanning set.

**Example 4.3.1.** The complex numbers  $\mathbb{C}$  is a  $\mathbb{R}$ -vector space with basis  $\{1, i\}$ . Bases are not unique, since  $\{1 + i, 1 - i\}$  is another basis for  $\mathbb{C}$ .

**Example 4.3.2.** If there is a vector space that we know to be a field, then it is automatically a field extension of its ground field.

**Definition 4.4.** The *dimension* of  $L$  is the cardinality of a basis for  $L : K$ .<sup>1</sup> The dimension is also called the *degree* of  $L : K$ , denoted  $[L : K]$ . We say that  $L$  is a *finite extension* if  $[L : K]$  is finite, and an *infinite extension* otherwise.

**Example 4.4.1.** We have  $[\mathbb{C} : \mathbb{R}] = 2$ , which is finite. On the other hand,  $\mathbb{R} : \mathbb{Q}$  is an infinite extension.

**Theorem 4.1.** Let  $L : K$  be a field extension. Then  $L = K$  if and only if  $[L : K] = 1$ .

*Proof.* ( $\Rightarrow$ ) If  $L = K$ , then  $\{1\}$  is a basis for  $L : K$ , and thus  $[L : K] = 1$ .

( $\Leftarrow$ ) If  $[L : K] = 1$ , then  $\{x\}$  is a basis for  $L : K$  for some  $x \in L$ . Then there exists some  $a \in K$  such that  $1 = ax$ , so  $x = a^{-1} \in K$ . For every  $y \in L$ , there exists  $b \in K$  such that  $y = bx$ . But then

$$y = bx = b(a^{-1}) \in K,$$

so  $y \in K$  as well by closure. Thus  $L = K$  as desired.  $\square$

**Remark.** Let  $L : K$  and  $M : L$  be field extensions with

$$K \xrightarrow{\alpha} L \xrightarrow{\beta} M$$

---

<sup>1</sup>Note that this is well-defined since any two bases of  $L$  have the same length.

Then  $M : K$  is also a field extension.

**Theorem 4.2.** *For field extensions  $L : K$  and  $M : L$ , we have  $[M : L][L : K] = [M : K]$ .*

*Proof.* Suppose  $\{a_1, a_2, \dots, a_r\}$  is a linearly independent subset of  $M$  over  $L$  and  $\{b_1, b_2, \dots, b_s\}$  is a linearly independent subset of  $L$  over  $K$ . Now we claim that

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

is a linearly independent subset of  $M$  over  $K$ . To see this, suppose

$$\sum_{i=1}^r \sum_{j=1}^s \lambda_{ij} a_i b_j = 0$$

for some  $\lambda_{ij} \in K$ . We can rewrite this as

$$\sum_{i=1}^r \left( \sum_{j=1}^s \lambda_{ij} b_j \right) a_i = 0.$$

Since the  $a_i$  are linearly independent over  $L$ , it follows that

$$\sum_{j=1}^s \lambda_{ij} b_j = 0$$

for each  $i = 1, \dots, r$ . Since the  $b_j$  are linearly independent over  $K$ , it follows that  $\lambda_{ij} = 0$  for each  $i, j$ , which proves the claim. Returning to the main proof, if  $[M : L]$  or  $[L : K]$  is infinite, then  $r$  or  $s$  can be made arbitrarily large, so

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

can also be made arbitrarily large, and hence  $[M : K]$  is infinite. Now suppose  $[M : L] = r < \infty$  and  $[L : K] = s < \infty$ . Let  $\{a_1, a_2, \dots, a_r\}$  be a basis for  $M : L$  and  $\{b_1, b_2, \dots, b_s\}$  be a basis for  $L : K$ . We will show that

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

is a basis for  $M : K$ . Since we already showed that  $\{a_i b_j\}$  is linearly independent, it only remains to show that they span  $M$  over  $K$ . For each  $z \in M$ , there exist  $\lambda_1, \dots, \lambda_r \in L$  such that

$$z = \sum_{i=1}^r \lambda_i a_i.$$

Then for each  $\lambda_i \in L$ , there exist  $\mu_{i1}, \dots, \mu_{is} \in K$  such that

$$\lambda_i = \sum_{j=1}^s \mu_{ij} b_j.$$

Combining this yields

$$z = \sum_{i=1}^r \sum_{j=1}^s \mu_{ij} a_i b_j$$

as desired, which finishes the proof. □

**Example 4.4.2.** Consider  $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ .

**Exercise 4.1.** Show that  $\mathbb{Q}[\sqrt{2}]$  is a field. (Hint:  $1/(a + b\sqrt{2}) = (a - b\sqrt{2})/(a^2 - 2b^2)$ .)

**Definition 4.5.** Let  $K$  be a subfield of  $L$  and  $S$  a subset of  $L$ . The *subfield of  $L$  generated over  $K$  by  $S$* , denoted  $K(S)$ , is the intersection of all subfields of  $L$  containing  $K \cup S$ . If  $S = \{\alpha_1, \dots, \alpha_n\}$  is finite, we write  $K(\alpha_1, \dots, \alpha_n)$ .

**Theorem 4.3.** Let  $E$  be the elements in  $L$  that can be expressed as quotients of finite  $K$ -linear combinations of finite products of elements in  $S$ . Then  $K(S) = E$ .

*Proof.* To see that  $K(S) \subseteq E$ , simply check that  $E$  is a subfield of  $L$  containing  $K \cup S$ .

For  $E \subseteq K(S)$ , note that any subfield of  $L$  containing  $K$  and  $S$  must contain all finite products of elements in  $S$ , all linear combinations of such products, and all quotients of such linear combinations. This is precisely what it means to have  $E \subseteq K(S)$ .  $\square$

**Definition 4.6.** A *simple extension* of  $K$  is  $K(\alpha)$ , i.e.  $S$  has a single element  $\alpha \notin K$ .

**Example 4.6.1.** The previous example  $\mathbb{Q}(\sqrt{2})$  is a simple extension.

**Theorem 4.4.** Let  $L$  be a field,  $K$  a subfield, and  $\alpha \in L$ . Then either

1.  $K(\alpha)$  is isomorphic to  $K(X)$ , the field of rational forms with coefficients in  $K$ ,
2. or there exists a unique monic polynomial  $m \in K[X]$  with the property that for all  $f \in K[X]$ ,
  - (a)  $f(\alpha) = 0$  if and only if  $m \mid f$ ,
  - (b) the field  $K(\alpha)$  coincides with  $K[\alpha]$ , the ring of all polynomials in  $\alpha$  with coefficients in  $K$ ,
  - (c) and  $[K[\alpha] : K] = \partial m$ .

*Proof.* Suppose there does not exist nonzero  $f \in K[X]$  such that  $f(\alpha) = 0$ . Then there exists a map  $\varphi : K(X) \rightarrow K(\alpha)$  with  $f/g \mapsto f(\alpha)/g(\alpha)$ , which is defined since  $g(\alpha) = 0$  only if  $g$  is the zero polynomial. Note that  $\varphi$  is a surjective homomorphism,<sup>2</sup> which one can check as an exercise. Now we show that  $\varphi$  is also injective. To see this, suppose

$$\varphi(f/g) = \varphi(p/q),$$

which happens if and only if

$$f(\alpha)q(\alpha) - p(\alpha)g(\alpha) = 0.$$

in  $L$ . This happens if and only if  $fq - pg = 0$  in  $K[X]$ , which happens if and only if  $f/g = p/q$  in  $K(X)$ . This completes the first case of the theorem.

Now suppose there exists nonzero  $g \in K[X]$  such that  $g(\alpha) = 0$ . Furthermore, suppose  $g$  is a polynomial of least degree with this property. Let  $a$  be the leading coefficient of  $g$ , and let  $m = g/a$ , so that  $m$  is monic and  $m(\alpha) = 0$  still. The reverse implication in (2a) is clear. For the forwards implication in (2a), note that by division with remainder for polynomials over a field, we can write

$$f = qm + r,$$

where  $\partial r < \partial m$ . By the minimality of  $\partial m$ , we must have  $r = 0$ , so  $m \mid f$ . For the uniqueness of  $m$ , suppose there exists  $m'$  with the same properties. Then  $m(\alpha) = m'(\alpha) = 0$ , so  $m \mid m'$  and  $m' \mid m$ , which

---

<sup>2</sup>Also check that  $\varphi$  is well-defined.

implies that  $m = m'$  since  $m$  and  $m'$  are monic. For the irreducibility of  $m$ , suppose for the sake of contradiction that  $m = pq$  with  $\partial p, \partial q < \partial m$ . Then  $m(\alpha) = p(\alpha)q(\alpha) = 0$ , so either  $p(\alpha) = 0$  or  $q(\alpha) = 0$ , which contradicts the minimality of  $\partial m$ .

Now we show (2b), which says that  $K(\alpha) = K[\alpha]$ . For this, consider  $p(\alpha)/q(\alpha) \in K(\alpha)$  for  $q(\alpha) \neq 0$ . Then  $m \nmid q$ , and since  $m$  is irreducible we have  $\gcd(m, q) = 1$ . Now by Theorem 2.15 of Howie (about gcd's in the Euclidean domain  $K[X]$ ), there exist polynomials  $a, b$  such that  $aq + bm = 1$ . Setting  $X = \alpha$  yields  $a(\alpha)q(\alpha) = 1$ , so

$$\frac{p(\alpha)}{q(\alpha)} = p(\alpha)a(\alpha) \in K[\alpha].$$

Thus  $K(\alpha) \subseteq K[\alpha]$ . Since we already know that  $K[\alpha] \subseteq K(\alpha)$ , we conclude that  $K(\alpha) = K[\alpha]$ .

Finally we show (2c), which claims that  $[K[\alpha] : K] = \partial m$ . For this, suppose  $\partial m = n$  and let

$$p(\alpha) \in K[\alpha] = K(\alpha).$$

Then  $p = qm + r$  where  $\partial r < \partial m = n$ . We have  $p(\alpha) = r(\alpha)$ , so if

$$r = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$$

for  $c_i \in K$ , then

$$p(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}.$$

So  $\{1, \alpha, \dots, \alpha^{n-1}\}$  is a spanning set for  $K[\alpha]$ . To see that  $\{1, \alpha, \dots, \alpha^{n-1}\}$  is also linearly independent, suppose there exists  $a_i \in K$  such that

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0.$$

Then  $a_0 = \cdots = a_{n-1} = 0$  since otherwise we would have a polynomial

$$p = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$$

with  $\partial p \leq n-1$  and  $p(\alpha) = 0$ , which is a contradiction with the minimality of  $\partial m = n$ . Thus  $\{1, \alpha, \dots, \alpha^{n-1}\}$  is a basis, and so  $[K[\alpha] : K] = n = \partial m$ .  $\square$

**Example 4.6.2.** Continuing the same example, note that

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \{a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + a_3\sqrt{2}^3 + \cdots + a_n\sqrt{2}^n \mid a_i \in \mathbb{Q}\},$$

which falls in the second case of the previous theorem.

**Remark.** We also have  $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[X]/\langle X^2 - 2 \rangle$ .

# Lecture 5

## Jan. 24 — Algebraic Extensions

### 5.1 Minimal Polynomials

**Remark.** The  $m$  in the previous theorem from last class is called the *minimal polynomial* of  $\alpha$ .

**Example 5.0.1.** Let

$$\mathbb{Q}[i\sqrt{3}] = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

Here  $m = X^2 + 3$ , so this is a degree 2 extension.

**Exercise 5.1.** Write  $1/(a + bi\sqrt{3})$  in the form  $c + di\sqrt{3}$ .

**Example 5.0.2.** Is  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  a simple extension? In fact it is! Note that certainly

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

For the reverse inclusion, observe that  $(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2}) = 1$ , so

$$1/(\sqrt{3} + \sqrt{2}) = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

From this we have

$$(\sqrt{3} + \sqrt{2}) + (\sqrt{3} - \sqrt{2}) = 2\sqrt{3},$$

which implies that  $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ . Similarly  $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ , so that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ . Now we can consider

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

First we have  $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ . Note that  $X^2 - 3$  is the minimal polynomial of  $\sqrt{3}$  over  $\mathbb{Q}[\sqrt{2}]$ , so  $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}]] = 2$ . Hence  $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4$  with basis  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ .<sup>1</sup> To find the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$ , we can compute

$$\begin{aligned}(\sqrt{2} + \sqrt{3})^2 &= 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \\(\sqrt{2} + \sqrt{3})^4 &= 25 + 20\sqrt{6} + 24 = 49 + 20\sqrt{6}.\end{aligned}$$

Thus  $X^4 - 10X^2 + 1$  is the minimal polynomial, since  $\alpha^4 - 10\alpha^2 + 1 = 0$  for  $\alpha = \sqrt{2} + \sqrt{3}$ .

---

<sup>1</sup>Since  $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\alpha]$  where  $\alpha = \sqrt{2} + \sqrt{3}$ , we have  $\{1, \alpha, \alpha^2, \alpha^3\}$  as another basis.

## 5.2 Algebraic Extensions

**Definition 5.1.** If  $\alpha$  has a minimal polynomial over  $K$ , we say  $\alpha$  is *algebraic* over  $K$ , and  $K[\alpha] = K(\alpha)$  is an *algebraic extension* of  $K$ . A complex number that is algebraic over  $\mathbb{Q}$  is called an *algebraic number*. Otherwise, if  $K(\alpha) \cong K(X)$ , then we say  $\alpha$  is *transcendental* over  $K$ . A transcendental number  $\alpha$  is a complex number that is transcendental over  $\mathbb{Q}$ .

**Example 5.1.1.** We have that  $\mathbb{Q}(i\sqrt{3})$ ,  $\mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q}(\sqrt{3})$ , and  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  are all simple algebraic extensions of  $\mathbb{Q}$ , whereas  $\mathbb{Q}(X)$  is a simple transcendental extension of  $\mathbb{Q}$ .

**Theorem 5.1.** Let  $K(\alpha)$  be a simple transcendental extension of  $K$ . Then  $[K(\alpha) : K] = \infty$ .

*Proof.* Observe that  $1, \alpha, \alpha^2, \dots$  are linearly independent over  $K$ , since no minimal polynomial exists.  $\square$

**Definition 5.2.** An extension  $L$  over  $K$  is an *algebraic extension* if any element of  $L$  is algebraic over  $K$ . Otherwise,  $L$  is a *transcendental extension*.

**Theorem 5.2.** Every finite extension is algebraic.

*Proof.* Let  $L : K$  be a finite extension and suppose for sake of contradiction that  $\alpha \in L$  is transcendental over  $K$ . Then  $1, \alpha, \alpha^2, \dots$  are linearly independent, contradicting the fact that  $L : K$  is finite.  $\square$

**Theorem 5.3.** Let  $L : K$  be a field extension and let  $\mathcal{A}(L)$  be the set of elements in  $L$  that are algebraic over  $K$ . Then  $\mathcal{A}(L)$  is a subfield of  $L$ .

*Proof.* See Howie. Just need to show the closure of algebraic elements under usual field operations.  $\square$

**Example 5.2.1.** For  $L = \mathbb{C}$  and  $K = \mathbb{Q}$ , we have that  $\mathcal{A}(\mathbb{C})$  is the field  $\mathbb{A}$  of algebraic numbers.

**Theorem 5.4.** The set of algebraic numbers  $\mathbb{A}$  is countable.

*Proof sketch.* Note that the set of monic polynomials of degree  $n$  with coefficients in  $\mathbb{Q}$  is countable, and each such polynomial has at most  $n$  distinct roots in  $\mathbb{C}$ . Hence the number of roots of such polynomials is countable. Then  $\mathbb{A}$  is the countable union of countable sets, so  $\mathbb{A}$  is countable.  $\square$

**Theorem 5.5.** Transcendental numbers exist.

*Proof.* Since  $|\mathbb{R}| = |\mathbb{C}| = 2^{\aleph_0} > \aleph_0$ , we must have that  $\mathbb{C} \setminus \mathbb{A}$  is nonempty.  $\square$

**Remark.** The above proof is very nonconstructive, what about actual examples of transcendental numbers? In 1844, Liouville constructed the following example:

$$\sum_{n=1}^{\infty} 10^{-n!},$$

which was shown to be transcendental. In 1873, Hermite showed that  $e$  is transcendental, and in 1882, Lindemann showed that  $\pi$  is transcendental.

**Theorem 5.6.** Let  $L : K$  be a field extension and  $\alpha_1, \dots, \alpha_n \in L$  have minimal polynomials  $m_1, \dots, m_n$ , respectively. Then  $[K(\alpha_1, \dots, \alpha_n) : K] \leq \partial m_1 \partial m_2 \dots \partial m_n$ .

*Proof.* See Howie. Uses induction and the fact that  $[M : L][L : K] = [M : K]$ .  $\square$

**Example 5.2.2.** Consider

$$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{6}] : \mathbb{Q}] = 2,$$

but  $[\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{6}] : \mathbb{Q}] = 4$ . So the bound in the previous theorem cannot be made into an equality.

**Proposition 5.1.** *A field extension  $L : K$  is finite if and only if for some  $n$ , there exist  $\alpha_1, \dots, \alpha_n$  algebraic over  $K$  such that  $L = K(\alpha_1, \dots, \alpha_n)$ .*

*Proof.* ( $\Leftarrow$ ) This is precisely the previous theorem.

( $\Rightarrow$ ) Suppose  $L : K$  is finite and  $\{\alpha_1, \dots, \alpha_n\}$  is a basis for  $L$  over  $K$ . Since finite extensions are algebraic, the  $\alpha_i$  must be algebraic.  $\square$

**Exercise 5.2.** Show that  $\varphi : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[X]/\langle X^2 - 2 \rangle$  defined by

$$a + b\sqrt{2} \mapsto a + bX + \langle X^2 - 2 \rangle$$

is an isomorphism.

**Theorem 5.7.** *Let  $K$  be a field and  $m$  a monic irreducible polynomial in  $K[X]$ . Then  $L = K[X]/\langle m \rangle$  is a simple algebraic extension  $K[\alpha]$  of  $K$ , and  $\alpha = X + \langle m \rangle$  has minimal polynomial  $m$  over  $K$ .*

*Proof.* First note that  $L$  is indeed a field since  $m$  is irreducible. Also  $L : K$  is indeed a field extension since  $\varphi : K \rightarrow L$  defined by  $a \mapsto a + \langle m \rangle$  is an injective homomorphism. Now let  $\alpha = X + \langle m \rangle$ . For

$$f = a_0 + a_1X + \dots + a_nX^n \in K[X],$$

we have

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \dots + a_n\alpha^n = a_0 + a_1(X + \langle m \rangle) + \dots + a_n(X + \langle m \rangle)^n \\ &= a_0 + a_1X + \dots + a_nX^n + \langle m \rangle = f + \langle m \rangle. \end{aligned}$$

So  $f(\alpha) = 0$  if and only if  $f \in \langle m \rangle$ , i.e.  $m|f$ . Hence  $m$  is the minimal polynomial of  $\alpha$ .  $\square$

# Lecture 6

## Jan. 29 — Geometric Constructions

### 6.1 $K$ -Isomorphisms

Recall from last class that  $L = K[X]/\langle m \rangle$  is a simple algebraic extension of  $K$ . In fact, we can show that the field  $L$  is essentially unique, i.e. unique up to isomorphism.

**Theorem 6.1.** *Let  $K$  be a field and  $f$  an irreducible polynomial in  $K[X]$ . If  $L$  and  $L'$  are two extensions of  $K$  containing roots  $\alpha$  and  $\alpha'$  respectively of  $f$ , then there exists an isomorphism  $K[\alpha] \rightarrow K[\alpha']$  which fixes every element of  $K$ .*

*Proof sketch.* Suppose

$$f = a_0 + a_1X + \cdots + a_nX^n.$$

Then  $K[\alpha]$  consists of polynomials of the form

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$

This is because multiplication in  $K[\alpha]$  relies on the observation that

$$\alpha^n = -\frac{1}{a_n}(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})$$

since  $\alpha$  is a root of  $f$ . Define  $\psi : K[\alpha] \rightarrow K[\alpha']$  by  $\psi(g(\alpha)) = g(\alpha')$  and show that  $\psi$  is an isomorphism.  $\square$

**Exercise 6.1.** Check the following from the previous proof:

1.  $\psi$  is one-to-one and onto,
2.  $\psi$  fixes  $K$ ,
3. and  $\psi$  is a homomorphism.

For the last point, the addition is mostly straightforward but the multiplication is more involved since we need to reduce when we get  $\alpha^n$  terms in the product.

**Definition 6.1.** A  $K$ -isomorphism is an isomorphism  $\varphi : L \rightarrow L'$  such that  $\varphi(x) = x$  for all  $x \in K$ .

**Example 6.1.1.** For  $\mathbb{C} : \mathbb{R}$ , the complex conjugation map  $\varphi : \mathbb{C} \rightarrow \mathbb{C}$  given by  $\varphi(a + bi) = a - bi$  is a  $\mathbb{R}$ -isomorphism.



