

## Contents

<b>1 Intro &amp; Rings .....</b>	<b>2</b>
1.1 Motivation .....	2
1.2 Review of ring theory .....	2
<b>2 Domains .....</b>	<b>4</b>
2.1 Irreducibles and primes .....	4
2.2 Ascending chains .....	5
2.3 Unique factorization domains .....	6
2.4 Principal ideal domains .....	8
2.5 Polynomials .....	10
<b>3 Field Extensions .....</b>	<b>13</b>
3.1 Basics .....	13
3.2 Simple extensions .....	14
3.3 Finite extensions and the algebraic closure .....	15
<b>4 Splitting Fields .....</b>	<b>17</b>
4.1 Existence .....	17
4.2 Uniqueness .....	18
<b>5 More Field Theory .....</b>	<b>20</b>
5.1 Prime fields .....	20
5.2 Formal derivatives and repeated roots .....	20
5.3 Finite fields .....	22
<b>6 Solvable and Automorphism Groups .....</b>	<b>25</b>
6.1 Solvable groups .....	25
6.2 Automorphism groups .....	27
6.3 Automorphism groups of splitting fields .....	28
<b>7 Separable and Normal Extensions .....</b>	<b>30</b>
7.1 Separable extensions .....	30
7.2 Normal extensions .....	31
<b>8 Galois Correspondence .....</b>	<b>34</b>
8.1 Galois extensions .....	34
8.2 The fundamental theorem .....	36
<b>Appendix A: Solutions to Exercises .....</b>	<b>41</b>

# 1 Intro & Rings

## 1.1 Motivation

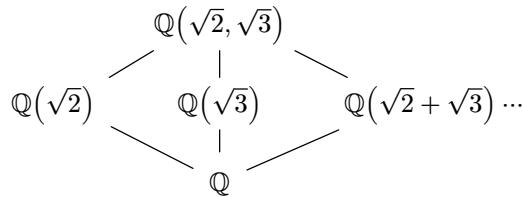
**Definition** (Radical): An expression involving only  $+, -, *, /, \sqrt[n]{\cdot}$ .

After a linear transformation, all cubics can be reduced to  $x^3 + px = q$ , and there is a formula for solutions to the above. Quartics can also be reduced to a cubic and solved.

The quintic was attempted by Euler, Bezout, Lagrange, etc without success. In 1799, Ruffini gave a 516-page proof on the insolubility of the quintic that was almost right. In 1824, Abel filled in the gap in Ruffini's proof.

The main steps of Galois theory are to:

1. Link a root  $\alpha$  of a quintic to  $\mathbb{Q}(\alpha)$ , the smallest field containing  $\alpha$ . It has more structure to be played with. Currently, our knowledge of  $\mathbb{Q}(\alpha)$  is lacking. For instance, we don't know how many intermediate fields there are between  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  and  $\mathbb{Q}$ .



We can list infinitely many of these intermediate fields, but how many are actually distinct?

2. To ameliorate the situation, we link the field  $\mathbb{Q}(\alpha)$  to a group. Precisely, we associate the field extension  $\mathbb{Q}(\alpha)/\mathbb{Q}$  to the group

$$\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\varphi : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\alpha) : \varphi|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}\}$$

i.e. the set of automorphisms that fix the smaller field. It can be shown that if  $\alpha$  is “good” then  $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$  is finite. Moreover, there is a bijection between the intermediate fields of  $\mathbb{Q}(\alpha)/\mathbb{Q}$  and the subgroups of  $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ . Galois theory is the interplay between fields and groups.

## 1.2 Review of ring theory

Rings in this course are by and large commutative and unital.

**Definition** (Integral Domain, Field): A ring  $R$  where for all  $a, b \in R$  m  $ab = 0 \implies a = 0$  or  $b = 0$  is an **integral domain**. A **field** is a ring  $R$  such that  $R^* = R \setminus \{0\}$ .

**Proposition 1.1** (Subrings of fields): Every subring of a field  $F$ , including  $F$  itself, is an integral domain.

**Definition** (Ideal): A subset  $I$  of a commutative ring such that  $0 \in I$ , and for  $a, b \in I$  and any  $r \in R$ ,  $a - b \in I$  and  $ra \in I$ .

*Remark:* If  $1 \in I$  is an ideal, then  $I = R$ , since any  $r \in R$  satisfies  $r1 = r \in I$ , so  $R \subseteq I$ .