**Example 6.1.2.** For  $\mathbb{Q}[X]/\langle X^2 + 3 \rangle : \mathbb{Q}$ ,<sup>1</sup> the map  $\psi : \mathbb{Q}[X]/\langle X^2 + 3 \rangle \rightarrow \mathbb{Q}[X]/\langle X^2 + 3 \rangle$  given by

$$\psi(a + bX + \langle X^2 + 3 \rangle) = a - bX + \langle X^2 + 3 \rangle$$

is a  $\mathbb{Q}$ -isomorphism. The analogous map  $\psi : \mathbb{Q}[i\sqrt{3}] \rightarrow \mathbb{Q}[i\sqrt{3}]$  given by  $\psi(a + bi\sqrt{3}) = a - bi\sqrt{3}$  also works, which we can view as a restriction of the complex conjugation map to  $\mathbb{Q}[i\sqrt{3}]$ .

## 6.2 Applications to Geometric Constructions

Consider the straightedge and compass Constructions from geometry. Let  $B_0$  be a set of points. Then we have the following operations:

1. (straightedge) Draw a straight line through any two points in  $B_0$ .
2. (compass) Draw a circle whose center is a point in  $B_0$  passing through another point in  $B_0$ .

Let  $C(B_0)$  be the set of points which are intersections of lines or circles obtained from  $B_0$  by (1) and (2). Let  $B_1 = B_0 \cup C(B_0)$ , and proceed inductively to get  $B_n = B_{n-1} \cup C(B_{n-1})$ .

**Definition 6.2.** A point is *constructible from  $B_0$*  if it belongs to  $B_n$  for some  $n$ . A point is *constructible* if it is constructible from  $\{O, I\}$  where  $O = (0, 0)$  and  $I = (1, 0)$ .

**Example 6.2.1.** To find the midpoint of the line segment  $OI$  from  $B_0 = \{O, I\}$ , we can do the following:

1. Draw a circle with center  $O$  passing through  $I$ .
2. Draw a circle with center  $I$  passing through  $O$ .
3. Mark points  $P$  and  $Q$  where these circles intersect. So  $B_1 \supseteq \{O, I, P, Q\}$ .
4. Draw a line connecting  $P$  and  $Q$ .
5. Draw a line connecting  $O$  and  $I$ .
6. Mark the point  $M$  where  $PQ$  and  $OI$  meet. So  $B_2 \supseteq \{O, I, P, Q, M\}$ .

Thus  $M$  is constructible from  $\{O, I\}$ .

The algebraic perspective is the following: Associate to  $B_i$  the subfield of  $\mathbb{R}$  generated by coordinates of points in  $B_i$ , i.e. view each coordinate of each point as an element and take the subfield generated.

**Example 6.2.2.** For  $B_0 = \{(0, 0), (1, 0)\}$ , we have  $\{0, 0, 1, 0\} \subseteq K_0 = \mathbb{Q}$  is the subfield of  $\mathbb{R}$  generated by the coordinates of  $B_0$ . Next take<sup>2</sup>

$$B_1 = \{O, I, P, Q\} = \{(0, 0), (1, 0), (1/2, \pm\sqrt{3}/2)\},$$

so that  $K_1 = \mathbb{Q}[\sqrt{3}]$  is the field generated by  $B_1$ . Then

$$B_2 = \{O, I, P, Q, M\} = \{(0, 0), (1, 0), (1/2, \pm\sqrt{3}/2), (1/2, 0)\},$$

and the field generated by  $B_2$  is still  $K_2 = \mathbb{Q}[\sqrt{3}]$ .

<sup>1</sup>Note that  $\mathbb{Q}[X]/\langle X^2 + 3 \rangle \cong \mathbb{Q}[i\sqrt{3}]$ . The isomorphism is given by  $a + bX + \langle X^2 + 3 \rangle \mapsto a + bi\sqrt{3}$ .

<sup>2</sup>There is some abuse of notation here since we take  $B_i$  to be only some subset of all the actual possible points.

**Theorem 6.2.** *Let  $P$  be a constructible point belonging to  $B_n$ , where  $B_0 = \{(0,0), (1,0)\}$ , and let  $K_n$  be the field generated over  $\mathbb{Q}$  by  $B_n$ . Then  $[K_n : \mathbb{Q}]$  is a power of 2.*

*Proof sketch.* We proceed by induction. The base case is  $K_0 = \mathbb{Q}$ , so  $[K_0 : \mathbb{Q}] = 1 = 2^0$ . Now suppose  $[K_{n-1} : \mathbb{Q}] = 2^k$  for some  $k \geq 0$ , and we want to show that  $[K_n : K_{n-1}]$  is a power of 2. Observe that new points in  $B_n$  can be obtained by

1. intersection of two lines,
2. intersection of a line and a circle,
3. or intersection of two circles.

In case (1), the intersection of two lines is given by solving a system of two linear equations, which only involves rational operations<sup>3</sup>. In other words, this case takes place entirely in  $K_{n-1}$ .

In case (2), the intersection of a line and a circle is given by solving of a system of one linear equation and one quadratic equation. Solving the linear equation for one of the variables and substituting into the quadratic equation reduces the system down to a single quadratic equation in a single variable. The solution involves  $\sqrt{\Delta}$ , where  $\Delta$  is the discriminant. Then the new points are in  $K_{n-1}[\sqrt{\Delta}]$ .

In case (3), the intersection of two circles is given by solving a system of two quadratic equations. Subtracting the two quadratic equations yields a linear equation, which reduces back to case (2).

Thus the elements in  $K_n$  are either in  $K_{n-1}$  or  $K_{n-1}[\sqrt{\Delta}]$  for some  $\Delta \in K_{n-1}$ .<sup>4</sup> Hence  $[K_n : K_{n-1}]$  is either 1 or 2, so by induction  $[K_n : \mathbb{Q}]$  is a power of 2.  $\square$

## 6.3 Classic Problems

### 6.3.1 Duplicating the Cube

Consider the problem of taking a cube of volume 1, and constructing a cube of volume 2. We need  $\alpha$  such that  $\alpha^3 = 2$ . But  $X^3 - 2$  is irreducible over  $\mathbb{Q}$  by Eisenstein's criterion, so  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ . This is not a power of 2, so  $\alpha$  is not constructible and thus we cannot duplicate the cube.

### 6.3.2 Trisecting the Angle

Recall the triple angle formula:

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

Suppose  $\cos 3\theta = c$ . So to find  $\cos \theta$ , we want a root of  $4X^3 - 3X - c = 0$ . This depends on  $c$ .

**Example 6.2.3.** If  $3\theta = \pi/2$ , then  $c = 0$  and the polynomial factors into

$$4X^3 - 3X = 4X(4X^2 - 3),$$

so  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$ . So in fact we can trisect  $\pi/2 = 90^\circ$ .

<sup>3</sup>By rational operations we mean addition, subtraction, multiplication, division.

<sup>4</sup>We can set it up so that we only gain one extra intersection, i.e. only one  $\Delta$ , at each step.

**Example 6.2.4.** If  $3\theta = \pi/3$ , then  $c = 1/2$  and we have  $4X^3 - 3X - 1/2$ . Let

$$f(X) = 8X^3 - 6X - 1,$$

so that  $g(X) = g(X/2) = X^3 - 3X - 1$ . Note that  $g$  does not factor over  $\mathbb{Z}$  since that requires a linear factor of  $X \pm 1$  but  $g(\pm 1) \neq 0$ . So  $g$  is irreducible over  $\mathbb{Z}$  and by Gauss's lemma,  $g$  is irreducible over  $\mathbb{Q}$ . Thus  $f$  is irreducible. Hence  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ , so we cannot trisect  $\pi/3$  with a straightedge and compass.

# Lecture 7

## Jan. 31 — Splitting Fields

### 7.1 Review of Notation

Recall that

$$\begin{aligned}\mathbb{Q}[X] &= \{a_0 + a_1X + \cdots + a_nX^n : a_i \in \mathbb{Q}\} \\ \mathbb{Q}(X) &= \{f/g : f, g \in \mathbb{Q}[X], g \neq 0\} / \sim,\end{aligned}$$

where  $\sim$  is the usual relation on fractions, e.g.  $2f/2g = f/g$ . Next, recall that

$$\mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} + \cdots + a_n\sqrt{2}^n : a_i \in \mathbb{Q}\} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

since  $\sqrt{2}^2 = 2$ . Also  $\mathbb{Q}(\sqrt{2})$  is the smallest subfield of  $\mathbb{R}$  containing  $\mathbb{Q} \cup \{\sqrt{2}\}$ . In this case,  $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$  since

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

Next, we have

$$\begin{aligned}\mathbb{Q}[X]/\langle X^2 - 2 \rangle &= \{a_0 + a_1X + \cdots + a_nX^n + \langle X^2 - 2 \rangle : a_i \in \mathbb{Q}\} \\ &= \{a + bX + \langle X^2 - 2 \rangle : a, b \in \mathbb{Q}\}\end{aligned}$$

since  $X^2 + \langle X^2 - 2 \rangle = 2 + \langle X^2 - 2 \rangle$ . In fact,  $\mathbb{Q}[X]/\langle X^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}]$ .<sup>1</sup>

### 7.2 Splitting Fields

The motivating question here is: When can we factor a polynomial into linear factors?

**Definition 7.1.** A polynomial *splits completely* over  $K$  if it can be factored into linear factors over  $K$ .

**Example 7.1.1.** The polynomial  $X^2 + 2$  splits completely over  $\mathbb{Q}[i\sqrt{2}]$  since  $X^2 + 2 = (X - i\sqrt{2})(X + i\sqrt{2})$ .

**Example 7.1.2.** The polynomial  $X^3 - 2$  is irreducible over  $\mathbb{Q}$  by Eisenstein's criterion. However, it factors as

$$X^3 - 2 = (X - \alpha)(X^2 + \alpha X + \alpha^2)$$

in  $\mathbb{Q}[\alpha]$ , where  $\alpha = \sqrt[3]{2}$ . Also  $X^2 + \alpha X + \alpha^2$  is irreducible over  $\mathbb{Q}[\alpha]$ , since its discriminant shows that it is irreducible even over  $\mathbb{R}$ . But in  $\mathbb{C}$ , we can factor it as

$$X^3 - 2 = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{4\pi i/3}).$$

A smaller field that  $X^3 - 2$  splits completely over is  $\mathbb{Q}[\sqrt[3]{2}, i\sqrt{3}]$ .

---

<sup>1</sup>Here the isomorphism  $\mathbb{Q}[X]/\langle X^2 - 2 \rangle \rightarrow \mathbb{Q}[\sqrt{2}]$  is given by  $a + bX + \langle X^2 - 2 \rangle \mapsto a + b\sqrt{2}$ .

**Definition 7.2.** Let  $K$  be a field and  $f \in K[X]$ . An extension  $L$  of  $K$  is a *splitting field* for  $f$  over  $K$  if

1.  $f$  splits completely over  $L$ ,
2. and  $f$  does not split completely over any subfield  $E$  with  $K < E < L$ .

**Example 7.2.1.** From the last two examples,  $\mathbb{Q}[i\sqrt{2}]$  is a splitting field over  $\mathbb{Q}$  for  $X^2 + 2$ , and  $\mathbb{Q}[\sqrt[3]{2}, i\sqrt{3}]$  is a splitting field for  $X^3 - 2$  over  $\mathbb{Q}$ .

**Theorem 7.1.** Let  $K$  be a field and  $f \in K[X]$  with  $\partial f = n$ . Then there exists a splitting field  $L$  for  $f$  over  $K$  and  $[L : K] \leq n!$ .

*Proof.* The proof is essentially the process we perform in the following example. At each step, construct an extension in which we can split off a linear factor from  $f$ . For more details, see Howie.  $\square$

**Example 7.2.2.** Let us find a splitting field for

$$f = X^5 + X^4 - X^3 - 3X^2 - 3X + 3$$

over  $\mathbb{Q}$ . Note that  $\partial f = n$ . Stare hard enough and we can see that

$$f = (X^3 - 3)(X^2 + X - 1),$$

where the first factor is irreducible by Eisenstein's criterion and the second factor is irreducible by checking the discriminant. Now add a root, say  $\alpha = \sqrt[3]{3}$ , and let  $E_1 = \mathbb{Q}(\alpha)$ . Then

$$f = (X - \alpha)(X^2 + \alpha X + \alpha^2)(X^2 + X - 1).$$

Note that  $[E_1 : K] \leq n = \partial f$ . Now let  $E_2 = E_1(\alpha e^{2\pi i/3})$ , so that

$$f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X^2 + X - 1).$$

Note that  $[E_2 : \mathbb{Q}] \leq n(n-1)$ . Next  $E_3 = E_2(\alpha e^{-2\pi i/3})$  with

$$f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X^2 + X - 1).$$

Note that  $[E_3 : K] \leq n(n-1)(n-2)$ . Now let

$$\gamma = \frac{-1 + \sqrt{5}}{2}, \quad \delta = \frac{-1 - \sqrt{5}}{2}.$$

Let  $E_4 = E_3(\gamma)$ ,

$$f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X - \gamma)(X - \delta).$$

Finally  $E_5 = E_4(\delta)$  is the splitting field for  $f$  over  $\mathbb{Q}$ . Note that we did much better than  $n!$  here, since

$$[E_1 : \mathbb{Q}] = 3, \quad [E_2 : E_1] = 2, \quad [E_3 : E_2] = 1, \quad [E_4 : E_3] = 2, \quad [E_5 : E_4] = 1,$$

so  $[E_5 : \mathbb{Q}] = 12 \leq 120$ .

**Remark.** Splitting fields are unique (up to isomorphism).

**Theorem 7.2.** Let  $L$  and  $L'$  be splitting fields of  $f$  over  $K$ . Then there exists an isomorphism  $\varphi : L \rightarrow L'$  fixing  $K$ .

*Proof sketch.* Induct on the number of roots of  $f$  that are not in  $K$ . The induction step uses Theorem 6.1 from last class giving an isomorphism  $K[\alpha] \rightarrow K[\alpha']$  for  $\alpha, \alpha'$  roots of an irreducible polynomial.  $\square$

**Example 7.2.3.** Let us find the splitting field of  $f = X^4 - 2$  over  $\mathbb{Q}$  and its degree. Note that  $X^4 - 2$  is irreducible over  $\mathbb{Q}$  by Eisenstein's criterion. Note that

$$X^4 - 2 = (X - \alpha)(X + \alpha)(X - i\alpha)(X + i\alpha)$$

where  $\alpha = \sqrt[4]{2}$ . So the splitting field is  $\mathbb{Q}(\sqrt[4]{2}, i)$ . For the degree, note that  $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$  since the minimal polynomial of  $\sqrt[4]{2}$  is  $X^4 - 2$ . A basis for this extension is  $\{1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3\}$ . Since  $i \notin \mathbb{Q}(\sqrt[4]{2})$ , we have  $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$  since the minimal polynomial of  $i$  over  $\mathbb{Q}(\sqrt[4]{2})$  is  $X^2 + 1$ . Thus we see that the degree of the splitting field is  $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$ .

**Example 7.2.4.** Let us look at monic quadratic polynomials over  $\mathbb{Z}_3 = \{-1, 0, 1\}$ .<sup>2</sup> These are

$$\begin{array}{ccc} X^2 & X^2 + 1 & X^2 - 1 \\ X^2 + X & X^2 + X + 1 & X^2 + X - 1 \\ X^2 - X & X^2 - X + 1 & X^2 - X - 1. \end{array}$$

We have 0 is a root of the polynomials in the first column, 1 is a root of  $X^2 - 1$  and  $X^2 + X + 1$ , and  $-1$  is a root of  $X^2 - X + 1$ . So the irreducible polynomials over  $\mathbb{Z}_3$  are

$$X^2 + 1, \quad X^2 + X - 1, \quad X^2 - X - 1.$$

Let  $L = \mathbb{Z}_3[X]/\langle X^2 + 1 \rangle$ . Observe that  $\alpha = X + \langle X^2 + 1 \rangle$  satisfies

$$\alpha^2 = X^2 + \langle X^2 + 1 \rangle = -1 + \langle X^2 + 1 \rangle.$$

Hence  $L$  is a splitting field for  $X^2 + 1$  since  $(X - \alpha)(X + \alpha) = X^2 + 1$ . Similarly,  $\mathbb{Z}_3[X]/\langle X^2 + X - 1 \rangle$  is a splitting field for  $X^2 + X - 1$  and  $\mathbb{Z}_3[X]/\langle X^2 - X - 1 \rangle$  is a splitting field for  $X^2 - X - 1$ . Note that each of these fields have  $9 = 3^2$  elements since they are degree 2 extensions of  $\mathbb{Z}_3$ .

**Remark.** In  $L$ , we had  $\alpha \in L$  such that  $\alpha^2 = -1$  and addition is performed modulo 3. Now observe

$$(\alpha + 1)^2 + (\alpha + 1) - 1 = (\alpha^2 - \alpha + 1) + (\alpha + 1) - 1 = \alpha^2 - \alpha + \alpha + 1 + 1 - 1 = 0$$

since  $\alpha^2 = -1$ . So  $\alpha + 1$  is a root of  $X^2 + X - 1$  in  $L$ . By a similar computation, we see that  $-\alpha + 1$  is a root of  $X^2 + X - 1$ , so  $L$  is also a splitting field for  $X^2 + X - 1$ . Additionally,  $\alpha - 1$  and  $-\alpha - 1$  are roots of  $X^2 - X - 1$ , so  $L$  is also a splitting field for  $X^2 - X - 1$ . So by uniqueness of splitting fields,

$$\mathbb{Z}_3[X]/\langle X^2 + 1 \rangle \cong \mathbb{Z}_3[X]/\langle X^2 + X - 1 \rangle \cong \mathbb{Z}_3[X]/\langle X^2 - X - 1 \rangle.$$

**Exercise 7.1.** Find explicit isomorphisms between these fields.

## 7.3 Finite Fields

**Definition 7.3.** Let  $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ . Then the *formal derivative* of  $f$  is

$$Df = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

**Exercise 7.2.** The usual formulas for derivatives

$$D(kf) = kDf, \quad D(f + g) = Df + Dg, \quad D(fg) = (Df)g + f(Dg)$$

all still hold for  $f, g \in K[X]$  and  $k \in K$ .

<sup>2</sup>Note that as opposite to  $\mathbb{Q}$ , this field has finite characteristic.

# Lecture 8

## Feb. 5 — Finite Fields

### 8.1 Last Time

**Example 8.0.1.** The splitting field of  $X^4 - 2$  over  $\mathbb{Q}$  is  $\mathbb{Q}(i, \sqrt[4]{2})$  since

$$X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2}).$$

**Example 8.0.2.** The splitting field of  $Y^2 + 1$  over  $\mathbb{Z}_3$  is  $\mathbb{Z}_3[X]/\langle X^2 + 1 \rangle$ . If  $\alpha = X + \langle X^2 + 1 \rangle$ , then

$$Y^2 + 1 = (Y - \alpha)(Y + \alpha).$$

Also the degree of this extension is  $[\mathbb{Z}_3[X]/\langle X^2 + 1 \rangle : \mathbb{Z}_3] = 2$ , and a basis for the extension is  $\{1, X\}$ .

### 8.2 Finite Fields

**Lemma 8.1.** *Let  $f \in K[X]$ ,  $K$  a field, and  $L$  be a splitting field for  $f$  over  $K$ . Then the roots of  $f$  are distinct if and only if  $f$  and  $Df$  have no nonconstant common factor.*

*Proof.* ( $\Leftarrow$ ) We show the contrapositive. Suppose  $f$  has a repeated root  $\alpha$  in  $L$ . Then

$$f = (X - \alpha)^r g$$

for some  $r \geq 2$ . Then

$$Df = (X - \alpha)^r Dg + r(X - \alpha)^{r-1}g,$$

so  $Df$  and  $f$  both have  $X - \alpha$  as a factor.

( $\Rightarrow$ ) Suppose the roots of  $f$  are all distinct. Then for each root  $\alpha$  of  $f$  in  $L$ , we have

$$f = (X - \alpha)g,$$

where  $g(\alpha) \neq 0$ . Then

$$Df = (X - \alpha)Dg + g,$$

so that

$$(Df)(\alpha) = g(\alpha) \neq 0,$$

i.e.  $X - \alpha \nmid Df$ . This holds for factor of  $f$  in  $L[X]$ , so  $f$  and  $Df$  have no common proper factors.  $\square$

**Theorem 8.1.** *Finite fields exist and are unique up to isomorphism. In particular,*

1. Let  $K$  be a finite field. Then  $|K| = p^n$  for some prime  $p$  and integer  $n \geq 1$ . Every element of  $K$  is a root of  $X^{p^n} - X$  and  $K$  is a splitting field of  $X^{p^n} - X$  over  $\mathbb{Z}_p$ .
2. Let  $p$  be a prime and  $n \in \mathbb{Z}$ ,  $n \geq 1$ . Then there exists a unique field of order  $p^n$  up to isomorphism.