The only ideals of a field  $F$  are  $\{0\}$  and  $F$ , since if  $a \in I$  with  $a \neq 0$ , then  $aa^{-1} = 1 \in I$ , so  $I = F$ .

Recall that using the division algorithm in  $\mathbb{Z}$ , we can prove all ideals of  $\mathbb{Z}$  are principal ideals.

*Remark:* The smallest field containing  $\mathbb{Z}$  is  $\mathbb{Q}$ .

**Definition** ( $F[x]$ ): Define  $F[x] = \{a_0 + \dots + a_m x^m : a_i \in F\}$ .

- If  $a_m = 1$ , we say  $f$  is **monic**.
- If  $a_m \neq 0$ , the **degree** of  $f$  is  $\deg(f) = m$ . By convention,  $\deg(0) = -\infty$ .

- For  $f, g \in F[x]$ ,  $\deg(fg) = \deg(f) + \deg(g)$ .

Notes about  $F[x]$ :

- $F[x]$  is an integral domain.
- The units of  $F[x]$  are  $F^* = F \setminus \{0\}$ , i.e. the unital constant polynomials.
- The division algorithm works. For  $f, g$  with  $f \neq 0$ , we can write  $g(x) = q(x)f(x) + r(x)$  with  $\deg(r) < \deg(f)$  (here the  $-\infty$  convention is handy).
- Using the DA, we can prove all ideals of  $F[x]$  are principal. Moreover, if we impose that generators  $f(x)$  are monic, then generators are unique.

*Remark:* The smallest field containing  $F[x]$  is the set of rational functions

$$F(x) := \left\{ \frac{f(x)}{g(x)} : f, g \in F[x] \text{ and } g \neq 0 \right\}$$

Recall when  $I$  is an ideal of  $R$ , that the additive quotient group  $R/I$  is a ring with multiplication  $(r+I)(s+I) = rs+I$ , and the unit of  $R/I$  is  $1+I$ .

**Theorem 1.2** (First Isomorphism Theorem): Let  $\varphi : R \rightarrow S$  be a ring homomorphism. Then  $\text{Ker}(\varphi)$  is an ideal of  $R$  and  $R/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$ .

*Example:* Let  $F$  be a field,  $S$  a ring, and  $\varphi : F \rightarrow S$  be a ring homomorphism. Then either  $\varphi$  is injective or the zero map, since  $\text{Ker}(\varphi)$  is an ideal of  $F$ , hence either  $\{0\}$  or  $F$ .

**Definition** (Prime, maximal): Let  $R$  be a commutative ring. An ideal  $P \neq R$  is a **prime** ideal if whenever  $rs \in P$ , then  $r \in P$  or  $s \in P$ .

An ideal  $M \neq R$  of  $R$  is **maximal** if whenever  $A$  is an ideal such that  $M \subseteq A \subseteq R$ , then  $A = M$  or  $A = R$ .

**Theorem 1.3:** Let  $I \neq R$  be an ideal of a commutative ring  $R$ . Then

- (1)  $I$  is maximal iff  $R/I$  is a field.
- (2)  $I$  is prime iff  $R/I$  is an integral domain.

*Proof:*

- (1) Suppose  $I$  is maximal. Note  $I \neq R \iff R/I$  is a commutative ring with 1. We show the non-zero elements in  $R/I$  have inverses. Let  $a \in R$  with  $a \notin I$ , so  $a+I \neq 0+I$ . Since  $a \notin I$ , we have  $I \subsetneq \langle a \rangle + I = \langle I \cup \{a\} \rangle = R$  by maximality, so  $\langle a \rangle + I$  contains 1. Notice

$$\langle a \rangle + I = \{ar + m : m \in I, r \in R\}$$

so say  $1 = ar + m$  where  $r \in R, m \in I$ . Then we have our inverse:

$$(a+I)(r+I) = ar + I = (ar + m) + I = 1 + I$$

Conversely if  $R/I$  is a field, since  $1+I \neq 0+I$  we have  $1 \notin I$  so  $I \neq R$ . Let  $A$  be an ideal with  $I \subseteq A \subseteq R$  and suppose  $A \neq I$ . Choose  $a \in A - I$  so  $a+I \neq 0+I$ . Then since  $R/I$  is a field,  $a+I$  has an inverse, say  $b+I$ . Then  $(a+I)(b+I) = ab+I = 1+I$ . Then  $1-ab \in I \subseteq A$ . Since  $a \in A$  we have  $ab \in A$ , so  $1 \in A \implies A = R$ . Thus  $I$  is maximal.