*Proof.* (1) Let  $\text{char } K = p$ . Then  $K$  is a finite extension of  $\mathbb{Z}_p$ . Let  $n = [K : \mathbb{Z}_p]$ . If  $\{\delta_1, \dots, \delta_n\}$  is a basis for  $K$  over  $\mathbb{Z}_p$ , then every element in  $K$  can be uniquely written as

$$a_1\delta_1 + \dots + a_n\delta_n$$

for some  $a_i \in \mathbb{Z}_p$ . There are  $p^n$  such elements, so  $|K| = p^n$ . Then  $|K^*| = p^n - 1$ .<sup>1</sup> For any  $\alpha \in K^*$ , the order of  $\alpha$  divides  $p^n - 1$ . So  $\alpha^{p^n-1} = 1$ , and hence  $\alpha^{p^n} - \alpha = 0$ . We also have  $0^{p^n} - 0 = 0$  so every element in  $K$  is a root of  $X^{p^n} - X$ . Hence  $X^{p^n} - X$  splits completely over  $K$ . Since  $X - \alpha$  is a factor of  $X^{p^n} - X$  for each of the  $p^n$  elements of  $K$ ,  $X^{p^n} - X$  does not split over any proper subfield of  $K$ . Thus we conclude that  $K$  is a splitting field of  $X^{p^n} - X$  over  $\mathbb{Z}_p$ .

(2) Given a prime  $p$  and an integer  $n \geq 1$ , let  $L$  be the splitting field of  $X^{p^n} - X$  over  $\mathbb{Z}_p$ . Note that

$$Df = p^n X^{p^n-1} - 1 = -1$$

since  $\text{char } \mathbb{Z}_p = p$ . Then  $Df$  and  $f$  have no nonconstant common factors, so by Lemma 8.1, we see that  $X^{p^n} - X$  has  $p^n$  distinct roots in  $L$ . Let  $K$  be the set of  $p^n$  distinct roots, and we claim that  $K$  is a subfield of  $L$ . To check this, let  $a, b \in K$ . Then by an extension of Theorem 2.4,

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

in  $\mathbb{Z}_p$ ,  $a - b \in K$ . Also

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

so  $ab^{-1} \in K$ . Hence  $K$  is a field of order  $p^n$ . In fact,  $K = L$  since  $K$  contains all the roots of  $X^{p^n} - X$  and no proper subfield does. By uniqueness of splitting fields,  $K$  is unique up to isomorphism.  $\square$

**Definition 8.1.** We call the field of order  $p^n$  the *Galois field* of order  $p^n$ , denoted  $\text{GF}(p^n)$ .

**Example 8.1.1.** We have  $\text{GF}(3^2) = \mathbb{Z}_3[X]/\langle X^2 + 1 \rangle \cong \mathbb{Z}_3[X]/\langle X^2 + X - 1 \rangle \cong \mathbb{Z}_3[X]/\langle X^2 - X - 1 \rangle$ .

**Remark.** Recall that for a finite group  $G$  and  $a \in G$ , the *order* of  $a$  is

$$\text{ord}(a) = \min\{k \in \mathbb{N} : a^k = 1\}.$$

The *exponent* of  $G$  is

$$\exp(G) = \min\{k \in \mathbb{N} : a^k = 1 \text{ for all } a \in G\}.$$

Also recall that  $\text{ord}(a)$  divides  $|G|$  for all  $a \in G$ , and thus  $\exp(G)$  divides  $|G|$ .

**Exercise 8.1.** Show that  $\exp(G) = \text{lcm}\{\text{ord}(a) : a \in G\}$ .

**Example 8.1.2.** For  $S_3 = \{\text{id}, (12), (23), (13), (123), (132)\}$ , the order of the transpositions is 2 and the order of 3-cycles is 3. So we see that  $\exp(S_3) = 6$ .

**Proposition 8.1.** If  $G$  is a finite abelian group, then there exists  $a \in G$  such that  $\text{ord}(a) = \exp(G)$ .

<sup>1</sup>Recall that  $K^*$  is the set of nonzero elements of  $K$ , which forms a group under multiplication. We also call  $K^*$  the group of units of  $K$ .



*Proof.* Suppose that

$$\exp(G) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where the  $p_i$  are distinct primes and  $\alpha_i \geq 1$  for all  $i$ . Since

$$\exp(G) = \text{lcm}\{\text{ord}(a) : a \in G\},$$

there exists  $h_1 \in G$  such that  $p_1^{\alpha_1} \mid \text{ord}(h_1)$ . So  $\text{ord}(h_1) = p_1^{\alpha_1} q_1$  where  $q_1 \mid p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ . Let  $g_1 = h_1^{q_1}$ . For each  $m \geq 1$ , we have  $g_1^m = h_1^{mq_1}$ , and

$$h_1^{mq_1} = 1 \iff p_1^{\alpha_1} q_1 \mid mq_1 \iff p_1^{\alpha_1} \mid m.$$

Hence  $\text{ord}(g_1) = p_1^{\alpha_1}$ . Similarly for  $i = 2, \dots, k$ , we can find elements  $g_i$  of order  $p_i^{\alpha_i}$ . Let

$$a = g_1 g_2 \cdots g_k$$

and  $n = \text{ord}(a)$ . Now check as an exercise that  $\text{ord}(a) = \exp(G)$ . This relies on

$$a^n = g_1^n g_2^n \cdots g_k^n = 1,$$

which uses the assumption that  $G$  is abelian. □

**Remark.** The previous example shows that the abelian condition in this theorem is necessary.

**Corollary 8.1.1.** *If  $G$  is a finite abelian group with  $\exp(G) = |G|$ , then  $G$  is cyclic.*

**Theorem 8.2.** *The group of units  $\text{GF}(p^n)^*$  of a Galois field is cyclic.*

*Proof.* Let  $e = \exp(\text{GF}(p^n)^*)$ . Then  $a^e = 1$  for all  $a \in \text{GF}(p^n)^*$ , so every element  $a \in \text{GF}(p^n)^*$  is a root of  $X^e - 1$ . Since  $X^e - 1$  has at most  $e$  roots, we see that  $|\text{GF}(p^n)^*| \leq e$ . But  $e \leq |\text{GF}(p^n)^*|$  since  $\exp(\text{GF}(p^n)^*)$  divides  $|\text{GF}(p^n)^*|$ . Hence  $|\text{GF}(p^n)^*| = e$ , so by Corollary 8.1.1,  $\text{GF}(p^n)^*$  is cyclic. □

## 8.3 Automorphisms of Fields

**Example 8.1.3.** The complex conjugation  $f : \mathbb{C} \rightarrow \mathbb{C}$  given by  $f(a + bi) = a - bi$  is an automorphism of  $\mathbb{C}$ . Observe that  $f(c) = c$  if and only if  $c \in \mathbb{R}$ .

**Theorem 8.3.** *Let  $K$  be a field. The set  $\text{Aut } K$  of automorphisms of  $K$  forms a group under composition.*

*Proof.* First observe that composition is associative. The identity element in  $\text{Aut } K$  is the identity map  $\text{id}_K$ . For inverses, let  $\alpha \in \text{Aut } K$ . Since  $\alpha$  is a bijection, there exists an inverse map  $\alpha^{-1} : K \rightarrow K$ , where  $\alpha^{-1}(x)$  is the unique element  $s$  such that  $\alpha(s) = x$ . Now we check that  $\alpha^{-1}$  is also a homomorphism. For this, let  $x, y \in K$  and suppose that  $\alpha^{-1}(x) = s$  and  $\alpha^{-1}(y) = t$ . Then  $\alpha(s) = x$  and  $\alpha(t) = y$ , so

$$\alpha(s + t) = \alpha(s) + \alpha(t) = x + y$$

since  $\alpha$  is a homomorphism. Then we see that

$$\alpha^{-1}(x + y) = s + t = \alpha^{-1}(x) + \alpha^{-1}(y).$$

Similarly,  $\alpha(st) = xy$ , so

$$\alpha^{-1}(xy) = st = \alpha^{-1}(x)\alpha^{-1}(y).$$

Hence  $\alpha^{-1} \in \text{Aut } K$  and  $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = \text{id}_K$ , so  $\text{Aut } K$  is indeed a group. □

**Definition 8.2.** We call  $\text{Aut } K$  the *group of automorphisms* of  $K$ .

**Definition 8.3.** Let  $L$  be a field extension of  $K$ . A  $K$ -*automorphism* is an automorphism  $\alpha : L \rightarrow L$  such that  $\alpha(x) = x$  for all  $x \in K$ . The *Galois group* of  $L$  over  $K$ , denoted  $\text{Gal}(L : K)$ , is the set of  $K$ -automorphisms of  $L$ . The *Galois group*  $\text{Gal}(f)$  of a polynomial  $f \in K[X]$  is  $\text{Gal}(L : K)$  where  $L$  is a splitting field of  $f$  over  $K$ .

**Theorem 8.4.** The Galois group  $\text{Gal}(L : K)$  is a subgroup of  $\text{Aut } L$ .

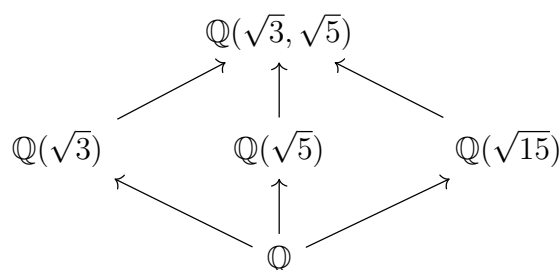
*Proof.* Clearly  $\text{id}_L \in \text{Gal}(L : K)$  since it fixes all elements of  $L$ . Now let  $\alpha, \beta \in \text{Gal}(L : K)$ . Then we have  $\alpha(x) = x$  and  $\beta(x) = x$  for all  $x \in K$ . Then  $\beta^{-1}(x) = x$ , which gives

$$\alpha\beta^{-1}(x) = \alpha(x) = x,$$

so  $\alpha\beta^{-1} \in \text{Gal}(L : K)$ . Thus  $\text{Gal}(L : K)$  is a subgroup of  $\text{Aut } L$ . □

**Remark.** The big idea here is that there is a correspondence between subfields  $E$  with  $K \subseteq E \subseteq L$  and subgroups  $H$  of  $\text{Gal}(L : K)$ .

**Exercise 8.2.** From a past homework, we identified the subfields of  $\mathbb{Q}(\sqrt{3}, \sqrt{5})$  as:



Compare the subgroups of  $\text{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q})$  to the subfields of  $\mathbb{Q}(\sqrt{3}, \sqrt{5})$  containing  $\mathbb{Q}$ .

# Lecture 9

## Feb. 7 — The Galois Correspondence

### 9.1 Automorphisms of Fields

**Example 9.0.1.** The complex conjugation  $\beta : \mathbb{C} \rightarrow \mathbb{C}$  given by  $\beta(a + bi) = a - bi$  is a nontrivial element of the Galois group of  $\mathbb{C} : \mathbb{R}$ . In fact,  $\text{Gal}(\mathbb{C} : \mathbb{R}) = \{\text{id}, \beta\}$ . Note that  $\beta$  fixes  $\mathbb{R}$ ,  $\text{id}$  fixes  $\mathbb{C}$ , and

$$\begin{array}{c} \mathbb{C} \\ \uparrow \\ \mathbb{R} \end{array}$$

### 9.2 The Galois Correspondence

**Definition 9.1.** Define

$$\begin{aligned} \Gamma(E) &= \{\alpha \in \text{Aut } L : \alpha(z) = z \text{ for all } z \in E\}, \\ \Phi(H) &= \{x \in L : \alpha(x) = x \text{ for all } \alpha \in H\}, \end{aligned}$$

where  $E$  is a subfield of  $L$  and  $H$  is a subgroup of  $\text{Gal}(L : K)$ . This is called the *Galois correspondence*.

**Example 9.1.1.** In the previous example of  $\mathbb{C} : \mathbb{R}$ , we have  $\Gamma(\mathbb{C}) = \{\text{id}\}$  and  $\Gamma(\mathbb{R}) = \{\text{id}, \beta\}$ . We also have  $\Phi(\{\text{id}, \beta\}) = \mathbb{R}$  and  $\Phi(\{\text{id}\}) = \mathbb{C}$ .

**Remark.** The goal is to determine: When are  $\Gamma$  and  $\Phi$  inverses of one another?

**Theorem 9.1.** *We have the following:*

1. *For every subfield  $E$  of  $L$  containing  $K$ ,  $\Gamma(E)$  is a subgroup of  $\text{Gal}(L : K)$ .*
2. *Conversely, for every subgroup  $H$  of  $\text{Gal}(L : K)$ ,  $\Phi(H)$  is a subfield of  $L$  containing  $K$ .*

*Proof.* See Howie. □

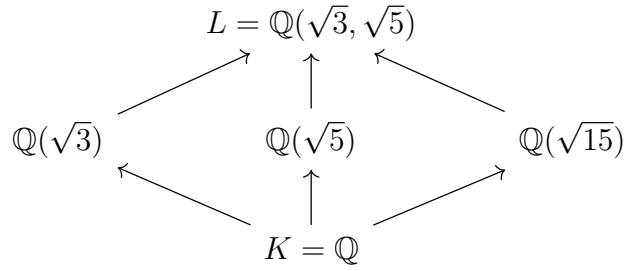
**Theorem 9.2.** *Let  $z \in L \setminus K$ . If  $z$  is a root of  $f \in K[X]$  and  $\alpha \in \text{Gal}(L : K)$ , then  $\alpha(z)$  is also a root of  $f$ .*

*Proof.* Let  $f = a_0 + a_1X + \cdots + a_nX^n$ , where  $a_i \in K$ . Then since  $\alpha$  fixes each  $a_i \in K$ , we have

$$\begin{aligned} f(\alpha(z)) &= a_0 + a_1\alpha(z) + \cdots + a_n(\alpha(z))^n = \alpha(a_0) + \alpha(a_1)\alpha(z) + \cdots + \alpha(a_n)(\alpha(z))^n \\ &= \alpha(a_0 + a_1z + \cdots + a_nz^n) = \alpha(0) = 0, \end{aligned}$$

which completes the proof. □

**Example 9.1.2.** Recall this example from homework:



A basis for  $L$  over  $K$  is  $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ . Since  $\sqrt{3}$  is a root of  $X^2 - 3$ , by the previous theorem, any element in  $\text{Gal}(L : K)$  must send  $\sqrt{3} \mapsto \pm\sqrt{3}$ . Similarly, any element must send  $\sqrt{5} \mapsto \pm\sqrt{5}$ . So the  $\mathbb{Q}$ -isomorphisms of  $\mathbb{Q}(\sqrt{3}, \sqrt{5})$  are

$$\begin{aligned}\alpha(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15}, \\ \beta(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= a + b\sqrt{3} - c\sqrt{5} - d\sqrt{15}, \\ \gamma(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= a - b\sqrt{3} - c\sqrt{5} + d\sqrt{15}, \\ \text{id}(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}.\end{aligned}$$

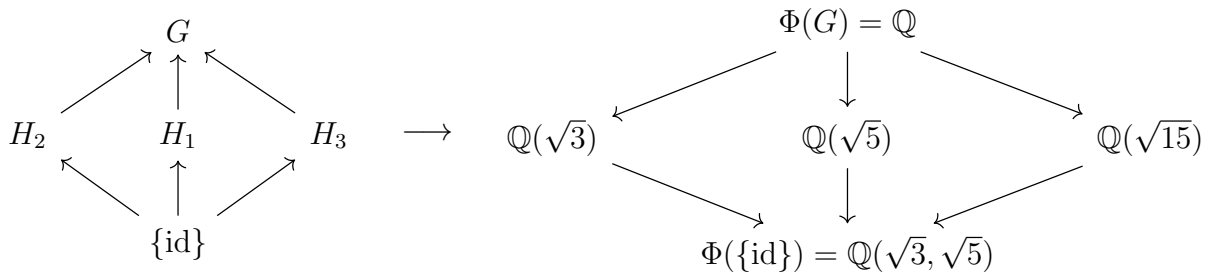
We can write the multiplication table for this group as:

$\times$	id	$\alpha$	$\beta$	$\gamma$
id	id	$\alpha$	$\beta$	$\gamma$
$\alpha$	$\alpha$	id	$\gamma$	$\beta$
$\beta$	$\beta$	$\gamma$	id	$\alpha$
$\gamma$	$\gamma$	$\beta$	$\alpha$	id

The proper subgroups are  $H_1 = \{\text{id}, \alpha\}$ ,  $H_2 = \{\text{id}, \beta\}$ , and  $H_3 = \{\text{id}, \gamma\}$ . Also  $\{\text{id}\}$  and  $G = \{\text{id}, \alpha, \beta, \gamma\}$  are subgroups. Then

$$\begin{aligned}\Phi(H_1) &= \mathbb{Q}(\sqrt{5}), & \Phi(H_2) &= \mathbb{Q}(\sqrt{3}), & \Phi(H_3) &= \mathbb{Q}(\sqrt{15}), \\ \Phi(\{\text{id}\}) &= \mathbb{Q}(\sqrt{3}, \sqrt{5}), & \Phi(G) &= \mathbb{Q}.\end{aligned}$$

Under  $\Phi$ , this gives the diagram:



Also note that  $\Gamma(\mathbb{Q}(\sqrt{3})) = \{\text{id}, \alpha\}$  since

$$\alpha(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) = a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15}.$$

**Exercise 9.1.** Show that  $\Gamma$  is the inverse of  $\Phi$  in the previous example.

**Theorem 9.3.** *Let  $L : K$  be a field extension. Then*

1. *If  $E_1, E_2$  are two subfields of  $L$  containing  $K$ , then  $E_1 \subseteq E_2$  implies  $\Gamma(E_1) \supseteq \Gamma(E_2)$ .*
2. *If  $H_1, H_2$  are subgroups of  $\text{Gal}(L : K)$ , then  $H_1 \subseteq H_2$  implies  $\Phi(H_1) \supseteq \Phi(H_2)$ .*

*Proof.* (1) Suppose  $E_1 \subseteq E_2$  and  $\alpha \in \Gamma(E_2)$ . Then  $\alpha$  fixes every element in  $E_2$ , so since  $E_1 \subseteq E_2$ ,  $\alpha$  also fixes every element in  $E_1$ . Hence  $\alpha \in \Gamma(E_1)$  by definition.

(2) Suppose  $H_1 \subseteq H_2$  and let  $z \in \Phi(H_2)$ . Then  $\alpha(z) = z$  for every  $\alpha \in H_2$ , and since  $H_1 \subseteq H_2$ ,  $\alpha(z) = z$  for every  $\alpha \in H_1$  as well. Hence  $z \in \Phi(H_1)$  by definition.  $\square$

**Remark.** Note that  $\Gamma$  and  $\Phi$  are not always inverses of one another.

**Example 9.1.3.** Consider the extension  $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ . If  $\alpha \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ , then

$$\alpha(\sqrt[3]{2})^3 = \alpha(2) = 2.$$

Since there is only one cube root of 2 in this field, we must have  $\alpha(\sqrt[3]{2}) = \sqrt[3]{2}$ . So  $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{\text{id}\}$ . So  $\Gamma$  cannot be the inverse of  $\Phi$  here since there are two subfields, namely  $\mathbb{Q}(\sqrt[3]{2})$  and  $\mathbb{Q}$ . In particular,

$$\Gamma(\mathbb{Q}(\sqrt[3]{2})) = \Gamma(\mathbb{Q}) = \{\text{id}\} \quad \text{and} \quad \Phi(\{\text{id}\}) = \mathbb{Q}(\sqrt[3]{2}).$$

**Theorem 9.4.** *For any subfield  $E$  of  $L$  and subgroup  $H$  of  $\text{Gal}(L : K)$ , we have*

1.  $E \subseteq \Phi(\Gamma(E))$
2. *and*  $H \subseteq \Gamma(\Phi(H))$ .

*Proof.* (1) Let  $z \in E$ . Then  $\Gamma(E)$  is the set of all automorphisms fixing every element of  $E$ , and so  $z$  is fixed by every element of  $\Gamma(E)$ . Hence  $z \in \Phi(\Gamma(E))$ .

(2) Let  $\alpha \in H$ . Then  $\Phi(H)$  is the set of elements of  $L$  fixed by every element of  $H$ , and so  $\alpha$  fixes every element of  $\Phi(H)$ . Hence  $\alpha \in \Gamma(\Phi(H))$ .  $\square$

**Remark.** Now the goal will be to find sufficient conditions for  $\Gamma$  and  $\Phi$  to be inverses of one another.

## 9.3 Normal Extensions

**Definition 9.2.** A field extension  $L : K$  is *normal* if every irreducible polynomial in  $K[X]$  having at least one root in  $L$  splits completely over  $L$ .

**Example 9.2.1.** A nonexample is  $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ . This is not a normal extension since  $X^3 - 2$  is irreducible and has a root in  $\mathbb{Q}(\sqrt[3]{2})$ , but does not split completely over  $\mathbb{Q}(\sqrt[3]{2})$ .

**Remark.** Is  $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$  normal?

**Theorem 9.5.** *A finite extension  $L : K$  is normal if and only if it is a splitting field for some polynomial in  $K[X]$ .*

*Proof.* ( $\Rightarrow$ ) Let  $L$  be a finite normal extension and  $\{z_1, \dots, z_n\}$  be a basis for  $L : K$ . let  $m_i$  be the minimal polynomial for  $z_i$ , and let

$$m = m_1 m_2 \dots m_n.$$

Each  $m_i$  has at least one root  $z_i$  in  $L$ , hence  $m$  splits completely over  $L$  since  $L$  is normal. Since  $L$  is generated by  $z_1, \dots, z_n$ , it is not possible for  $m$  to split over a proper subfield of  $L$ , hence  $L$  is a splitting field for  $m$  over  $K$ .

( $\Leftarrow$ ) See Howie. Relies on the isomorphism  $K(\alpha) \rightarrow K(\beta)$  for  $\alpha, \beta$  roots of an irreducible polynomial  $f$ . We also need properties of degrees of field extensions.  $\square$

**Corollary 9.5.1.** *Let  $L$  be a normal extension of  $K$  and  $E$  a subfield of  $L$  containing  $K$ . Then every injective  $K$ -homomorphism  $\varphi : E \rightarrow L$  can be extended to a  $K$ -automorphism  $\varphi^*$  of  $L$ .*

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & L \\ i \downarrow & \nearrow \varphi^* & \\ L & & \end{array}$$

*Proof.* By the theorem, there exists  $f \in K[X]$  such that  $L$  is a splitting field for  $f$  over  $K$ . But  $L$  is also a splitting field for  $f$  over  $E$  and  $\varphi(E)$ . From here, a slight generalization of the proof of uniqueness of splitting fields gives the desired  $K$ -automorphism of  $L$  extending  $\varphi$ .  $\square$

**Example 9.2.2.** Let  $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ ,  $K = \mathbb{Q}$ , and  $E = \mathbb{Q}(\sqrt{3})$ . Define  $\varphi : E \rightarrow L$  by

$$\varphi(a + b\sqrt{3}) = a - b\sqrt{3},$$

which is an injective  $K$ -homomorphism. We have the following diagram:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{3}) & \xrightarrow{\varphi} & \mathbb{Q}(\sqrt{3}, \sqrt{5}) \\ i \downarrow & \nearrow \varphi^* & \\ \mathbb{Q}(\sqrt{3}, \sqrt{5}) & & \end{array}$$

Then we can define

$$\varphi^*(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) = a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15}$$

as an extension of  $\varphi$ . Note that we could have also defined

$$\varphi^*(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) = a - b\sqrt{3} - c\sqrt{5} + d\sqrt{15}.$$

**Remark.** From the previous example we see that  $\varphi^*$  is not unique.

# Lecture 10

## Feb. 12 — Normal Closures

### 10.1 Normal Closures

Recall this theorem from last time:

**Theorem 9.5.** A finite extension  $L : K$  is normal if and only if it is a splitting field for some polynomial in  $K[X]$ .

A natural question to ask is: Can we always extend a finite extension to make it normal?

**Definition 10.1.** Let  $L : K$  be a finite extension. A field  $N$  containing  $L$  is a *normal closure* of  $L : K$  if

1.  $N$  is a normal extension of  $K$ ,
2. and if  $E$  is a proper subfield of  $N$  containing  $L$ , then  $E$  is not a normal extension of  $K$ .

**Theorem 10.1.** Let  $L : K$  be a finite extension. Then

1. there exists a normal closure  $N$  of  $L$  over  $K$ ,
2. and  $N$  is unique up to isomorphism.

*Proof.* Let  $\{z_1, \dots, z_n\}$  be a basis for  $L : K$ . Since  $L : K$  is finite, each  $z_i$  is algebraic over  $K$ , with say minimal polynomial  $m_i \in K[X]$ . Let

$$m = m_1 \dots m_n,$$

and let  $N$  be the splitting field of  $m$  over  $L$ . Then  $N$  is also a splitting field of  $m$  over  $K$ , since  $L$  is generated over  $K$  by some of the roots of  $m$  in  $N$ . Hence  $N$  is a normal extension of  $K$  containing  $L$ .

To see that  $N$  is the smallest such field, suppose  $E$  is a subfield of  $N$  containing  $L$ , and suppose  $E$  is normal. For each  $m_i$ ,  $E$  contains a root  $z_i$ , so the normality of  $E$  implies that  $E$  contains all the roots of  $m$ , so  $E = N$ . For uniqueness, see Howie. The proof relies on the uniqueness of splitting fields.  $\square$

**Definition 10.2.** Let  $K_1, \dots, K_n$  be subfields of  $L$ . The *join* of  $K_1, \dots, K_n$ , denoted

$$K_1 \vee K_2 \vee \dots \vee K_n,$$

is the smallest subfield of  $L$  containing  $K_1 \cup K_2 \cup \dots \cup K_n$ .

**Remark.** The smallest subfield of  $L$  containing  $K_1 \cup K_2$  is  $K_1 \vee K_2 = K_1(K_2) = K_2(K_1)$ , similar to how the smallest subfield of  $\mathbb{R}$  containing  $\mathbb{Q} \cup \{\sqrt{3}\}$  is  $\mathbb{Q}(\sqrt{3})$ .

**Example 10.2.1.** Let  $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(e^{2\pi i/3} \cdot \sqrt[3]{2}) \subseteq \mathbb{C}$ . Then  $\mathbb{Q}(\sqrt[3]{2}) \vee \mathbb{Q}(e^{2\pi i/3} \cdot \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ , since

$$e^{2\pi i/3} \cdot \sqrt[3]{2} = -\frac{\sqrt[3]{2}}{2} + \frac{i\sqrt{3}}{2}\sqrt[3]{2}.$$

**Remark.** In the above example, we have  $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(e^{2\pi i/3} \cdot \sqrt[3]{2}) \cong \mathbb{Q}[X]/\langle X^3 - 2 \rangle$ .

**Corollary 10.1.1.** Let  $L : K$  be a finite extension, and  $N$  the normal closure of  $L : K$ . Then

$$N = L_1 \vee L_2 \vee \cdots \vee L_k,$$

where  $L_1, L_2, \dots, L_k$  are subfields of  $N$  containing  $K$  isomorphic to  $L$ .

*Proof.* As in the previous proof, suppose  $\{z_1, \dots, z_n\}$  is a basis for  $L : K$ , so  $L = K(z_1, \dots, z_n)$ , and  $m_i$  is a minimal polynomial for  $z_i$ , and  $N$  a splitting field for  $m = m_1 \dots m_n$  over  $K$ . Let  $z'_i$  be an arbitrary root of  $m_i$ . Since  $z_i$  and  $z'_i$  are both roots of  $m_i$ , there exists a  $K$ -isomorphism  $\varphi : K(z_i) \rightarrow K(z'_i)$ , which by Corollary 9.5.1 implies there exists a  $K$ -automorphism  $\varphi^* : N \rightarrow N$ . We have that

$$z'_i \in \varphi^*(L) \cong L,$$

so every root of  $m_i$  is contained in a subfield  $L' = \varphi^*(L)$  of  $N$  that contains  $K$  and is isomorphic to  $L$ , since  $\varphi^*$  is a  $K$ -automorphism. Since  $N$  is generated over  $K$  by the roots of  $m$ , it is generated by finitely many subfields containing  $K$  and isomorphic to  $L$ .  $\square$

**Example 10.2.2.** Find the normal closure of  $\mathbb{Q}(\sqrt[3]{2})$  over  $\mathbb{Q}$ . Following the proof of the theorem,

$$\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$$

is a basis of  $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ . The minimal polynomials of  $1, \sqrt[3]{2}, \sqrt[3]{2}^2$  are  $X - 1, X^3 - 2, X^3 - 4$ , respectively. The splitting field of

$$(X - 1)(X^3 - 2)(X^3 - 4)$$

over  $\mathbb{Q}$  is  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ , since

$$X^3 - 2 = (X - \sqrt[3]{2})(X - e^{2\pi i/3}\sqrt[3]{2})(X - e^{-2\pi i/3}\sqrt[3]{2})$$

and

$$X^3 - 4 = (X - \sqrt[3]{2}^2)(X - e^{2\pi i/3}\sqrt[3]{2}^2)(X - e^{-2\pi i/3}\sqrt[3]{2}^2).$$

So  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = L_1 \vee L_2 \vee L_3$ , where  $L_1 = \mathbb{Q}(\sqrt[3]{2})$ ,  $L_2 = \mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$ , and  $L_3 = \mathbb{Q}(e^{-2\pi i/3}\sqrt[3]{2})$ , and

$$L_1 \cong L_2 \cong L_3 \cong \mathbb{Q}[X]/\langle X^3 - 2 \rangle.$$

**Theorem 10.2.** Let  $L : K$  be a finite normal extension and  $E$  a subfield of  $L$  containing  $K$ . Then  $E$  is a normal extension of  $K$  if and only if every  $K$ -monomorphism of  $E$  into  $L$  is a  $K$ -automorphism of  $E$ .

*Proof.* ( $\Rightarrow$ ) Suppose  $E : K$  is normal and let  $\varphi : E \rightarrow L$  be a  $K$ -monomorphism. Now we would like to show that  $\varphi(E) \subseteq E$ . So let  $z \in E$  and suppose

$$m = a_0 + a_1X + \cdots + a_nX^n$$



is the minimal polynomial of  $z$  over  $K$ . Then

$$a_0 + a_1z + \cdots + a_nz^n = 0,$$

so that

$$a_0 + a_1\varphi(z) + \cdots + a_n\varphi(z)^n = 0$$

since  $\varphi$  is a homomorphism fixing  $K$  pointwise. Hence  $\varphi(z)$  is also a root of  $m$  in  $L$ . Since  $E : K$  is normal, the irreducible polynomial  $m$  splits completely over  $E$ . Hence  $\varphi(z) \in E$ , so that  $\varphi(E) \subseteq E$ . Then<sup>1</sup>

$$[\varphi(E) : K] = [\varphi(E) : \varphi(K)] = [E : K] = [E : \varphi(E)][\varphi(E) : K],$$

so  $[E : \varphi(E)] = 1$ . Hence  $\varphi(E) = E$ , so  $\varphi$  is a  $K$ -automorphism of  $E$ .

( $\Leftarrow$ ) Suppose every  $K$ -monomorphism  $E \rightarrow L$  is a  $K$ -automorphism of  $E$ . Let  $f$  be an irreducible polynomial in  $K[X]$  having a root  $z \in E$ . We need to show that  $f$  splits completely over  $E$ . Since  $L$  is normal,  $f$  splits completely over  $L$ . Let  $z'$  be another root of  $f$  in  $L$ . Then there exists a  $K$ -automorphism  $K(z) \rightarrow K(z')$  which sends  $z \mapsto z'$ , which by Corollary 9.5.1 extends to a  $K$ -automorphism  $\psi$  of  $L$ . Let  $\psi^* = \psi|_E$ , i.e. the restriction of  $\psi$  to  $E$ . By hypothesis,  $\psi^*$  is a  $K$ -automorphism of  $E$ , so

$$z' = \psi(z) = \psi^*(z) \in E.$$

That is,  $E$  is normal. □

**Example 10.2.3.** Consider  $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ , which is not normal. The  $\mathbb{Q}$ -monomorphism  $\varphi : \mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{C}$  given by

$$\varphi(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + be^{2\pi i/3}\sqrt[3]{2} + ce^{-2\pi i/3}\sqrt[3]{2}^2$$

is not an automorphism of  $\mathbb{Q}(\sqrt[3]{2})$ .

**Example 10.2.4.** Consider  $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ , which is normal. The  $\mathbb{Q}$ -monomorphisms are  $\text{id}$  and

$$\varphi(a + b\sqrt{2}) = a - b\sqrt{2},$$

which are both  $\mathbb{Q}$ -automorphisms of  $\mathbb{Q}(\sqrt{2})$ .

## 10.2 Separable Extensions

**Definition 10.3.** An irreducible polynomial  $f \in K[X]$  is *separable* over  $K$  if it has no repeated roots over a splitting field. A polynomial  $g \in K[X]$  is *separable* over  $K$  if its irreducible factors are separable over  $K$ . An algebraic element in  $L : K$  is *separable* over  $K$  if its minimal polynomial is separable over  $K$ . An algebraic extension  $L : K$  is *separable* if every  $\alpha \in L$  is separable over  $K$ .

**Remark.** A polynomial like  $(X - 2)^2$  actually *is* separable over  $\mathbb{Q}$  since its irreducible factors are  $X - 2$  and  $X - 2$ , which are each separable.

**Definition 10.4.** A field  $K$  is *perfect* if every polynomial in  $K[X]$  is separable over  $K$ .

**Theorem 10.3.** We have the following:

1. Every field of characteristic 0 is perfect.

---

<sup>1</sup>We need to make this argument since  $E$  may be infinite, so injectivity does not imply bijectivity.

2. Every finite field is perfect.

*Proof.* (1) It suffices to show that if  $\text{char } K = 0$ , then any irreducible polynomial  $f$  is separable. Let

$$f = a_0 + a_1X + \cdots + a_nX^n$$

for  $n \geq 1$  and suppose  $f$  is not separable. Then  $f$  and  $Df$  have a non-constant common factor  $d$ . Since  $f$  is irreducible,  $d$  must be a constant multiple of  $f$ , and thus  $d$  cannot divide  $Df$  unless

$$Df = a_1 + 2a_2X + \cdots + na_nX^{n-1}$$

is the zero polynomial, by comparing degrees. Then

$$a_1 = 2a_2 = \cdots = na_n = 0.$$

Since  $\text{char } K = 0$ , this implies

$$a_1 = a_2 = \cdots = a_n = 0,$$

and so  $f = a_0$ , a constant polynomial.<sup>2</sup> Contradiction. Hence  $f$  is separable.

(2) The same argument as above implies the only possible inseparable irreducible polynomials are of the form<sup>3</sup>

$$f(X) = b_0 + b_1X^p + b_2X^{2p} \cdots + b_mX^{mp}.$$

Now Theorem 7.24 of Howie implies that if  $K$  is finite, such a polynomial is reducible. Hence every irreducible polynomial is separable, so  $K$  is perfect. See Howie for details.  $\square$

**Remark.** Recall that  $\mathbb{Z}_p(X)$  is an example of an infinite field with characteristic  $p$ .

---

<sup>2</sup>Recall that an irreducible polynomial is by definition a non-unit.

<sup>3</sup>We can still conclude  $ka_k = 0$  implies  $a_k = 0$  when  $k$  is not a multiple of  $p$ .

# Lecture 11

## Feb. 21 — Galois Extensions

### 11.1 Example of an Inseparable Extension

**Example 11.0.1.** The field  $K = \mathbb{Z}_p(X)$  is not perfect. Consider the polynomial

$$f = Y^p - X \in \mathbb{Z}_p(X)[Y],$$

which is irreducible. Now let  $L$  be a splitting field of  $f$  over  $K$  and  $\alpha$  a root of  $f$ , i.e.  $\alpha^p - X = 0$ . Then

$$(Y - \alpha)^p = Y^p - \alpha^p = Y^p - X$$

by freshman exponentiation. In particular,  $\alpha$  is a repeated root of  $f$  in  $L$ .

### 11.2 Galois Extensions

**Definition 11.1.** A *Galois extension* of  $K$  is a finite extension that is both normal and separable.

**Remark.** The main goal here is: For a Galois extension,  $\Gamma$  and  $\Phi$  are inverses of one another.

**Theorem 11.1.** *Let  $L : K$  be a separable extension of degree  $n$ . Then there are exactly  $n$  distinct  $K$ -monomorphisms of  $L$  into a normal closure  $N$  of  $L$  over  $K$ .*

*Proof.* Use strong induction on the degree of  $L : K$ . See Howie for details. □

**Corollary 11.1.1.** *If  $L : K$  is Galois, then  $|\text{Gal}(L : K)| = [L : K]$ .*

*Proof.* If  $L : K$  is Galois, then  $L : K$  is normal and separable. So the previous theorem applies, where  $L$  is its own normal closure. So we get exactly  $[L : K]$  distinct  $K$ -monomorphisms of  $L$  into  $L$ , which are precisely the  $K$ -automorphisms of  $L$  and thus the elements of the Galois group. □

**Example 11.1.1.** The extension  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}$  is Galois with  $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$ . We could have

$$\sqrt[3]{2} \mapsto \sqrt[3]{2} \text{ or } e^{2\pi i/3} \sqrt[3]{2} \text{ or } e^{-2\pi i/3} \sqrt[3]{2} \quad \text{and} \quad i\sqrt{3} \mapsto i\sqrt{3} \text{ or } -i\sqrt{3}.$$

Combining these options gives us 6 distinct maps, so these must in fact all be  $\mathbb{Q}$ -automorphisms of  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ , since we know the Galois group has size 6. In fact,  $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}) \cong S_3 \cong D_3$ .

**Remark.** The proper nontrivial subfields of  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$  are  $\mathbb{Q}(\sqrt[3]{2})$ ,  $\mathbb{Q}(e^{2\pi i/3} \sqrt[3]{2})$ ,  $\mathbb{Q}(e^{-2\pi i/3} \sqrt[3]{2})$ , and  $\mathbb{Q}(i\sqrt{3})$ . Maybe draw a pretty diagram with this showing the Galois correspondence.

**Exercise 11.1.** Show that  $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

**Exercise 11.2.** Show that  $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

**Theorem 11.2.** Let  $L : K$  be a finite extension. Then  $\Phi(\text{Gal}(L : K)) = K$  if and only if  $L : K$  is normal and separable.

*Proof.* ( $\Leftarrow$ ) Let  $[L : K] = n$ . By Corollary 11.1.1, we have  $|\text{Gal}(L : K)| = n$ . Let  $K' = \Phi(\text{Gal}(L : K))$ . By definition,  $K \subseteq K'$ . By Theorem 7.12 of Howie, we find that

$$[L : K'] = |\text{Gal}(L : K)|.$$

Hence  $[L : K'] = [L : K]$  and thus we conclude that  $K = K'$ .

( $\Rightarrow$ ) See Howie. □

**Exercise 11.3.** Show that if  $K \subseteq K'$  and  $[L : K'] = [L : K]$ , then  $K = K'$ .

**Theorem 11.3.** Let  $L : K$  be Galois and  $E$  a subfield of  $L$  containing  $K$ . If  $\delta \in \text{Gal}(L : K)$ , then

$$\Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}.$$

*Proof.* We begin by showing  $\delta\Gamma(E)\delta^{-1} \subseteq \Gamma(\delta(E))$ . For this, let  $\theta \in \Gamma(E)$  and  $z' \in \delta(E)$ . Then there exists a unique  $z \in E$  such that  $\delta(z) = z'$ , since  $\delta$  is an automorphism. Then

$$\delta\theta\delta^{-1}(z') = \delta\theta(z) = \delta(z) = z'$$

since  $\delta(z) = z'$  and  $\theta \in \Gamma(E)$ . So we see that  $\delta\theta\delta^{-1} \in \Gamma(\delta(E))$ .

Now for  $\Gamma(\delta(E)) \subseteq \delta\Gamma(E)\delta^{-1}$ , we will show that  $\delta^{-1}\Gamma(\delta(E))\delta \subseteq \Gamma(E)$ . Let  $\theta' \in \Gamma(\delta(E))$  and  $z \in E$ . Then  $\delta(z) \in \delta(E)$  and so  $\theta'(\delta(z)) = \delta(z)$ . Thus

$$(\delta^{-1}\theta'\delta)(z) = (\delta^{-1} \circ \delta)(z) = z,$$

so we get  $\delta^{-1}\theta'\delta \in \Gamma(E)$ , as desired. □

**Example 11.1.2.** Consider  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}$ . Define the elements of  $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q})$  by

$$\begin{aligned} \mu_1 : \sqrt[3]{2} &\mapsto \sqrt[3]{2}, i\sqrt{3} \mapsto -i\sqrt{3}, & \mu_2 : \sqrt[3]{2} &\mapsto e^{2\pi i/3}\sqrt[3]{2}, i\sqrt{3} \mapsto -i\sqrt{3}, \\ \mu_3 : \sqrt[3]{2} &\mapsto e^{-2\pi i/3}\sqrt[3]{2}, i\sqrt{3} \mapsto -i\sqrt{3}, \\ \rho_1 : \sqrt[3]{2} &\mapsto e^{2\pi i/3}\sqrt[3]{2}, i\sqrt{3} \mapsto i\sqrt{3}, & \rho_2 : \sqrt[3]{2} &\mapsto e^{-2\pi i/3}\sqrt[3]{2}, i\sqrt{3} \mapsto i\sqrt{3}. \end{aligned}$$

Let  $\delta = \mu_3$  and  $E = \mathbb{Q}(\sqrt[3]{2})$ . Then  $\delta(E) = \mathbb{Q}(e^{-2\pi i/3}\sqrt[3]{2})$  since  $\mu_3(\sqrt[3]{2}) = e^{-2\pi i/3}\sqrt[3]{2}$ . Now

$$\begin{aligned} \mu_2(e^{-2\pi i/3}\sqrt[3]{2}) &= \mu_2(e^{-2\pi i/3})\mu_2(\sqrt[3]{2}) = \mu_2(-\frac{1}{2} - i\frac{\sqrt{3}}{2})\mu_2(\sqrt[3]{2}) \\ &= (-\frac{1}{2} + i\frac{\sqrt{3}}{2})(e^{2\pi i/3}\sqrt[3]{2}) = e^{2\pi i/3}e^{2\pi i/3}\sqrt[3]{2} = e^{-2\pi i/3}\sqrt[3]{2}, \end{aligned}$$

so  $\Gamma(\delta(E)) = \{\text{id}, \mu_2\}$ . Also  $\Gamma(E) = \{\text{id}, \mu_1\}$ , and we find that

$$\delta\Gamma(E)\delta^{-1} = \{\delta\text{id}\delta^{-1}, \delta\mu_1\delta^{-1}\} = \{\text{id}, \mu_3\mu_1\mu_3^{-1}\} = \{\text{id}, \mu_2\},$$

so indeed we have  $\Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}$  in this case.