- (2) Since  $I \neq R$ ,  $R/I$  is a commutative ring with 1. For  $a, b \in R$ ,

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

and  $a+P = 0+P \iff a \in P$ . So  $(a+P)(b+P) = 0+P \iff ab \in P$ . The result is immediate.  $\square$

**Corollary 1.4:** Every maximal ideal is prime.

## 2 Domains

### 2.1 Irreducibles and primes

**Definition (Divides):** Let  $R$  be an integral domain and  $a, b \in R$ . We say  $a$  divides  $b$ , denoted  $a | b$ , if  $ca = b$  for some  $c \in R$ .

Notice in  $\mathbb{Z}$  that if  $n | m$  and  $m | n$ , then  $n = \pm m$  so  $\langle n \rangle = \langle m \rangle$ .

**Proposition 2.1** (Divisibility characterization): Let  $R$  be an integral domain. For  $a, b \in R$ , TFAE:

- (1)  $a | b$  and  $b | a$
- (2)  $a = ub$  for some unit  $u \in R$
- (3)  $\langle a \rangle = \langle b \rangle$

*Proof:*

(1  $\implies$  2) Suppose there are  $u, v \in R$  so  $b = ua$  and  $a = vb$ . If  $a = 0$ , then  $b = 0$  so  $a = 1b$ . Otherwise,

$$a = vb = v(ua) = (vu)a \implies a(1 - vu) = 0.$$

Since  $R$  is an integral domain and  $a \neq 0$ ,  $1 - vu = 0 \iff vu = 1$ . Thus  $v$  is a unit.

(2  $\implies$  3) Say  $a = ub$ . Then  $a \in \langle b \rangle$ , so  $\langle a \rangle \subseteq \langle b \rangle$ . Since  $u$  is a unit and  $b = u^{-1}a$ ,  $\langle b \rangle \subseteq \langle a \rangle$ .

(3  $\implies$  1) If  $\langle a \rangle = \langle b \rangle$ , then  $a \in \langle a \rangle = \langle b \rangle$ , so  $a = tb$  for some  $t \in R$ , giving  $b | a$ . Similarly,  $a | b$ .  $\square$

**Definition (Associated):** Let  $R$  be an integral domain. For  $a, b \in R$ , we say  $a$  is associated to  $b$ , denoted  $a \sim b$ , if  $a | b$  and  $b | a$ .

Often this is most useful with  $a = ub$  for a unit  $u$ . From the previous proposition, we can show  $\sim$  is an equivalence relation on  $R$ .

- $a = 1a \implies a \sim a$
- $a \sim b \implies a = ub \implies b = u^{-1}a \implies b \sim a$
- $a \sim b$  and  $b \sim c$  gives  $a = ub$  and  $b = vc$  so  $a = uvc$  where  $uv$  is a unit with inverse  $v^{-1}u^{-1}$ , so  $a \sim c$ .

*Exercise 2.1:* Show that for  $a, b \in R$  where  $R$  is an integral domain,

- (a) if  $a \sim a'$  and  $b \sim b'$  then  $ab \sim a'b'$ .
- (b) if  $a \sim a'$  and  $b \sim b'$  then  $a | b \iff a' | b'$ .

*Example:* Let  $R = \mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} : m, n \in \mathbb{Z}\}$ . This is an integral domain, where  $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$ , so  $2 + \sqrt{3}$  is a unit in  $R$ . Since  $3 + 2\sqrt{3} = (2 + \sqrt{3})\sqrt{3}$ , we have  $3 + 2\sqrt{3} \sim \sqrt{3}$ .

**Definition (Irreducible):** Let  $R$  be an integral domain. We say  $p \in R$  is **irreducible** if  $p \neq 0$  and for all  $b, c \in R$ , if  $p = bc$  then one of  $b, c$  is a unit.

*Example:* Let  $R := \mathbb{Z}[\sqrt{-5}]$  and  $p := 1 + \sqrt{-5}$ . We claim  $p$  is irreducible. Suppose it is reducible, so  $p = ab$  where  $a, b$  are not units.

**Definition (Norm in  $\mathbb{Z}[\sqrt{d}]$ ):** Let  $R$  be the ring  $\mathbb{Z}[\sqrt{d}]$  where  $1 \neq d \in \mathbb{Z}$  is squarefree and non-zero. Define  $N : R \rightarrow \mathbb{Z}$  by

$$N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

*Exercise 2.2:* Prove that  $N(xy) = N(x)N(y)$  for all  $x, y \in R$ .