# Lecture 12

## Feb. 26 — The Fundamental Theorem

### 12.1 Normal Subgroups

Recall the following:

**Definition 12.1.** A subgroup  $H$  of  $G$  is *normal* if

$$gHg^{-1} = H$$

for all  $g \in G$  (equivalently,  $gH = Hg$  for all  $g \in G$ ). This is denoted  $H \triangleleft G$ .

**Remark.** If  $G$  is abelian, then every subgroup of  $G$  is normal.

**Exercise 12.1.** If  $[G : H] = 2$ , then  $H$  is normal.

**Remark.** Normality is a necessary and sufficient condition for  $G/H$  to be a well-defined group (with operation induced by the operation on  $G$ ).

**Theorem 12.1.** Let  $\varphi : G \rightarrow G'$  be a surjective homomorphism with kernel  $H$ . Then there exists a unique isomorphism  $\alpha : G/H \rightarrow G'$  such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & \nearrow \alpha & \\ G/H & & \end{array}$$

Here  $\pi : G \rightarrow G/H$  is the canonical projection  $g \mapsto gH$ .

### 12.2 The Fundamental Theorem of Galois Theory

**Theorem 12.2** (Fundamental theorem of Galois theory). Let  $L : K$  be a separable, normal extension of finite degree  $n$ . Then

- For all subfields  $E$  of  $L$  containing  $K$  and for all subgroups  $H$  of  $\text{Gal}(L : K)$ ,
  - $\Phi(\Gamma(E)) = E$  and  $|\Gamma(E)| = [L : E]$ ,
  - $\Gamma(\Phi(H)) = H$  and  $|\text{Gal}(L : K)|/|\Gamma(E)| = [E : K]$ .
- A subfield  $E$  is a normal extension of  $K$  if and only if  $\Gamma(E)$  is a normal subgroup of  $\text{Gal}(L : K)$ . If  $E : K$  is normal, then

$$\text{Gal}(E : K) \cong \text{Gal}(L : K)/\Gamma(E).$$

*Proof.* (1) By a homework exercise,  $L : K$  being normal implies that  $L : E$  is normal. Also, by Howie's Theorem 7.26,  $L : K$  being finite and separable implies that  $L : E$  is separable. Hence  $L : E$  is Galois, so  $|\Gamma(E)| = [L : E]$ . Then

$$[E : K] = \frac{[L : K]}{[L : E]} = \frac{|\text{Gal}(L : K)|}{|\Gamma(E)|}.$$

Now  $\Gamma(E) = \text{Gal}(L : E)$ , so  $L : E$  being Galois and Howie's Theorem 7.30 imply that  $\Phi(\Gamma(E)) = E$ . Now let  $H$  be a subgroup of  $\text{Gal}(L : K)$ . We showed that  $H \subseteq \Gamma(\Phi(H))$ . Also  $\Phi\Gamma\Phi = \Phi$ , so

$$|H| = [L : \Phi(H)] = [L : \Phi\Gamma\Phi(H)] = |\Gamma\Phi(H)|$$

by Howie's Theorem 7.12. Now finiteness and  $H \subseteq \Gamma(\Phi(H))$  imply that  $H = \Gamma(\Phi(H))$ .

(2) ( $\Rightarrow$ ) Suppose  $E : K$  is normal and let  $\delta \in \text{Gal}(L : K)$ . Let  $\delta' = \delta|_E$ , the restriction of  $\delta$  to  $E$ . Hence  $\delta'$  is a monomorphism  $E \rightarrow L$  and thus a  $K$ -automorphism of  $E$ , by Howie's Theorem 7.21. Hence

$$\delta(E) = \delta'(E) = E,$$

and so by Theorem 11.3,

$$\Gamma(E) = \Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1},$$

i.e.  $\Gamma(E)$  is a normal subgroup of  $\text{Gal}(L : K)$ .

( $\Leftarrow$ ) Suppose  $\Gamma(E)$  is a normal subgroup of  $\text{Gal}(L : K)$ . Let  $\delta_1$  be a  $K$ -monomorphism from  $E$  to  $L$ . This extends (by Howie's Corollary 7.14) to a  $K$ -automorphism  $\delta$  of  $L$ . Since  $\Gamma(E)$  is normal,  $\delta\Gamma(E)\delta^{-1} = \Gamma(E)$ . Hence by Theorem 11.3, we get  $\Gamma(\delta(E)) = \Gamma(E)$ . Since  $\Gamma$  is injective,

$$\delta_1(E) = \delta(E) = E,$$

so  $\delta$  is a  $K$ -automorphism of  $E$ . By Howie's Theorem 7.21, this implies  $E : K$  is normal.

Now suppose  $E : K$  is normal, and we want to show that

$$\text{Gal}(E : K) \cong \text{Gal}(L : K)/\Gamma(E).$$

Let  $\delta \in \text{Gal}(L : K)$  and  $\delta' = \delta|_E$ . By Howie's Theorem 7.21, having  $E : K$  be normal implies that  $\delta'(E) = E$ . Thus we can define  $\theta : \text{Gal}(L : K) \rightarrow \text{Gal}(E : K)$  by  $\delta \mapsto \delta'$ , i.e. restricting  $\delta$  to  $E$ . Clearly  $\theta$  is surjective onto  $\text{Gal}(E : K)$ . Also, we see that

$$\ker \theta = \{\delta \in \text{Gal}(L : K) \mid \delta|_E = \text{id}_E\} = \Gamma(E).$$

Hence by the first isomorphism theorem,  $\text{Gal}(E : K) \cong \text{Gal}(L : K)/\ker \theta = \text{Gal}(L : K)/\Gamma(E)$ .  $\square$

**Exercise 12.2.** Show that  $\Phi\Gamma\Phi = \Phi$ .

**Exercise 12.3.** Check that  $\theta$  is a homomorphism.

**Example 12.1.1.** Let  $L = \mathbb{Q}(\sqrt[4]{2}, i)$  with  $[L : \mathbb{Q}] = 8$ . Any  $\mathbb{Q}$ -automorphism in  $\text{Gal}(L : \mathbb{Q})$  must map

$$i \mapsto \pm i, \quad \sqrt[4]{2} \mapsto \pm \sqrt[4]{2}, \pm i \sqrt[4]{2}.$$

So there are only 8 possible automorphisms, and thus each of these must in fact be automorphisms since  $|\text{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}] = 8$ . We can enumerate these automorphisms via

$$\begin{aligned} \text{id}, \quad \alpha : \sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto i, \quad \beta : \sqrt[4]{2} \mapsto -\sqrt[4]{2}, i \mapsto i, \quad \gamma : \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, i \mapsto i, \\ \lambda : \sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto -i, \quad \mu : \sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto -i, \quad \nu : \sqrt[4]{2} \mapsto -\sqrt[4]{2}, i \mapsto -i, \\ \rho : \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, i \mapsto -i. \end{aligned}$$

Note that  $\text{Gal}(L : \mathbb{Q})$  is not abelian, as

$$\lambda\alpha(\sqrt[4]{2}) = \lambda(i\sqrt[4]{2}) = -i\sqrt[4]{2}, \quad \lambda\alpha(i) = \lambda(i) = i,$$

so  $\lambda\alpha = \rho$ . We can show as an exercise that  $\alpha\lambda = \mu \neq \rho$ , so  $\lambda\alpha \neq \alpha\lambda$ . The subgroups of  $\text{Gal}(L : \mathbb{Q})$  are

$$\begin{aligned} G = \text{Gal}(L : \mathbb{Q}), \quad & \{\text{id}\}, \quad \{\text{id}, \beta\}, \quad \{\text{id}, \mu\}, \quad \{\text{id}, \nu\}, \quad \{\text{id}, \rho\}, \\ & \{\text{id}, \alpha, \beta, \gamma\}, \quad \{\text{id}, \beta, \lambda, \nu\}, \quad \{\text{id}, \beta, \mu, \rho\}. \end{aligned}$$

Now we could draw a nice subgroup lattice for this (identical to  $D_4$ , the dihedral group of order 8). The normal subgroups of  $\text{Gal}(L : \mathbb{Q})$  are

$$G, \quad \{\text{id}, \beta, \lambda, \nu\}, \quad \{\text{id}, \alpha, \beta, \gamma\}, \quad \{\text{id}, \beta, \mu, \rho\}, \quad \{\text{id}, \beta\}, \quad \{\text{id}\}.$$

Let  $H_1 = \{\text{id}, \alpha, \beta, \gamma\}$ . Then  $\Phi(H_1) = \mathbb{Q}(i)$ . Also  $\Phi(\{\text{id}, \lambda\}) = \mathbb{Q}(\sqrt[4]{2})$  and  $\Phi(\{\text{id}, \nu\}) = \mathbb{Q}(i\sqrt[4]{2})$ . We can also see that  $\Phi(\{\text{id}, \mu\}) = \mathbb{Q}((1+i)\sqrt[4]{2})$  and  $\Phi(\{\text{id}, \rho\}) = \mathbb{Q}((1-i)\sqrt[4]{2})$ .

**Exercise 12.4.** Write out the multiplication table for  $\text{Gal}(L : \mathbb{Q})$ .

# Lecture 13

## Feb. 28 — Join of Subgroups and Subfields

### 13.1 Join of Subgroups

Let  $H_1, H_2$  be subgroups of  $G$ .

**Exercise 13.1.** Show that  $H_1 \cap H_2$  is a subgroup of  $G$ .

**Remark.** In general,  $H_1 \cup H_2$  is *not* a subgroup of  $G$ .

**Definition 13.1.** The *join* of  $H_1$  and  $H_2$ , denoted  $H_1 \vee H_2$ , is the smallest subgroup of  $G$  containing  $H_1 \cup H_2$ , i.e.  $H_1 \vee H_2$  consists of all products of the form

$$a_1 b_1 \dots a_n b_n,$$

where  $a_i \in H_1$  and  $b_i \in H_2$  for all  $n$ .

**Remark.** Recall that if  $E_1$  and  $E_2$  are subfields of  $L$ , then  $E_1 \cap E_2$  is also a subfield of  $L$ , as is the join

$$E_1 \vee E_2 = E_1(E_2) = E_2(E_1).$$

**Example 13.1.1.** In Example 12.1.1, we have  $\{\text{id}, \beta\} \vee \{\text{id}, \lambda\} = \{\text{id}, \beta, \lambda, \nu\}$ . Now notice that

$$\Phi(\{\text{id}, \beta\}) = \mathbb{Q}(i, \sqrt{2}), \quad \Phi(\{\text{id}, \lambda\}) = \mathbb{Q}(\sqrt[4]{2}), \quad \Phi(\{\text{id}, \beta, \lambda, \nu\}) = \mathbb{Q}(\sqrt{2}).$$

Notice that  $\mathbb{Q}(i, \sqrt{2}) \cap \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\sqrt{2})$ .

**Theorem 13.1.** Let  $L : K$  be Galois and  $E_1, E_2$  subfields of  $L$  containing  $K$ . If

$$\Gamma(E_1) = H_1, \quad \Gamma(E_2) = H_2,$$

then  $\Gamma(E_1 \cap E_2) = H_1 \vee H_2$  and  $\Gamma(E_1 \vee E_2) = H_1 \cap H_2$ .

*Proof.* Certainly  $E_1 \cap E_2 \subseteq E_1$ , so  $H_1 = \Gamma(E_1) \subseteq \Gamma(E_1 \cap E_2)$ , since the Galois correspondence is order reversing. Similarly,  $H_2 = \Gamma(E_2) \subseteq \Gamma(E_1 \cap E_2)$ , so  $H_1 \vee H_2 \subseteq \Gamma(E_1 \cap E_2)$ . Now  $H_1 \subseteq H_1 \vee H_2$ , so we get  $E_1 = \Phi(H_1) \supseteq \Phi(H_1 \vee H_2)$ . Similarly,  $E_2 = \Phi(H_2) \supseteq \Phi(H_1 \vee H_2)$ , so  $\Phi(H_1 \vee H_2) \subseteq E_1 \cap E_2$ . Since  $L : K$  is Galois, we get

$$H_1 \vee H_2 \supseteq \Gamma(E_1 \cap E_2)$$

by applying  $\Gamma$  to both sides. So  $\Gamma(E_1 \cap E_2) = H_1 \vee H_2$ .

The proof for  $\Gamma(E_1 \vee E_2) = H_1 \cap H_2$  is similar, see Howie for details. □



# Lecture 14

## Mar. 4 — Solvable Groups

### 14.1 Solvable Groups

**Definition 14.1.** A finite group  $G$  is *solvable* if, for some  $m \geq 0$ , it has a finite series

$$\{\text{id}\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$$

of subgroups such that for  $i = 0, \dots, m-1$ ,

1.  $G_i \triangleleft G_{i+1}$ ,
2. and  $G_{i+1}/G_i$  is cyclic.

**Remark.** We require  $G_i \triangleleft G_{i+1}$ , but  $G_i$  need not be normal in  $G$ .

**Example 14.1.1.** Let  $G = \text{Gal}(\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q})$  from Example 12.1.1. We have

$$\{\text{id}\} \subseteq \{\text{id}, \lambda\} \subseteq \{\text{id}, \beta, \lambda, \nu\} \subseteq G,$$

where  $G_i \triangleleft G_{i+1}$  and  $|G_{i+1}/G_i| = 2$ , so it is cyclic. Observe that  $\{\text{id}, \lambda\}$  is not normal in  $G$ , since

$$\alpha\{\text{id}, \lambda\} = \{\alpha, \mu\} \neq \{\alpha, \rho\} = \{\text{id}, \lambda\}\alpha.$$

**Theorem 14.1.** *Every finite abelian group  $G$  is solvable.*

*Proof.* Recall from the structure theorem for finitely generated abelian groups that every finite abelian group is a direct sum of cyclic groups. Then

$$G = U_1 \oplus U_2 \oplus \cdots \oplus U_k$$

where each  $U_i$  is cyclic. Let

$$G_i = U_1 \oplus \cdots \oplus U_i.$$

Observe that  $G_i \triangleleft G_{i+1}$  since  $G$  is abelian, and  $G_{i+1}/G_i \cong U_{i+1}$ , which is cyclic. So  $G$  is solvable.  $\square$

**Remark.** Recall that  $S_n$  is the symmetric group on  $n$  elements.

**Theorem 14.2.** *Every permutation can be expressed as a product of transpositions (i.e. 2-cycles).*

**Definition 14.2.** A permutation  $\sigma$  is *even* (respectively *odd*) if  $\sigma$  can be expressed as a product of an *even* (respectively *odd*) number of transpositions. This is well defined. The set

$$A_n = \text{subgroup of even permutations}$$

is called the *alternating group*.

**Example 14.2.1.** We have  $S_3 = \{\text{id}, (12), (23), (13), (123), (132)\}$ . We can write

$$\{\text{id}\} \subseteq \{\text{id}, (123), (132)\} \subseteq S_3.$$

Call these  $G_i$  for  $i = 0, 1, 2$ . Then  $G_i \triangleleft G_{i+1}$ , and  $G_2/G_1 \cong \mathbb{Z}_2$  and  $G_1/G_0 = G_1 \cong \mathbb{Z}_3$ . So  $S_3$  is solvable.

**Example 14.2.2.** The symmetric group  $S_4$  is solvable. We can write

$$\{\text{id}\} \subseteq \{\text{id}, (12)(34)\} \subseteq \{\text{id}, (12)(34), (13)(24), (14)(23)\} \subseteq A_4 \subseteq S_4.$$

Call the first three subgroups  $G_i$  for  $i = 0, 1, 2$ . Then  $G_i \triangleleft G_{i+1}$ , and we have

$$S_4/A_4 \cong \mathbb{Z}_2, \quad A_4/G_2 \cong \mathbb{Z}_3, \quad G_2/G_1 \cong \mathbb{Z}_2, \quad G_1/G_0 \cong \mathbb{Z}_2.$$

**Exercise 14.1.** Show that  $G_2 = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4$ .

**Definition 14.3.** A group is *simple* if it has no proper normal subgroups.

**Remark.** A non-abelian simple group is not solvable.

**Theorem 14.3.** For  $n \geq 5$ , the alternating group  $A_n$  is simple.

*Proof.* See Howie. □

**Theorem 14.4.** We have the following:

1. If  $G$  is solvable, then every subgroup of  $G$  is solvable.
2. If  $G$  is solvable and  $N \triangleleft G$ , then  $G/N$  is solvable.
3. Let  $N \triangleleft G$ . Then  $G$  is solvable if and only if  $N$  and  $G/N$  are solvable.

*Proof.* (1) Since  $G$  is solvable, there exists

$$\{\text{id}\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$$

where  $G_i \triangleleft G_{i+1}$  and  $G_{i+1}/G_i$  is cyclic. Now let  $H$  be a subgroup of  $G$ . Let  $K_i = G_i \cap H$ . Now check as an exercise that

$$\{\text{id}\} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = H$$

is the desired series of subgroups. In particular, check that  $K_i \triangleleft K_{i+1}$  and  $K_{i+1}/K_i$  is cyclic (show that it is a subgroup of the cyclic group  $G_{i+1}/G_i$ ).

(2) Take

$$N/N = NG_0/N \subseteq NG_1/N \subseteq \cdots \subseteq NG_m/N = G/N$$

as the desired series of subgroups. Here

$$NG = \{ng \mid n \in N, g \in G\}.$$

Check as an exercise that this construction works. For the cyclic part, verify that  $(NG_{i+1}/N)/(NG_i/N)$  is a quotient of the cyclic group  $G_{i+1}/G_i$ . One of the isomorphism theorems may help here.

(3) ( $\Rightarrow$ ) this follows from (1) and (2).

( $\Leftarrow$ ) Suppose  $N$  and  $G/N$  are solvable. Then there exists a series

$$\{\text{id}\} \subseteq N_0 \subseteq N_1 \subseteq \cdots \subseteq N_p = N$$

such that  $N_i \triangleleft N_{i+1}$  and  $N_{i+1}/N_i$  is cyclic, and a series

$$\{\text{id}\} = N/N = G_0/N \subseteq G_1/N \subseteq \cdots \subseteq G_n/N = G/N$$

such that  $G_i/N \triangleleft G_{i+1}/N$  and  $(G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i$  by one of the isomorphism theorems, so it is cyclic as well. Now check as an exercise that

$$\{\text{id}\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_p = N = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

is the desired series (i.e. check the normal and cyclic conditions).  $\square$

**Corollary 14.4.1.** *For  $n \geq 5$ ,  $S_n$  is not solvable.*

*Proof.* For  $n \geq 5$ ,  $A_n$  is simple, hence it is not solvable. Now if  $S_n$  were solvable, all of its subgroups would be solvable, which leads to a contradiction since  $A_n \subseteq S_n$ .  $\square$

## 14.2 Solvable Polynomials

**Definition 14.4.** A field extension  $L : K$  is a *radical extension* if there exists a sequence

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$$

such that  $L_{j+1} = L_j(\alpha_j)$ , where  $\alpha_j$  is a root of a polynomial in  $L_j[X]$  of the form  $X^{n_j} - c_j$ .

**Example 14.4.1.** For  $L_0 = \mathbb{Q}$ , we can take

$$\begin{aligned} L_0 &= \mathbb{Q}, \\ L_1 &= L_0(\alpha_0), & \alpha_0^2 &= 2, \\ L_2 &= L_1(\alpha_1), & \alpha_1^5 &= 3 + \sqrt{2} \in L_1, \\ L_3 &= L_2(\alpha_2), & \alpha_2^2 &= 2 + \sqrt[5]{3 + \sqrt{2}} \in L_2. \end{aligned}$$

This is a radical extension of  $\mathbb{Q}$ .

**Definition 14.5.** A polynomial  $f \in K[X]$  is *solvable by radicals* if there is a splitting field for  $f$  contained in a radical extension of  $K$ .

**Example 14.5.1.** Any quadratic  $f = X^2 + bX + c \in \mathbb{Q}[X]$  is solvable by radicals, since its roots are

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

**Remark.** In the 16th and 17th centuries, mathematicians proved that cubics

$$X^3 + a_2X^2 + a_1X + a_0$$

and quartics

$$X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$$

are solvable by radicals. For cubics, the idea is to *depress* the cubic, i.e. make a substitution to remove the quadratic term. Then we get

$$Y^3 + 3aY + b = 0.$$

By a lengthy algebra argument, the roots are

$$q + r, \quad q\omega + r\omega^2, \quad q\omega^2 + r\omega,$$

where

$$q = \left( \frac{1}{2}(-b + \sqrt{b^2 + 4a^3}) \right)^{1/3}$$

and we have similar expressions for  $r$  and  $\omega$ . A similar but longer algebraic manipulations can be made for quartics. In particular, the expressions for the roots of cubics and quartics only involve radicals.