Now  $N(p) = 6 = N(a)N(b)$  but  $N(a), N(b) \neq 1$  as  $N(x) = 1$  iff  $x$  is a unit. Therefore  $N(a), N(b) \in \{2, 3\}$ . Say  $a = u + v\sqrt{-5}$  so  $N(a) = u^2 + 5v^2$ . Then we see  $N(a) = u^2 \pmod{5}$ , but the possible values of  $u^2$  are

0, 1, 4 since  $u \in \{0, \pm 1, \pm 2\} \mapsto \{0, 1, 4\}$  mod 5. Therefore  $N(a)$  cannot be 2 or 3, a contradiction, so  $p$  is irreducible.

**Proposition 2.2** (Characterizations of irreducibility): Let  $R$  be an integral domain and  $p \in R, p \neq 0$  with  $p$  not a unit. TFAE:

- (1)  $p$  is irreducible.
- (2) if  $d | p$ , then  $d \sim 1$  or  $d \sim p$ .
- (3) if  $p \sim ab$ , then  $p \sim a$  or  $p \sim b$ .
- (4) If  $p = ab$ , then  $p \sim a$  or  $p \sim b$ .

*Proof:*

- (1  $\implies$  2) Suppose  $p = ad$  so one of  $a, d$  is a unit. If  $a$  is a unit then  $p \sim d$ . If  $d$  is a unit,  $d \sim 1$ .
- (2  $\implies$  3) Suppose  $p \sim ab$ , then  $b | p$ . Then  $b \sim 1$  or  $b \sim p$ . If the latter, we're done, if  $b \sim 1$ , then  $a \sim p$ .
- (3  $\implies$  4) Suppose  $p = ab$ , then  $p = 1ab \sim ab$  and by assumption  $p \sim a$  or  $p \sim b$ .
- (4  $\implies$  1) Say  $p = ab$ . If  $p \sim a$  then  $a = up$  for a unit  $u$ . Since  $R$  is commutative,  $p = ab = upb = pub$  so  $1 = ub$  since  $R$  is an integral domain. Thus  $b$  is a unit. Similarly,  $p \sim b \implies a$  is a unit.  $\square$

**Definition** (Prime): Let  $R$  be an integral domain and  $p \in R$ . We say  $p$  is **prime** if  $p \neq 0$  is not a unit, and if  $p | ab \in R$  then  $p | a$  or  $p | b$ .

*Remark:* If  $p \sim q$ , then  $p$  is prime iff  $q$  is prime. Indeed, say  $p$  is prime and suppose  $q | ab \in R$ . Then  $dq = ab$  for some  $d \in R$ . Say  $p = uq$  for a unit  $u \in R$ , so  $ab = du^{-1}p$  so  $p | ab$ , so  $p | a$  or  $p | b$ . If  $p | a$  then  $cp = a = cuq$  so  $q | a$ . Similarly  $p | b \implies q | b$ . The converse is identical.

By induction we can also show if  $p$  is prime and  $p | a_1 \cdots a_n$  then  $p | a_i$  for some  $i$ .

**Proposition 2.3** (Primes are irreducible): Let  $R$  be an integral domain,  $p \in R$ . If  $p$  is prime, then  $p$  is irreducible.

*Proof:* Say  $p = ab \in R$ , and wlog  $p | a$ . Write  $a = dp, d \in R$ , so by commutativity  $p = dpb = pdb$  so as  $p \neq 0$ , we have  $db = 1$ . Thus  $b$  is a unit, so  $p$  is irreducible.  $\square$

*Example:* The converse is false. Consider  $R = \mathbb{Z}[\sqrt{-5}]$ , where we know  $p = 1 + \sqrt{-5}$  is irreducible. Note

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

so  $p | 2 \cdot 3$  but neither of 2 or 3. Indeed, if  $p | 2$  then  $qp = 2$  for some  $q$ , then  $N(2) = N(q)N(p) \iff 4 = N(q)6$  but there are no integer solutions to this. The same argument works for 3.

*Exercise 2.3:* Construct a ring  $R$  and an element in  $R$  that is irreducible but not prime, different to the above example. ►

Recall that for a prime  $p \in \mathbb{Z}$ ,  $\pm 1 \cdot \pm p$  are the only factorizations of  $p$ , so  $p$  is irreducible. Also, we can prove Euclid's lemma, showing  $p$  is prime. The same things hold for  $F[x]$  when  $F$  is a field. We want to know the additional property of  $\mathbb{Z}$  or  $F[x]$  that gives us irreducible implying prime.