**Theorem 14.5.** *Let  $L : K$  be a radical extension and  $N$  the normal closure of  $L$  over  $K$ . Then  $N$  is also a radical extension of  $K$ .*

*Proof.* By Corollary 10.1.1, we have

$$N = L_1 \vee \cdots \vee L_k,$$

where each  $L_i \cong L$ , hence they are all radical. Now it suffices to show that the join of two radical extensions is radical. For this, let

$$L_1 = K(\alpha_1, \dots, \alpha_m), \quad L_2 = K(\beta_1, \dots, \beta_n),$$

where  $\alpha_i^{k_i} \in K(\alpha_1, \dots, \alpha_{i-1})$  and  $\beta_j^{l_j} \in K(\beta_1, \dots, \beta_{j-1})$ . Then

$$L_1 \vee L_2 = K(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n),$$

where  $\alpha_i^{k_i} \in K(\alpha_1, \dots, \alpha_{i-1})$  and  $\beta_j^{l_j} \in K(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_{j-1})$ , so  $L_1 \vee L_2$  is radical.  $\square$

**Remark.** Radical extensions involve polynomials of the form  $X^m - c$ . Let us look more closely at  $X^m - 1$ . We focus on fields  $K$  of characteristic 0, so that the splitting field  $L$  of  $X^m - 1$  over  $K$  is normal and separable.

**Lemma 14.1.** *The set  $R$  of roots of  $X^m - 1$  is a cyclic group under multiplication.*

*Proof.* Check as an exercise that  $R$  is indeed a subgroup of  $L$ . To see that it is cyclic, recall that

$$\exp(R) = \text{smallest positive integer } e \text{ such that } a^e = 1 \text{ for all } a \in R.$$

Clearly we have  $\exp(R) \leq |R|$ . Now observe that  $x^e - 1$  has at most  $e$  roots, so  $|R| \leq e$ . Hence  $e = |R| = m$ , so  $(R, \cdot)$  is cyclic.  $\square$

**Definition 14.6.** A *primitive  $m$ th root of unity*  $\omega$  is a generator for  $(R, \cdot)$ .

**Remark.** We have

$$R = \{1, \omega, \omega^2, \dots, \omega^{m-1}\},$$

and  $\omega^i$  is a primitive  $m$ th root of unity if  $\gcd(m, i) = 1$ .

**Definition 14.7.** Let  $P_m = \{\text{primitive } m\text{th roots of unity}\}$ . The *cyclotomic polynomial*  $\Phi_m$  is

$$\Phi_m = \prod_{\varepsilon \in P_m} (X - \varepsilon).$$

# Lecture 15

## Mar. 6 — Cyclotomic Polynomials

### 15.1 Cyclotomic Polynomials

**Example 15.0.1.** For  $X^p - 1$  with  $p$  prime, all roots except 1 are primitive:

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

So we get  $\Phi_p = X^{p-1} + X^{p-2} + \cdots + 1$ .

**Example 15.0.2.** Consider  $f = X^{12} - 1$ , where  $L \subseteq \mathbb{C}$  is the splitting field of  $f$  over  $\mathbb{Q}$ . We have

$$P_{12} = \{\omega, \omega^5, \omega^7, \omega^{11}\},$$

the powers of  $\omega = e^{2\pi i/12}$  relatively prime to 12. This gives

$$\begin{aligned}\Phi_{12} &= (X - \omega)(X - \omega^{11})(X - \omega^5)(X - \omega^7) = (X^2 - (\omega + \omega^{11})X + 1)(X^2 - (\omega^5 + \omega^7)X + 1) \\ &= (X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1) = X^4 - X^2 + 1,\end{aligned}$$

since  $\omega^{11} = \bar{\omega}$  with  $\operatorname{Re}(\omega) = \sqrt{3}/2$  (a similar analysis works for  $\omega^5$  and  $\omega^7$ ). We have  $P_6 = \{\omega^2, \omega^{10}\}$ , so

$$(X - \omega^2)(X - \omega^{10}) = X^2 - (\omega^2 + \omega^{10})X + 1 = X^2 - X + 1$$

Next  $P_3 = \{\omega^3, \omega^9\} = \{\pm i\}$ , so

$$\Phi_4 = (X - i)(X + i) = X^2 + 1.$$

Now  $P_3 = \{\omega^4, \omega^8\}$ , so

$$\Phi_2 = (X - \omega^4)(X - \omega^8) = X^2 + X + 1.$$

Finally  $P_2 = \{\omega^6\}$ , so  $\Phi_2 = X + 1$ , and  $P_1 = \{1\} = \{\omega^{12}\}$ , so  $\Phi_1 = X - 1$ .

**Remark.** Observe that

$$X^{12} - 1 = \prod_{d|12} \Phi_d = (X - 1)(X + 1)(X^2 + X + 1)(X^2 + 1)(X^2 - X + 1)(X^4 - X^2 + 1).$$

This works in general, i.e.

$$X^m - 1 = \prod_{d|m} \Phi_d.$$

Note that we need  $1|m$  and  $m|m$  here.

**Remark.** The question here is: Does  $\Phi_d$  always have coefficients in  $K$ ?

**Lemma 15.1.** *Let  $K, L$  be fields and  $K \subseteq L$ . If  $f, g \in L[X]$  such that  $f, fg \in K[X]$ , then  $g \in K[X]$ .*

*Proof.* Let

$$f = a_0 + a_1X + \cdots + a_mX^m$$

for  $a_i \in K$ ,  $a_m \neq 0$ , and

$$g = b_0 + b_1X + \cdots + b_nX^n$$

for  $b_i \in L$ ,  $b_n \neq 0$ . Then

$$fg = c_0 + c_1X + \cdots + c_{m+n}X^{m+n}$$

for  $c_i \in K$ , so  $b_n = c_{m+n}/a_m \in K$ . Now suppose inductively that  $b_j \in K$  for all  $j > r$ . Then

$$c_{m+r} = a_mb_r + a_{m-1}b_{r+1} + \cdots + a_{m-n+r}b_n$$

where  $a_i = 0$  if  $i < 0$ . Then we get that

$$b_r = \frac{c_{m+r} - a_{m-1}b_{r+1} - \cdots - a_{m-n+r}b_n}{a_m}.$$

Since each  $a_i \in K$ ,  $c_{m+r} \in K$ , and  $b_j \in K$  for  $j > r$ , we get that  $b_r \in K$ . So in fact  $b_j \in K$  for all  $j$  by induction, and thus  $g \in K[X]$ .  $\square$

**Theorem 15.1.** *Let  $\text{char } K = 0$  (so the prime subfield  $K_0 \cong \mathbb{Q}$ ). Suppose  $K$  contains the  $m$ th roots of unity, where  $m \geq 2$ . Then for every divisor  $d$  of  $m$ ,  $\Phi_d \in K_0[X]$ .*

*Proof.* Note that  $\Phi_1 = X - 1 \in K_0[X]$ . Let  $d|m$ ,  $d \neq 1$ , and suppose inductively that  $\Phi_r \in K_0[X]$  for all proper divisors  $r$  of  $d$ . Now

$$X^d - 1 = \left( \prod_{r|d, r \neq d} \Phi_r \right) \Phi_d,$$

so Lemma 15.1 gives  $\Phi_d \in K_0[X]$ .  $\square$

**Remark.** In fact,  $\Phi_m \in \mathbb{Z}[X]$ .

**Theorem 15.2.** *The cyclotomic polynomials  $\Phi_m$  are irreducible over  $\mathbb{Q}$ .*

*Proof.* See Howie.  $\square$

## 15.2 The Galois Groups of Cyclotomic Polynomials

**Remark.** When we talk about the *Galois group of a polynomial*, we mean the Galois group of the splitting field of that polynomial.

**Theorem 15.3.** *Let  $L$  be a splitting field over  $\mathbb{Q}$  of  $X^m - 1$ . Then  $\text{Gal}(L : \mathbb{Q}) \cong \mathbb{Z}_m^*$ .*

*Proof.* Let  $\omega$  be a primitive  $m$ th root of unity and  $\sigma \in \text{Gal}(L : \mathbb{Q})$ . Since  $L = \mathbb{Q}(\omega)$ ,  $\sigma(\omega)$  must be another primitive  $m$ th root of unity, so  $\sigma \in \text{Gal}(L : \mathbb{Q})$  if and only if  $\sigma(\omega) = \omega^{k_\sigma}$  where  $\gcd(k_\sigma, m) = 1$ . Then  $\sigma \mapsto k_\sigma$  is an isomorphism  $\text{Gal}(L : \mathbb{Q}) \rightarrow \mathbb{Z}_m^*$ , so  $\text{Gal}(L : \mathbb{Q}) \cong \mathbb{Z}_m^*$ .  $\square$

**Exercise 15.1.** Show that the map  $\sigma \mapsto k_\sigma$  is an isomorphism  $\text{Gal}(L : \mathbb{Q}) \rightarrow \mathbb{Z}_m^*$ .

**Corollary 15.3.1.** *If  $L$  is a splitting field of  $X^p - 1$  over  $\mathbb{Q}$  with  $p$  prime, then  $\text{Gal}(L : \mathbb{Q})$  is cyclic.*

*Proof.* By Theorem 15.3,  $\text{Gal}(L : \mathbb{Q}) \cong \mathbb{Z}_p^*$ , which we have previously shown is cyclic.  $\square$

**Example 15.0.3.** Consider the splitting field  $\mathbb{Q}(\omega)$  of  $X^8 - 1$  over  $\mathbb{Q}$ , where  $\omega = e^{2\pi i/8} = e^{\pi i/4}$ . Then

$$\text{Gal}(\mathbb{Q}(\omega) : \mathbb{Q}) = \{\omega \mapsto \omega, \omega \mapsto \omega^3, \omega \mapsto \omega^5, \omega \mapsto \omega^7\} \cong \mathbb{Z}_8^*.$$

In particular,  $\text{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$  is not cyclic since every element has order 2.

**Example 15.0.4.** Consider the splitting field  $\mathbb{Q}(\omega)$  of  $X^5 - 1$  over  $\mathbb{Q}$ , where  $\omega = e^{2\pi i/5}$ . Then

$$\text{Gal}(\mathbb{Q}(\omega) : \mathbb{Q}) = \{\omega \mapsto \omega, \omega \mapsto \omega^2, \omega \mapsto \omega^3, \omega \mapsto \omega^4\} \cong \mathbb{Z}_5^*.$$

**Theorem 15.4.** *Let  $f = X^m - a \in K[X]$ , where  $\text{char } K = 0$ . Let  $L$  be a splitting for  $f$  over  $K$ . Then*

1.  $L$  contains a primitive  $m$ th root of unity  $\omega$ ,
2.  $\text{Gal}(L : K(\omega))$  is cyclic, with order dividing  $m$ ,
3. and  $|\text{Gal}(L : K(\omega))| = m$  if and only if  $f$  is irreducible over  $K(\omega)$ .

*Proof.* If  $\alpha$  is a root of  $f$ , then over  $L$  we have

$$f = (X - \alpha)(X - \omega\alpha)(X - \omega^2\alpha) \dots (X - \omega^{m-1}\alpha)$$

where  $\omega$  is a primitive  $m$ th root of unity. Since  $\alpha, \omega\alpha \in L$ , this proves (1). Thus  $L = K(\omega, \alpha)$ , and an element  $\sigma \in \text{Gal}(L : K(\omega))$  is determined by  $\sigma(\alpha)$ , which must be another root of  $f$ . Hence  $\sigma(\alpha) = \omega^{k_\sigma}\alpha$  for some  $k_\sigma \in \{0, 1, \dots, m-1\}$ . Now for  $\sigma, \tau \in \text{Gal}(L : K(\omega))$ ,

$$\sigma \circ \tau(\alpha) = \sigma(\omega^{k_\tau}\alpha) = \omega^{k_\tau}\sigma(\alpha) = \omega^{k_\tau}\omega^{k_\sigma}\alpha = \omega^{k_\sigma + k_\tau}\alpha,$$

so  $\sigma \mapsto k_\sigma$  is a homomorphism  $\text{Gal}(L : K(\omega)) \rightarrow \mathbb{Z}_m$ . This homomorphism is injective since

$$k_\sigma \equiv 0 \pmod{m}$$

if and only if  $m|k_\sigma$ , if and only if  $\sigma(\alpha) = \alpha$ . Hence  $\text{Gal}(L : K(\omega))$  is isomorphic to a subgroup of the cyclic group  $\mathbb{Z}_m$ , so  $\text{Gal}(L : K(\omega))$  is cyclic (subgroups of cyclic groups are cyclic). This proves (2).

(3) ( $\Leftarrow$ ) Suppose  $f$  is irreducible over  $K(\omega)$ . Then by the Galois correspondence

$$|\text{Gal}(L : K(\omega))| = [L : K(\omega)] = \partial f = m,$$

where the second equality follows from the characterization of simple algebraic extensions. So we get  $\text{Gal}(L : K(\omega)) \cong \mathbb{Z}_m$ , since we already showed that  $\text{Gal}(L : K(\omega))$  is isomorphic to a subgroup of  $\mathbb{Z}_m$ .

(3) ( $\Rightarrow$ ) We show the contrapositive. Suppose  $f$  is not irreducible over  $K(\omega)$ , so  $f$  has a monic proper factor  $g$  with  $\partial g < m$ . Let  $\beta$  be a root of  $g$ . Then

$$X^m - a = (X - \beta)(X - \omega\beta) \dots (X - \omega^{m-1}\beta),$$

so  $L = K(\omega, \beta)$  is a splitting field for  $f$  over  $K(\omega)$ . Hence

$$|\text{Gal}(L : K(\omega))| = [L : K(\omega)] = \partial g < m,$$

so the Galois group is a proper subgroup of  $\mathbb{Z}_m$ .  $\square$

**Theorem 15.5** (Abel's theorem). *Let  $\text{char } K = 0$ ,  $p$  prime, and  $a \in K$ . If  $X^p - a$  is reducible over  $K$ , then it has a linear factor  $X - c$  in  $K[X]$ .*

*Proof.* Suppose  $f = X^p - a$  is reducible over  $K$ . Let  $g \in K[X]$  be a monic irreducible factor of  $f$  of degree  $d$ . If  $d = 1$ , then we are done, so suppose  $1 < d < p$ . Let  $L$  be a splitting field of  $f$  over  $K$ , and  $\beta$  a root of  $f$  in  $L$ . Then in  $L[X]$ ,

$$g = (X - \omega^{n_1}\beta)(X - \omega^{n_2}\beta) \dots (X - \omega^{n_d}\beta)$$

where  $\omega$  is a primitive  $p$ th root of unity and  $0 \leq n_1 < n_2 < \dots < n_d < p$ . Suppose

$$g = X^d - b_{d-1}X^{d-1} + \dots + (-1)^d b_0.$$

Then we have

$$b_0 = \omega^{n_1+n_2+\dots+n_d}\beta^d = \omega^n \beta^d$$

where  $n = n_1 + n_2 + \dots + n_d$ . So

$$b_0^p = \omega^{pn} \beta^{pd} = (\beta^p)^d = a^d$$

since  $\omega^p = 1$  and  $\beta$  is a  $p$ th root of  $a$ . We have  $\gcd(d, p) = 1$  since  $p$  is prime, so there exist  $s, t \in \mathbb{Z}$  such that  $sd + tp = 1$ . Then since  $a^d = b_0^p$ , we get that

$$a = a^{sd+tp} = a^{sd} a^{tp} = b_0^{sp} a^{tp} = (b_0^s a^t)^p.$$

Now  $X - b_0^s a^t$  is the desired linear factor of  $f$  in  $K[X]$ . □

**Example 15.0.5.** Let  $L$  be the splitting field of  $X^5 - 7$  over  $\mathbb{Q}$ . We have  $L = \mathbb{Q}(\sqrt[5]{7}, \omega)$ , where  $\omega = e^{2\pi i/5}$ . Note that the minimum polynomial of  $\omega$  is  $X^4 + X^3 + X^2 + X + 1$ . What is  $\text{Gal}(L : \mathbb{Q})$ ? First we show that  $X^5 - 7$  is irreducible over  $\mathbb{Q}(\omega)$ . To do this, suppose not. Then by Abel's theorem,  $X^5 - 7$  has a linear factor  $X - c$  in  $\mathbb{Q}(\omega)[X]$ , i.e.  $c = \sqrt[5]{7} \in \mathbb{Q}(\omega)$  and  $[\mathbb{Q}(c) : \mathbb{Q}] = 5$ . But if  $c \in \mathbb{Q}(\omega)$ , then

$$[\mathbb{Q}(c) : \mathbb{Q}] \leq [\mathbb{Q}(\omega) : \mathbb{Q}] = 4,$$

a contradiction. Now notice that the roots of  $X^5 - 7$  in  $\mathbb{C}$  are

$$\alpha, \omega\alpha, \omega^2\alpha, \omega^3\alpha, \omega^4\alpha,$$

where  $\alpha = \sqrt[5]{7}$ . Since  $|\text{Gal}(L : \mathbb{Q})| = 20$ , define the maps

$$\sigma_{p,q} : \alpha \mapsto \omega^p \alpha, \quad \omega \mapsto \omega^q$$

for  $0 \leq p \leq 4$  and  $1 \leq q \leq 4$ . Then we can write

$$\text{Gal}(L : \mathbb{Q}) = \{\sigma_{p,q} \mid 0 \leq p \leq 4, 1 \leq q \leq 4\},$$

where the identity element is  $\text{id} = \sigma_{0,1}$ .

**Exercise 15.2.** Check that

$$\sigma_{p,q}\sigma_{r,s} = \sigma_{rq+p,qs}$$

in the above example, where the subscripts are taken modulo 5 (i.e. compute  $\sigma_{p,q}\sigma_{r,s}(\alpha)$  and  $\sigma_{p,q}\sigma_{r,s}(\omega)$ ).



# Lecture 16

## Mar. 11 — Solvable Polynomials

### 16.1 More on Cyclotomic Polynomials

**Exercise 16.1.** From Example 15.0.5, check that

$$(\sigma_{1,1})^n = \sigma_{n,1}, \quad (\sigma_{0,2})^n = \sigma_{0,2^n}, \quad \sigma_{2,1}\sigma_{0,2} = \sigma_{2,2} = \sigma_{0,2}\sigma_{1,1}.$$

Let  $a = \sigma_{1,1}$  and  $b = \sigma_{0,2}$ . Use the above to show that

$$\text{Gal}(L : \mathbb{Q}) = \langle a, b \mid a^5 = 1, b^4 = 1, a^2b = ba \rangle$$

is a presentation for  $\text{Gal}(L : \mathbb{Q})$  in terms of generators and relations.

**Theorem 16.1.** *Let  $\text{char } K = 0$  and suppose  $X^m - 1$  splits completely over  $K$ . Let  $L : K$  be a cyclic extension with  $[L : K] = m$ . Then there exists  $a \in K$  such that*

1.  $X^m - a$  is irreducible over  $K$ ,
2.  $L$  is a splitting field for  $X^m - a$  over  $K$ ,
3. and  $L = K(\alpha)$  where  $\alpha$  is a root of  $X^m - a$ .

*Proof.* See Howie. □

**Remark.** This is a partial converse to Theorem 15.4.

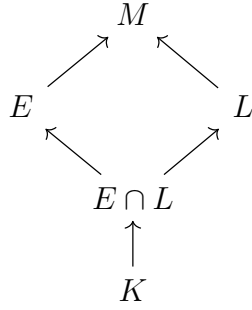
### 16.2 Solvable Polynomials

**Remark.** For  $f \in K[X]$ , we define  $\text{Gal}(f) = \text{Gal}(L : K)$  where  $L$  is a splitting field for  $f$  over  $K$ .