## 2.2 Ascending chains

**Definition** (ACCP): An integral domain  $R$  is said to satisfy the **ascending chain conditions on principal ideals** (ACCP) if for any chain

$$0 \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots$$

of principal ideals in  $R$ , there is  $n \in \mathbb{N}$  so

$$\langle a_n \rangle = \langle a_{n+1} \rangle = \dots$$

That is, the chain stabilizes eventually.

*Example:*  $\mathbb{Z}$  satisfies ACCP.

Given a chain, we see  $a_2 \mid a_1$  and  $a_3 \mid a_2$ , and so on. Thus taking absolute values gives

$$|a_1| \geq |a_2| \geq \dots$$

Since each  $|a_n| \geq 0 \in \mathbb{Z}$ , we get  $|a_n| = |a_{n+1}| = \dots$  for some  $n$ , so  $a_{n+1} = \pm a_i$  for all  $i \geq n$ . Thus the chain stabilizes, so  $\mathbb{Z}$  satisfies ACCP.

Notice this proof uses the well-ordering principle on  $\mathbb{N}$ , and so does the proof of unique factorization over  $\mathbb{Z}$  (MATH135).

**Theorem 2.4** (Product of irreducibles): Let  $R$  be an integral domain satisfying ACCP. If  $a \in R$  is not zero and not a unit, then  $a$  is a product of irreducibles.

*Proof:* Suppose bwoc  $a$  is not a product of irreducibles. Say  $a = x_1 a_1$  where wlog  $a_1$  is not a product of irreducibles, and  $a$  is not irreducible so  $a \not\sim x_1, a_1$ . Inductively, construct  $a_n = x_{n+1} a_{n+1}$  so  $a_n \not\sim a_{n+1}$  and  $a_{n+1}$  is not a product of irreducibles. Then

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \dots$$

which violates ACCP, where the ideal containments are proper since  $a_n \not\sim a_{n+1}$ .  $\diamond$

**Theorem 2.5** ( $R[x]$  ACCP): If  $R$  is an integral domain satisfying ACCP, so is  $R[x]$ .

*Proof:* Suppose bwoc there is a chain

$$\{0\} \subsetneq \langle f_1 \rangle \subseteq \langle f_2 \rangle \subseteq \dots \in R[x].$$

Since  $f_{i+1} \mid f_i$ , let  $a_i$  be the leading coefficient of each  $f_i$  to get  $a_{i+1} \mid a_i$  for all  $i$ . Thus

$$\{0\} \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots$$

Since  $R$  has ACCP, there is  $n \in N$  so  $\langle a_n \rangle = \langle a_{n+1} \rangle = \dots$ . For  $m \geq n$ , we have  $f_m = g f_{m+1}$  for some  $g(x) \in R[x]$ , say  $g$  has leading coefficient  $b$ . Then  $a_m = b a_{m+1}$ , so  $b$  must be a unit and  $\langle a_m \rangle = \langle a_{m+1} \rangle$ . Now, if  $g = b$  is a constant polynomial, then

$$\langle f_m \rangle = \langle f_{m+1} \rangle,$$

a contradiction, so  $\deg(g) \geq 1$ . Thus  $\deg(f_m) > \deg(f_{m+1})$  for all  $m \geq n$ , but this is also a contradiction as  $\deg(f_i) \geq 0$ .  $\diamond$

*Example:* Since  $\mathbb{Z}$  satisfies ACCP, so does  $\mathbb{Z}[x]$ .

*Example:* Consider  $R = \{n + xf : n \in \mathbb{Z}, f \in \mathbb{Q}[x]\}$ , i.e. the set of polynomials in  $\mathbb{Q}[x]$  with integer constant term.  $R$  is an integral domain, but consider

$$\langle x \rangle = \{x(n + xf)\}, \quad \left\langle \frac{1}{2}x \right\rangle = \left\{ \frac{1}{2}x(n + xf) \right\}$$

and so on. This gives

$$\langle x \rangle \subsetneq \left\langle \frac{1}{2}x \right\rangle \subsetneq \left\langle \frac{1}{2^2}x \right\rangle \subsetneq \dots$$

Thus  $R$  is an integral domain that does not satisfy ACCP.