**Theorem 16.2.** *Let  $\text{char } K = 0$  and  $f \in K[X]$ . If  $\text{Gal}(f)$  is solvable, then  $f$  is solvable by radicals.*

*Proof.* Let  $L$  be a splitting field of  $f$  over  $K$ , where  $\text{Gal}(L : K)$  is solvable by hypothesis, and let  $m = |\text{Gal}(L : K)|$ . If  $K$  does not contain an  $m$ th root of unity, adjoin one, i.e. let  $E$  be the splitting

field of  $X^m - 1$  over  $K$ . Let  $M$  be the splitting field of  $f$  over  $E$ . This gives the subfield lattice:



By Theorem 7.36 of Howie, we get  $G = \text{Gal}(M : E) \cong \text{Gal}(L : E \cap L)$ . Now  $\text{Gal}(L : E \cap L) \subseteq \text{Gal}(L : K)$ , i.e.  $G$  is isomorphic to a subgroup of a solvable group, hence it is also solvable. So

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{r-1} \triangleleft G_r = G,$$

with  $G_{i+1}/G_i$  cyclic. By the fundamental theorem of Galois theory, we get

$$M_0 = M \supseteq M_1 \supseteq \cdots \supseteq M_{r-1} \supseteq M_r = E \supseteq K,$$

where  $M_i : M_{i+1}$  is normal. We have  $\text{Gal}(M : M_i) = G_i$ , so

$$\text{Gal}(M_i : M_{i+1}) \cong \text{Gal}(M : M_i) / \Gamma(M_i) \cong G_{i+1} / G_i,$$

which yields that  $M_i : M_{i+1}$  is cyclic. Let  $d_i = [M_i : M_{i+1}]$ . Then  $d_1 \mid [M : E] = \text{Gal}(M : E)$ . Now since  $\text{Gal}(M : E) \cong \text{Gal}(L : E \cap L)$ , we have that

$$|\text{Gal}(L : E \cap L)| \mid |\text{Gal}(L : K)| = m,$$

so  $d_1 \mid m$ . Since  $M_{i+1}$  contains  $E$ , it contains every  $m$ th root of unity, so  $E$  also contains all  $d_i$ th roots of unity. By Theorem 15.4, there exists  $\beta_i \in M_i$  such that  $M_i = M_{i+1}(\beta_i)$ , where  $\beta_i$  is a root of  $X^{d_i} - c_{i+1}$  with  $c_{i+1} \in M_{i+1}$ . Hence we get that  $f$  is solvable by radicals.  $\square$

**Theorem 16.3.** *Let  $\text{char } K = 0$  and  $K \subseteq L \subseteq M$  where  $M$  is a radical extension. Then  $\text{Gal}(L : K)$  is solvable.*

*Proof.* By hypothesis, there exists a sequence

$$M_r = M \supseteq M_{r-1} \supseteq \cdots \supseteq M_1 \supseteq M_0 = K,$$

where  $M_{i+1} = M_i(\alpha_i)$  with  $\alpha_i$  a root of  $X^{n_i} - a_i \in M_i[X]$ . The main idea from here is that if  $L : K$  and  $M : K$  are normal, then

$$\text{Gal}(L : K) \cong \text{Gal}(M : K) / \text{Gal}(M : L),$$

so it is sufficient to show that  $\text{Gal}(M : K)$  is solvable. Now use Theorem 8.18 and Corollary 8.14 from Howie to show that  $\text{Gal}(M : K)$  is solvable (uses induction). See Howie for details.  $\square$

**Theorem 16.4.** *A polynomial  $f \in K[X]$  with  $\text{char } K = 0$  is solvable by radicals if and only if  $\text{Gal}(f)$  is solvable.*

*Proof.* This is summarizing the previous two theorems.  $\square$

## 16.3 Insolvability of the Quintic

**Theorem 16.5.** *Let  $f \in \mathbb{Q}[X]$  be a monic irreducible polynomial with  $\partial f = p$ ,  $p$  prime. Suppose  $f$  has exactly two roots in  $\mathbb{C} \setminus \mathbb{R}$ . Then  $\text{Gal}(f) = S_p$ .*

*Proof.* Let  $L \subseteq \mathbb{C}$  be a splitting field for  $f$ . Now  $G = \text{Gal}(L : \mathbb{Q})$  is a subgroup of  $S_p$  since  $G$  is a group of permutations on the  $p$  roots of  $f$  in  $L$ . Consider  $\mathbb{Q}(\alpha)$ , where  $\alpha$  has minimum polynomial  $f$ . Then  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ , so we get that

$$|G| = |\text{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] \cdot p.$$

By the Sylow theorems,  $G$  has an element of order  $p$ .<sup>1</sup> Now  $G$  is a subgroup of  $S_p$ , and the only elements in  $S_p$  of order  $p$  are  $p$ -cycles, so  $G$  contains a  $p$ -cycle. Also complex roots of  $f$  come in conjugate pairs, so  $G$  contains a transposition  $\tau$  that swaps conjugate roots (there are only two complex roots of  $f$  in  $\mathbb{C} \setminus \mathbb{R}$ ). Then  $G$  is a subgroup of  $S_p$  that contains a  $p$ -cycle and a transposition, so by Homework 8,  $G = S_p$ .  $\square$

**Example 16.0.1.** Consider the polynomial  $f = X^5 - 8X + 2$ , which is irreducible over  $\mathbb{Q}$  by Eisenstein's criterion. Now we have:

$$\begin{array}{c|ccccc} X & -2 & -1 & 0 & 1 & 2 \\ \hline f(X) & -14 & 9 & 2 & -5 & 18 \end{array}$$

So by the intermediate value theorem,  $f$  has at least 3 real roots. Then  $f'(X) = 5X^4 - 8$ , and  $f'(X) \leq 0$  if and only if

$$-\sqrt[4]{\frac{8}{5}} \leq X \leq \sqrt[4]{\frac{8}{5}} \approx 1.12.$$

Rolle's theorem tells us that there exists at least one zero of  $f'(X)$  between zeroes of  $f(X)$ .<sup>2</sup> Thus  $f$  has exactly 3 real roots. Then by the previous theorem,  $\text{Gal}(f) = S_5$ , so  $f$  is not solvable by radicals since  $S_5$  is not solvable. So there exists a quintic polynomial which is not solvable by radicals.

## 16.4 Finitely-Generated Extensions

**Definition 16.1.** A subset  $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq L$  is *algebraically independent* over  $K$  if for all polynomials  $f(X_1, X_2, \dots, X_n)$  with coefficients in  $K$ , we have

$$f(\alpha_1, \alpha_2, \dots, \alpha_n) = 0 \iff f = 0..$$

**Example 16.1.1.** Notably, this is a stronger condition than linear independence. A non-example is  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ , which is linearly independent over  $\mathbb{Q}$  but not algebraically independent, since

$$\sqrt{2} \cdot \sqrt{3} - \sqrt{6} = 0.$$

This means we can take  $f(X_1, X_2, X_3, X_4) = X_2 \cdot X_3 - X_4$  to get  $f(1, \sqrt{2}, \sqrt{3}, \sqrt{6}) = \sqrt{2} \cdot \sqrt{3} - \sqrt{6} = 0$ .

**Exercise 16.2.** Show that  $\{\alpha_1, \dots, \alpha_n\}$  is algebraically independent over  $K$  if and only if  $\alpha_1$  is transcendental over  $K$  and for each  $2 \leq d \leq n$ ,  $\alpha_d$  is transcendental over  $K(\alpha_1, \dots, \alpha_{d-1})$ . Also show that this is if and only if

$$K(\alpha_1, \alpha_2, \dots, \alpha_n) \cong K(X_1, X_2, \dots, X_n).$$

<sup>1</sup>Cauchy's theorem directly gives this, but also  $|S_p| = p!$ , so the  $p$ -Sylow subgroup can only have order  $p$ .

<sup>2</sup>The above conditions guarantee that  $f'(X)$  has only two zeroes, so  $f(X)$  can have at most three.

**Definition 16.2.** An extension  $L$  of  $K$  is *finitely generated* if  $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$  for some natural number  $n$ .

**Example 16.2.1.** Finite extensions are finitely generated.

**Example 16.2.2.** The extension  $K(X)$  is finitely generated but not a finite extension.

**Theorem 16.6.** Let  $L = K(\alpha_1, \dots, \alpha_n)$  be a finitely generated extension of  $K$ . Then there exists a field  $E$  with  $K \subseteq E \subseteq L$  such that for some  $m$  with  $0 \leq m \leq n$ ,

1.  $E = K(\beta_1, \beta_2, \dots, \beta_m)$ , where  $\{\beta_1, \beta_2, \dots, \beta_m\}$  are algebraically independent,
2. and  $[L : E]$  is finite.

*Proof.* If all the  $\alpha_i$  are algebraic over  $K$ , then  $[L : K]$  is finite and we can take  $E = K$  with  $m = 0$ . Otherwise, there exists  $\alpha_i$  that is transcendental over  $K$ . Let  $\beta_1 = \alpha_i$ . If  $[L : K(\beta_1)]$  is not finite, then there exists  $\alpha_j$  that is transcendental over  $K(\beta_1)$ . Let  $\beta_2 = \alpha_j$ , and so on. Repeat this process, which terminates in at most  $n$  steps, so

$$E = K(\beta_1, \beta_2, \dots, \beta_m)$$

with  $m \leq n$ . By construction,  $\{\beta_1, \dots, \beta_m\}$  are algebraically independent over  $K$  and  $[L : E]$  is finite.  $\square$

**Remark.** We can think of this theorem as saying that  $E$  is the “transcendental part” of the extension.

**Remark.** The elements  $\beta_i$  are not unique, but the number  $m$  is determined uniquely by  $L$  and  $K$ .

# Lecture 17

## Mar. 13 — Symmetric Polynomials

### 17.1 Transcendental Extensions

**Theorem 17.1.** Let  $K, L, m, E, \beta_1, \dots, \beta_m$  be as defined in Theorem 16.6. If  $K \subseteq F \subseteq L$  and

1.  $F = K(\gamma_1, \gamma_2, \dots, \gamma_p)$  where  $\{\gamma_1, \gamma_2, \dots, \gamma_p\}$  are algebraically independent over  $K$ ,
2.  $[L : F]$  is finite,

then  $p = m$ .

*Proof.* Suppose  $p > m$ . Since  $[L : E]$  is finite,  $\gamma_1$  is algebraic over  $E$ , so  $\gamma_1$  is the root of a polynomial with coefficients in  $E = K(\beta_1, \dots, \beta_m)$ . In other words, there exists a nonzero polynomial  $f$  with coefficients in  $K$  such that

$$f(\beta_1, \dots, \beta_m, \gamma_1) = 0.$$

Since  $\gamma_1$  is transcendental over  $K$ , at least one  $\beta_i$  (without loss of generality say  $\beta_1$ ) must show up in this polynomial. Hence  $\beta_1$  is algebraic over  $K(\beta_2, \beta_3, \dots, \beta_m, \gamma_1)$  and  $[L : K(\beta_2, \dots, \beta_m, \gamma_1)]$  is finite. Repeat this argument, replacing each  $\beta_i$  with  $\gamma_i$ , so  $[L : K(\gamma_1, \dots, \gamma_m)]$  is finite. Recall that  $p > m$  by assumption. But  $\gamma_{m+1}$  is transcendental over  $K(\gamma_1, \dots, \gamma_m)$ , a contradiction. Thus we must have  $p \leq m$ .

We also get  $m \leq p$  for free by symmetry, so we conclude that  $p = m$ .  $\square$

**Definition 17.1.** The  $m$  in Theorem 16.6 is called the *transcendence degree* of  $L : K$ .

### 17.2 Symmetric Polynomials

**Definition 17.2.** Let  $L = K(t_1, t_2, \dots, t_n)$  where  $\{t_1, \dots, t_n\}$  are algebraically independent over  $K$ . For  $\sigma \in S_n$ , define the  $K$ -automorphism  $\varphi_\sigma : L \rightarrow L$  by  $\varphi_\sigma(t_i) = t_{\sigma(i)}$ , i.e. it permutes the  $t_i$ 's by  $\sigma$ . Let

$$\text{Aut}_n = \{\varphi_\sigma \mid \sigma \in S_n\}.$$

**Example 17.2.1.** If  $\sigma = (1\ 2\ 3)$ , then we have

$$\varphi_\sigma \left( \frac{t_1 + t_2}{t_3} \right) = \frac{t_2 + t_3}{t_1}.$$

**Exercise 17.1.** Show that the map  $\sigma \mapsto \varphi_\sigma$  is an isomorphism  $S_n \rightarrow \text{Aut}_n$ .

**Example 17.2.2.** What is  $\Phi(\text{Aut}_n)$ , the fixed field of  $\text{Aut}_n$ ? Certainly  $\Phi(\text{Aut}_n)$  includes all of

$$\begin{aligned} s_1 &= t_1 + t_2 + \cdots + t_n, \\ s_2 &= t_1 t_2 + t_1 t_3 + \cdots + t_{n-1} t_n, \\ &\vdots \\ s_n &= t_1 t_2 \cdots t_n. \end{aligned}$$

We call these the *elementary symmetric polynomials*. All rational combinations of the  $s_i$  are also fixed.

**Exercise 17.2.** Show

$$X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n = \prod_{i=1}^n (X - t_i).$$

**Example 17.2.3.** The sum of the squares of the  $t_i$  is fixed by  $\text{Aut}_n$ . We can also see that

$$t_1^2 + t_2^2 + \cdots + t_n^2 = s_1^2 - 2s_2.$$

**Theorem 17.2.** *The fixed field of  $\text{Aut}_n$  is precisely  $\Phi(\text{Aut}_n) = K(s_1, s_2, \dots, s_n)$ .*

*Proof.* We claim  $[K(t_1, \dots, t_n) : K(s_1, \dots, s_n)] \leq n!$ . The proof follows since  $K(s_1, \dots, s_n) \subseteq \Phi_n(\text{Aut}_n)$  and we have<sup>1</sup>

$$[K(t_1, \dots, t_n) : \Phi_n(\text{Aut}_n)] = |\text{Aut}_n| = n!.$$

So it suffices to prove the claim to finish.

We show the claim by induction on  $n$ . The base case  $n = 1$  is clear. Now for the inductive step, suppose we have

$$K(t_1, \dots, t_n) \supseteq K(s_1, \dots, s_n, t_n) \supseteq K(s_1, \dots, s_n).$$

Note that

$$f(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n = (X - t_1) \cdots (X - t_n)$$

over  $K(t_1, \dots, t_n)$ , so the minimum polynomial of  $t_n$  over  $K(s_1, \dots, s_n)$  divides  $f$ . So we get

$$[K(t_1, \dots, t_n) : K(s_1, \dots, s_n)] \leq n. \quad (\star)$$

Now let  $s'_1, \dots, s'_{n-1}$  be the elementary symmetric polynomials in  $t_1, \dots, t_{n-1}$ , and notice that

$$\begin{aligned} s'_1 &= t_1 + t_2 + \cdots + t_{n-1}, \\ s_2 &= s'_1 + t_n \\ &\vdots \\ s_j &= s'_j + s'_{j-1} t_n, \\ &\vdots \\ s_n &= s'_{n-1} t_n. \end{aligned}$$

So  $K(s_1, \dots, s_n) = K(s'_1, \dots, s'_{n-1}, t_n)$  and so

$$\begin{aligned} [K(t_1, \dots, t_n) : K(s_1, \dots, s_n t_n)] &= [K(t_1, \dots, t_n) : K(s'_1, \dots, s'_{n-1}, t_n)] \\ &= [K(t_n)(t_1, \dots, t_{n-1}) : K(t_n)(s'_1, \dots, s'_{n-1})] \leq (n-1)! \end{aligned}$$

by the inductive hypothesis. So this combined with  $(\star)$  completes the inductive step.  $\square$

<sup>1</sup>Note that  $K(s_1, \dots, s_n) \subseteq \Phi(\text{Aut}_n) \subseteq K(t_1, \dots, t_n)$ .

**Theorem 17.3.** *The elementary symmetric polynomials  $s_1, \dots, s_n$  are algebraically independent.*

*Proof.* We have  $[K(t_1, \dots, t_n) : K(s_1, \dots, s_n)]$  is finite since  $t_1, \dots, t_n$  are roots of

$$X^n - s_1 X^{n-1} + \dots + (-1)^n s_n.$$

Hence  $K(t_1, \dots, t_n)$  and  $K(s_1, \dots, s_n)$  have the same transcendence degree over  $K$ , namely  $n$ , so we get that  $s_1, \dots, s_n$  must be algebraically independent.  $\square$

**Definition 17.3.** The *general polynomial* of degree  $n$  over  $K$  is

$$f = X^n - s_1 X^{n-1} + \dots + (-1)^n s_n.$$

**Remark.** Note that:

1. The coefficients live in  $K(s_1, \dots, s_n)$ .
2. For now,  $s_i$  are just algebraically independent elements.

**Theorem 17.4.** *Let  $\text{char } K = 0$  and  $f$  as above. Let  $L$  be a splitting field for  $f$  over  $K(s_1, \dots, s_n)$ . Then*

1. *the zeros  $t_1, \dots, t_n$  of  $f$  in  $L$  are algebraically independent over  $K$ ,*
2. *and  $\text{Gal}(L : K(s_1, \dots, s_n)) = S_n$ .*

*Proof.* Note that  $[L : K(s_1, \dots, s_n)]$  is finite, so the transcendence degree of  $L$  over  $K$  is the transcendence degree of  $K(s_1, \dots, s_n)$  over  $K$ , which is  $n$ . So  $L = K(t_1, \dots, t_n)$ , which means that  $t_1, \dots, t_n$  must be algebraically independent. Then we have that

$$X^n - s_1 X^{n-1} + \dots + (-1)^n s_n = \prod_{i=1}^n (X - t_i),$$

so  $s_1, \dots, s_n$  are precisely the elementary symmetric polynomials in  $t_1, \dots, t_n$ . So by Theorem 10.8 from Howie, we get  $\Phi(\text{Aut}_n) = K(s_1, \dots, s_n)$ . From here we have

$$[L : K(s_1, \dots, s_n)] = [L : \Phi(\text{Aut}_n)] = |\text{Aut}_n| = |S_n| = n!,$$

so  $\text{Gal}(L : K(s_1, \dots, s_n)) \cong S_n$ .  $\square$

**Corollary 17.4.1.** *If  $\text{char } K = 0$  and  $n \geq 5$ , then the general polynomial*

$$X^n - s_1 X^{n-1} + \dots + (-1)^n s_n$$

*is not solvable by radicals.*

**Corollary 17.4.2.** *Every finite group is the Galois group of some field extension.*

*Proof.* Recall that by Cayley's theorem, every finite group is a subgroup of  $S_n$  for some  $n$ . By Theorem 17.4, we can realize  $S_n$  as the Galois group of  $L : K(s_1, \dots, s_n)$ . The fundamental theorem of Galois theory then says that for every subgroup  $G$  of  $S_n$ , there exists a subfield  $M$  of  $L$  containing  $K(s_1, \dots, s_n)$  such that  $G = \text{Gal}(L : M)$ .  $\square$

**Remark.** In the above theorem, we kind of lost control of the ground field, which is just some field  $M$ . Given a finite group  $G$ , is it the Galois group of a Galois extension over  $\mathbb{Q}$ ? Equivalently, does there exist  $f \in \mathbb{Q}[X]$  such that  $G = \text{Gal}(f)$ ? If so, we say that  $G$  is *realizable* (over  $\mathbb{Q}$ ). This is known as the *inverse Galois problem*.

**Remark.** In 1956, Shafarevich showed that every solvable group is realizable. An open question is: Is every finite simple group realizable?



# Lecture 18

## Mar. 25 — Modules

### 18.1 Introduction to Modules

**Remark.** Let  $(G, +)$  be an abelian group. Recall that given  $n \in \mathbb{Z}$ , we defined

$$ng = \begin{cases} g + \cdots + g & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ (-g) + \cdots + (-g) & \text{if } n < 0, \end{cases}$$

where we add  $g$  or its inverse  $n$  times. This gives a map  $\mathbb{Z} \times G \rightarrow G$  by  $(n, g) \mapsto ng$  that satisfies

1.  $(n_1 n_2)g = n_1(n_2 g)$ ,
2.  $(n_1 + n_2)g = n_1 g + n_2 g$ ,
3. and  $n(g_1 + g_2) = ng_1 + ng_2$ .

From this, we would say that every abelian group  $G$  is naturally a  $\mathbb{Z}$ -module.

**Definition 18.1.** A *module*  $M$  over a ring  $R$  is an abelian group  $M$  together with a map  $R \times M \rightarrow M$ , called the *product*, satisfying

1.  $(r_1 r_2)m = r_1(r_2 m)$ ,
2.  $(r_1 + r_2)m = r_1 m + r_2 m$ ,
3.  $r(m_1 + m_2) = rm_1 + rm_2$ ,
4. and  $1m = m$ .

**Remark.** For this class, we will only consider modules over commutative rings with unity.

**Exercise 18.1.** Verify the following:

1.  $0m = 0$ ,  $r0 = 0$ ,
2.  $r(-m) = -(rm) = (-r)m$ ,
3.  $(-1)m = -m$ .

**Example 18.1.1.** A  $K$ -vector space is a module over  $K$ , where  $K$  is a field.

**Example 18.1.2.** A ring  $R$  is always a module over itself, where the product  $R \times R \rightarrow R$  is the normal ring multiplication in  $R$ .

**Example 18.1.3.** An ideal  $I$  in a ring  $R$  is a module over  $R$ . The product  $R \times I \rightarrow I$  is given by  $(r, m) \mapsto rm$ , where  $rm \in I$  since  $I$  is an ideal.

**Example 18.1.4.** The set  $R^n = R \times \cdots \times R$  is an  $R$ -module, where the product is given by

$$r(r_1, r_2, \dots, r_n) = (rr_1, rr_2, \dots, rr_n).$$

## 18.2 Submodules

**Definition 18.2.** A  $R$ -submodule of an  $R$ -module  $M$  is a subgroup  $W$  of  $M$  such that for all  $r \in R$  and  $w \in W$ , we have  $rw \in W$ .

**Example 18.2.1.** Recall that  $R$  is a module over itself. Then any ideal of  $R$  is a submodule, and conversely, any submodule is an ideal.

**Proposition 18.1.** Let  $M$  be an  $R$ -module.

1. If  $\{M_\alpha\}$  is a collection of submodules of  $M$ , then  $\bigcap_\alpha M_\alpha$  is also a submodule.
2. If  $M_1 \subseteq M_2 \subseteq \dots$  is an increasing sequence of submodules, then  $\bigcup_n M_n$  is a submodule.
3. If  $A$  and  $B$  are submodules of  $M$ , then  $A + B = \{a + b \mid a \in A, b \in B\}$  is a submodule of  $M$ .

*Proof.* Left as an exercise. □

**Definition 18.3.** Let  $M$  be an  $R$ -module and  $S$  a subset of  $M$ . The submodule of  $M$  generated by  $S$  is

$$RS = \{r_1s_1 + r_2s_2 + \cdots + r_ns_n \mid r_i \in R, s_i \in S, n \in \mathbb{N}\}.$$

**Exercise 18.2.** Verify that  $RS$  is a submodule.

**Example 18.3.1.** If  $S = \{x\}$  for some  $x \in M$ , then  $R\{x\}$  is the *cyclic module* generated by  $x$ .

**Definition 18.4.** If there exists  $x \in M$  such that  $M = R\{x\}$ , then we say  $M$  is *cyclic*. If there exists a finite set  $S \subseteq M$  such that  $M = RS$ , then  $M$  is *finitely generated*.

## 18.3 Module Homomorphisms

**Definition 18.5.** Let  $M$  and  $N$  be  $R$ -modules. Then an  $R$ -module *homomorphism*  $\varphi : M \rightarrow N$  is a homomorphism of abelian groups such that  $\varphi(rm) = r\varphi(m)$  for all  $r \in R$  and  $m \in M$ .

**Definition 18.6.** An  $R$ -module *isomorphism* is a bijective  $R$ -module homomorphism. An  $R$ -module *endomorphism* is an  $R$ -module homomorphism from  $M$  to itself.

**Remark.** The set of all  $R$ -module homomorphisms from  $M$  to  $N$  is denoted  $\text{Hom}_R(M, N)$ , and the set of all  $R$ -module endomorphisms of  $M$  is denoted  $\text{End}_R(M)$ .

**Definition 18.7.** The *kernel* of an  $R$ -module homomorphism  $\varphi \in \text{Hom}_R(M, N)$  is

$$\ker \varphi = \{x \in M \mid \varphi(x) = 0\}.$$

**Example 18.7.1.** Let  $M = R^m$  and  $N = R^n$ , thought of as column vectors. Let  $T$  be a fixed  $n \times m$  matrix with entries in  $R$ . Then left multiplication by  $T$  is an  $R$ -module homomorphism from  $M$  to  $N$ .

## 18.4 Direct Sums of Modules

**Definition 18.8.** The *direct sum* of  $R$ -modules  $M_1, \dots, M_n$ , denoted

$$M_1 \oplus \cdots \oplus M_n,$$

is the product  $M_1 \times \cdots \times M_n$  endowed with the operations

$$(x_1, \dots, x_n) + (x'_1, \dots, x'_n) = (x_1 + x'_1, \dots, x_n + x'_n) \quad \text{and} \quad r(x_1, \dots, x_n) = (rx_1, \dots, rx_n).$$

**Remark.** Note that  $M_i$  is naturally isomorphic to the following submodule of  $M_1 \oplus \cdots \oplus M_n$ :

$$\widetilde{M}_i = \{0\} \oplus \cdots \oplus M_i \oplus \cdots \oplus \{0\},$$

and  $M = \widetilde{M}_1 + \cdots + \widetilde{M}_n = \{m_1 + \cdots + m_n \mid m_i \in \widetilde{M}_i\}$ .

**Proposition 18.2.** Let  $M$  be an  $R$ -module with submodules  $A_1, \dots, A_s$  such that  $M = A_1 + \cdots + A_s$ . Then the following are equivalent:

1.  $(a_1, \dots, a_s) \mapsto a_1 + \cdots + a_s$  is a group isomorphism  $A_1 \times \cdots \times A_s \rightarrow M$ .
2.  $(a_1, \dots, a_s) \mapsto a_1 + \cdots + a_s$  is an  $R$ -module isomorphism  $A_1 \times \cdots \times A_s \rightarrow M$ .
3. Each element  $x \in M$  can be expressed as a sum

$$x = a_1 + \cdots + a_s$$

with  $a_i \in A_i$  in exactly one way.

4. If  $0 = a_1 + \cdots + a_s$  with  $a_i \in A_i$ , then  $a_i = 0$  for all  $i$ .

*Proof.* (2)  $\Rightarrow$  (1) This is clear since an  $R$ -module isomorphism is also a group isomorphism.

(1)  $\Rightarrow$  (2) Let  $\varphi : A_1 \times \cdots \times A_s \rightarrow M$  be the given group isomorphism. Then

$$\varphi(r(a_1, \dots, a_s)) = \varphi(ra_1, \dots, ra_s) = ra_1 + \cdots + ra_s = r(a_1 + \cdots + a_s) = r\varphi(a_1, \dots, a_s),$$

so  $\varphi$  is also an  $R$ -module isomorphism.

Now observe that (1), (3), (4) say nothing about the module structure of  $R$ , so from here (1)  $\Leftrightarrow$  (3)  $\Leftrightarrow$  (4) is just an exercise in group theory.  $\square$

**Example 18.8.1.** Let  $M = \mathbb{Z}_6$  with  $R = \mathbb{Z}$ , and let  $A_1 = \{0, 2, 4\}$  and  $A_2 = \{0, 3\}$ . Then the map  $A_1 \oplus A_2 \rightarrow M$  given by

$$(a_1, a_2) \mapsto a_1 + a_2.$$

We can see that this is an isomorphism since  $A_1 \cong \mathbb{Z}_3$  and  $A_2 \cong \mathbb{Z}_2$ .

**Definition 18.9.** A subset  $S \subseteq M$  is *linearly independent* over  $R$  if for any distinct  $x_1, \dots, x_n \in S$ ,

$$r_1x_1 + \cdots + r_nx_n = 0$$

if and only if  $r_i = 0$  for all  $i$ .

**Definition 18.10.** A *basis* for  $M$  is a linearly independent set  $S$  with  $RS = M$ . An  $R$ -module  $M$  is called *free* if it has a basis.

**Example 18.10.1.** Every vector space over a field  $K$  is free as a  $K$ -module.

**Example 18.10.2.** Note that  $\mathbb{Z}_n$  is not a free  $\mathbb{Z}$ -module since  $na = 0$  for all  $a \in \mathbb{Z}_n$ . So  $\{a\}$  for  $a \neq 0$  is in fact linearly dependent. More generally, any finite abelian group  $G$  is not a free  $\mathbb{Z}$ -module.

**Example 18.10.3.** However,  $\mathbb{Z}$  is a free  $\mathbb{Z}$ -module. In general,  $R^n$  is a free  $R$ -module. The *standard basis* for  $R^n$  is the set  $\{e_1, \dots, e_n\}$  where

$$e_1 = (1, 0, 0, \dots, 0), \quad \dots, \quad e_n = (0, 0, 0, \dots, 1).$$

**Definition 18.11.** Let  $M$  be an  $R$ -module and  $B = \{x_1, \dots, x_n\}$  be distinct nonzero elements in  $M$ . Then the following are equivalent:

1.  $B$  is a basis for  $M$ .
2. The map  $\varphi : (r_1, \dots, r_n) \mapsto r_1x_1 + \dots + r_nx_n$  is an  $R$ -module isomorphism from  $R^n$  to  $M$ .
3. For each  $i$ , the map  $R \rightarrow M$  given by  $r \mapsto rx_i$  is injective and  $M = Rx_1 \oplus \dots \oplus Rx_n$ .

*Proof.* (1)  $\Leftrightarrow$  (2) Observe that  $B$  is linearly independent if and only if  $\varphi$  is injective and  $B$  spans  $M$  if and only if  $\varphi$  is surjective. Now check as an exercise that  $\varphi$  is an  $R$ -module homomorphism.

(1)  $\Leftrightarrow$  (3) Left as an exercise. □

**Proposition 18.3.** *We have the following:*

1. If  $\varphi \in \text{Hom}_R(M, N)$ , then  $\ker \varphi$  is a submodule of  $M$  and  $\varphi(M)$  is a submodule of  $N$ .
2. If  $\varphi \in \text{Hom}_R(M, N)$  and  $\psi \in \text{Hom}_R(N, P)$ , then  $\psi \circ \varphi \in \text{Hom}_R(M, P)$ .

*Proof.* (1) We need to show that if  $m \in \ker \varphi$  and  $r \in R$ , then  $rm \in \ker \varphi$ . For this, observe that

$$\varphi(rm) = r\varphi(m) = r0 = 0$$

since  $m \in \ker \varphi$ , so we have  $rm \in \ker \varphi$ . The rest of the proof is left as an exercise. □

**Proposition 18.4.** *We have the following:*

1.  $\text{Hom}_R(M, N)$  is an abelian group with the operation

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m).$$

2.  $\text{End}_R(M)$  is a ring with addition as above and multiplication given by composition.

*Proof.* (1) Clearly the addition is associative and commutative. The identity element is the zero map, and the inverse of  $\varphi$  is  $-\varphi$ , i.e. if  $\varphi : m \mapsto n$ , then  $-\varphi : m \mapsto -n$ .

(2) Left as an exercise (the multiplicative identity is the identity map  $\text{id}_M$ ). □

**Remark.** Many of the usual facts about group and ring homomorphisms have module analogues.

**Proposition 18.5.** *Let  $M$  be an  $R$ -module and  $N$  an  $R$ -submodule. Then the quotient group  $M/N$  is an  $R$ -module and the quotient map  $\pi : M \rightarrow M/N$  is an  $R$ -module homomorphism.*

*Proof.* Define the product  $R \times M/N \rightarrow M/N$  by

$$r(m + N) = rm + N.$$

To see that this product is well-defined, observe that if  $m + N = m' + N$ , then  $m - m' \in N$ . Hence

$$rm - rm' = r(m - m') \in N$$

since  $N$  is an  $R$ -submodule. Thus  $rm + N = rm' + N$  as desired. Now check as an exercise that this makes  $M/N$  into an  $R$ -module.

For the latter part about the quotient map  $\pi : M \rightarrow M/N$ , simply observe that

$$\pi(rm) = rm + N = r(m + N) = r\pi(m),$$

so indeed  $\pi$  is an  $R$ -module homomorphism. □

# Lecture 19

## Mar. 27 — Multilinear Functions

### 19.1 The Homomorphism Theorem

**Theorem 19.1** (Homomorphism theorem). *Let  $\varphi : M \rightarrow \overline{M}$  be a surjective  $R$ -module homomorphism with kernel  $N$ . Then  $\varphi$  descends to an homomorphism on the quotient  $M/N$ , i.e. there exists  $\tilde{\varphi} : M/N \rightarrow \overline{M}$  such that the following diagram commutes (i.e.  $\varphi = \tilde{\varphi} \circ \pi$ ):*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & \overline{M} \\ \pi \downarrow & \nearrow \tilde{\varphi} & \\ M/N & & \end{array}$$

*In particular,  $\tilde{\varphi}$  is an  $R$ -module isomorphism.*

*Proof.* Define  $\tilde{\varphi} : M/N \rightarrow \overline{M}$  by  $\tilde{\varphi}(m + N) = \varphi(m)$  for any  $m \in M$ . To see that  $\tilde{\varphi}$  is well-defined, suppose  $m + N = m' + N$ . Then  $m' = m + n$  for some  $n \in N$ , so

$$\tilde{\varphi}(m' + N) = \varphi(m') = \varphi(m + n) = \varphi(m) + \varphi(n) = \varphi(m) = \tilde{\varphi}(m + N)$$

since  $n \in N = \ker \varphi$ . So  $\tilde{\varphi}$  is well-defined. Now by the usual first isomorphism theorem for groups,  $\tilde{\varphi}$  is a group homomorphism. To see that  $\tilde{\varphi}$  also respects  $R$ -actions, observe that

$$\tilde{\varphi}(r(m + N)) = \tilde{\varphi}(rm + N) = \varphi(rm) = r\varphi(m) = r\tilde{\varphi}(m + N)$$

So  $\tilde{\varphi}$  is an  $R$ -module homomorphism. We also get that  $\tilde{\varphi}$  is bijective for free by the first isomorphism theorem for groups. Thus  $\tilde{\varphi}$  is an  $R$ -module isomorphism.  $\square$

**Example 19.0.1.** Let  $M$  be an  $R$ -module and let  $x \in M$ . Consider the cyclic submodule

$$R_x = \{rx \mid r \in R\}.$$

Then  $\varphi : R \rightarrow R_x$  defined by  $r \mapsto rx$  is an  $R$ -module homomorphism (and is surjective). The kernel  $\ker \varphi$  is called the *annihilator* of  $x$ , denoted  $\text{ann}(x)$ . Then by the homomorphism theorem,  $R/\text{ann}(x) \cong R_x$ .

**Example 19.0.2.** Let  $R = \mathbb{Z}$  and  $M = \mathbb{Z}/n\mathbb{Z}$ . Let  $x = 1$ . Then  $\text{ann}(x) = n\mathbb{Z} = \ker \varphi$  where  $\varphi : \mathbb{Z} \rightarrow R_x$  is defined by  $r \mapsto rx$ . Then by the homomorphism theorem,  $\mathbb{Z}/n\mathbb{Z} \cong R/\text{ann}(x) \cong R_x = M \cong \mathbb{Z}/n\mathbb{Z}$ .

## 19.2 Multilinear Functions

**Definition 19.1.** Let  $M_1, \dots, M_n, N$  be  $R$ -modules. We say that a function  $\varphi : M_1 \times \dots \times M_n \rightarrow N$  is *R-multilinear* (or just *multilinear*) if for each  $j$  and fixed  $x_i \in M_i$  for  $i \neq j$ , the map  $M_j \rightarrow N$  given by

$$x \mapsto \varphi(x_1, \dots, x_{j-1}, x, x_{j+1}, \dots, x_n)$$

is an  $R$ -module homomorphism.

**Exercise 19.1.** If  $\varphi : M_1 \times M_2 \rightarrow N$  is multilinear, then

1.  $\varphi(m_1 + m'_1, m_2) = \varphi(m_1, m_2) + \varphi(m'_1, m_2)$ ,
2.  $\varphi(m_1, m_2 + m'_2) = \varphi(m_1, m_2) + \varphi(m_1, m'_2)$ ,
3.  $\varphi(rm_1, m_2) = r\varphi(m_1, m_2)$ ,
4. and  $\varphi(m_1, rm_2) = r\varphi(m_1, m_2)$ .

**Remark.** We will focus on the case where all the  $M_i$ 's are the same, i.e.  $\varphi : M^n \rightarrow N$ .

**Remark.** Recall that a permutation  $\sigma \in S_n$  is *even* (respectively *odd*) if it can be expressed as a product of an even (respectively odd) number of transpositions. We say that the *sign* of  $\sigma$  is

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Note that the sign  $\varepsilon : S_n \rightarrow \{\pm 1\}$  is in fact a group homomorphism.

**Example 19.1.1.** The permutation  $(123) = (12)(23)$  is even and the permutation  $(12)$  is odd.

**Definition 19.2.** We say that an  $R$ -multilinear function  $\varphi : M^n \rightarrow N$  is *symmetric*<sup>1</sup> if

$$\varphi(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \varphi(x_1, x_2, \dots, x_n)$$

for all  $x_1, \dots, x_n \in M$  and  $\sigma \in S_n$ . We say that  $\varphi$  is *skew-symmetric*<sup>2</sup> if

$$\varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma)\varphi(x_1, \dots, x_n)$$

for all  $x_1, \dots, x_n \in M$  and  $\sigma \in S_n$ . We say that  $\varphi$  is *alternating* if

$$\varphi(x_1, \dots, x_n) = 0$$

whenever  $x_i = x_j$  for some  $i \neq j$ .

**Example 19.2.1.** Let  $M = \mathbb{Z}^2$ , where we write  $x_1, x_2 \in M$  as

$$x_1 = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \quad \text{and} \quad x_2 = \begin{bmatrix} a_2 \\ b_2 \end{bmatrix},$$

where  $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ . Consider the map  $\varphi : M^2 \rightarrow \mathbb{Z}$  defined by

$$\varphi(x_1, x_2) = \begin{bmatrix} a_1 & b_1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \end{bmatrix} \begin{bmatrix} 2a_2 + b_2 \\ a_2 + 5b_2 \end{bmatrix} = 2a_1a_2 + a_1b_2 + b_1a_2 + 5b_1b_2.$$

<sup>1</sup>Recall that a matrix  $A$  is *symmetric* if  $A^T = A$ .

<sup>2</sup>Recall that a matrix  $A$  is *skew-symmetric* if  $A^T = -A$ .

Now observe that

$$\varphi(x_2, x_1) = \begin{bmatrix} a_2 & b_2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \end{bmatrix} \begin{bmatrix} 2a_1 + b_1 \\ a_1 + 5b_1 \end{bmatrix} = 2a_1a_2 + a_2b_1 + b_2a_1 + 5b_2b_1,$$

so  $\varphi(x_1, x_2) = \varphi(x_2, x_1)$  and in fact  $\varphi$  is symmetric. Notice the the matrix we picked was symmetric.

**Example 19.2.2.** Taking the matrix

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

makes  $\varphi$  in the above example skew-symmetric (and alternating). Notice that  $A$  is skew-symmetric.

**Lemma 19.1.** *The symmetric group  $S_n$  acts on the set of  $R$ -multilinear functions from  $M^n \rightarrow N$  by*

$$\sigma\varphi(x_1, \dots, x_n) = \varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

*Additionally, the sets of symmetric, skew-symmetric, and alternating multilinear functions are invariant under this action.*

*Proof.* Check as an exercise that  $\text{id}$  acts as it's supposed to. To see that  $\sigma(\tau\varphi) = (\sigma\tau)\varphi$  for all  $\sigma, \tau \in S_n$ , observe that

$$\sigma(\tau\varphi)(x_1, \dots, x_n) = (\tau\varphi)(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = (\tau\varphi)(y_1, \dots, y_n)$$

if we let  $y_i = x_{\sigma(i)}$ . Then  $y_{\tau(j)} = x_{\sigma(\tau(j))} = x_{(\sigma\tau)(j)}$ , and thus

$$\begin{aligned} \sigma(\tau\varphi)(x_1, \dots, x_n) &= (\tau\varphi)(y_1, \dots, y_n) \\ &= \varphi(y_{\tau(1)}, \dots, y_{\tau(n)}) = \varphi(x_{(\sigma\tau)(1)}, \dots, x_{(\sigma\tau)(n)}) = (\sigma\tau)\varphi(x_1, \dots, x_n). \end{aligned}$$

So we indeed have a group action (technically still need to check that  $\sigma\varphi$  is still multilinear). The rest of the proof (if  $\varphi$  is symmetric, skew-symmetric, or alternating, then so is  $\sigma\varphi$ ) is left as an exercise.  $\square$

**Remark.** We see that  $\varphi$  is symmetric if and only if  $\sigma\varphi = \varphi$  for all  $\sigma \in S_n$ , and  $\varphi$  is skew-symmetric if and only if  $\sigma\varphi = \varepsilon(\sigma)\varphi$  for all  $\sigma \in S_n$ .

**Lemma 19.2.** *An alternating multilinear function  $\varphi : M^n \rightarrow N$  is skew-symmetric.*

*Proof.* Fix  $i < j$  and elements  $x_k \in M$  for  $k \neq i, j$ . Define  $\lambda : M^2 \rightarrow N$  by

$$\lambda(x, y) = \varphi(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_{j-1}, y, x_{j+1}, \dots, x_n).$$

Since  $\varphi$  is multilinear and alternating,  $\lambda$  is bilinear and alternating. Hence,

$$0 = \lambda(x + y, x + y) = \lambda(x, x) + \lambda(x, y) + \lambda(y, x) + \lambda(y, y) = \lambda(x, y) + \lambda(y, x)$$

since  $\lambda$  is alternating (so  $\lambda(x, x) = 0$ ). Thus  $\lambda(x, y) = -\lambda(y, x)$ , so  $\lambda$  is skew-symmetric. Thus

$$\varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = -\varphi(x_1, \dots, x_n)$$

when  $\sigma$  is a transposition  $(ij)$ . Since any  $\sigma$  is a product of transpositions  $\sigma = \tau_1 \dots \tau_\ell$ , we have

$$\sigma\varphi = (\tau_1 \dots \tau_\ell)\varphi = (-1)^\ell \varphi = \varepsilon(\sigma)\varphi.$$

This gives that  $\varphi$  is skew-symmetric.  $\square$



**Lemma 19.3.** *Let  $\varphi : M^n \rightarrow N$  be multilinear. Then*

$$S(\varphi) = \sum_{\sigma \in S_n} \sigma\varphi \text{ is symmetric} \quad \text{and} \quad A(\varphi) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\sigma\varphi \text{ is alternating and skew-symmetric.}$$

*Proof.* Next class.

□