## 2.3 Unique factorization domains

**Definition (UFD):** An integral domain  $R$  is called a UFD if it satisfies:

- If  $a \neq 0 \in R$  is not a unit, then  $a$  is a product of irreducibles
- If  $p_1 p_2 \dots p_n \sim q_1 q_2 \dots q_s$  where  $p_i, q_j$  are irreducible, then  $r = s$  and after possible relabelling,  $p_i \sim q_i$  for all  $i = 1, \dots, r$ .

*Example:*  $\mathbb{Z}$  and  $F[x]$  are UFDs, and a field  $F$  is also a UFD.

**Proposition 2.6** (Irreducible implies prime): Let  $R$  be a UFD and  $p \in R$ . If  $p$  is irreducible, then  $p$  is prime.

*Proof:* Let  $p \in R$  be irreducible. If  $p \mid ab \in R$ , write  $ab = pd$  for  $d \in R$ . Since  $R$  is a UFD, we can factor  $a, b, d$  into irreducible elements:

$$\begin{aligned} a &= q_1 \dots q_k \\ b &= s_1 \dots s_\ell \\ d &= r_1 \dots r_m. \end{aligned}$$

We allow  $k, \ell, m$  to be 0 in case  $a, b, d$  are units. Now since  $pd = ab$ ,

$$pr_1 \dots r_m = q_1 \dots q_k s_1 \dots s_\ell.$$

Since  $p$  is irreducible and  $R$  is a UFD,  $m + 1 = k + \ell$  and  $p \sim q_i$  or  $p \sim s_j$  for some  $i$  or  $j$ . Thus  $p \mid a$  or  $p \mid b$ .  $\square$

*Example:*  $\mathbb{Z}$  is a UFD, where we know a prime satisfies Euclid's lemma. A similar statement holds for  $F[x]$ .

*Example:* Consider  $R = \mathbb{Z}[\sqrt{-5}]$  and  $p = 1 + \sqrt{-5}$ . We have seen that  $p$  is irreducible but not prime, so  $R$  is not a UFD. Claim:  $R$  satisfies ACCP. Say

$$\{0\} \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$$

Then  $a_{i+1} \mid a_i$  for all  $i$ , and as the norm is non-negative, and multiplicative,

$$N(a_{i+1}) \leq N(a_i).$$

Therefore,

$$N(a_1) \geq N(a_2) \geq \dots,$$

but each  $N(a_n) \geq 0$ , so we must have  $N(a_n) = N(a_{n+1}) = \dots$  for some  $n \in \mathbb{N}$ .

The takeaway here is UFD implies ACCP, but ACCP does not imply UFD. We would like to know exactly how much stronger a UFD is than an integral domain with ACCP.

**Definition (GCD):** Let  $R$  be an integral domain and  $a, b \in R$ . We say  $d \in R$  is a **greatest common divisor** of  $a$  and  $b$ , denoted  $\gcd(a, b)$  if:

- $d \mid a, b$ .
- If  $e \in R$  with  $e \mid a, b$  then  $e \mid d$ .

*Remark:* One can show if  $R$  is a UFD and  $a, b$  are non-zero and  $p_1, \dots, p_k$  are non-associated primes dividing  $a, b$ , say

$$\begin{aligned} a &\sim p_1^{\alpha_1} \dots p_k^{\alpha_k} \\ b &\sim p_1^{\beta_1} \dots p_k^{\beta_k} \end{aligned}$$

Then  $\gcd(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \dots p_k^{\min\{\alpha_k, \beta_k\}}$ .

Furthermore, if  $R$  is a UFD and  $d, a_1, \dots, a_m \in R$ , we have

$$\gcd(da_1, \dots, da_m) = d \gcd(a_1, \dots, a_m).$$

**Exercise 2.4:** Prove the above remark. ▶

**Theorem 2.7** (UFD characterization): Let  $R$  be an integral domain. TFAE:

- (1)  $R$  is a UFD
- (2)  $R$  satisfies ACCP and  $\gcd(a, b)$  exists for all  $a, b \neq 0 \in R$
- (3)  $R$  satisfies ACCP and every irreducible element is prime.

*Proof:*

(1  $\implies$  2) By the previous remark,  $\gcd(a, b)$  exists for all  $a, b \neq 0$ . Also, suppose

$$\{0\} \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$$

Since  $\langle a_1 \rangle \neq \{0\}$  and  $a_1$  is not a unit, we can write  $a \sim p_1^{k_1} \cdots p_r^{k_r}$  where  $p_i$  are non-associated primes and  $k_i \in \mathbb{N}$ . Since  $a_i \mid a_1$  for all  $i$  we have

$$a_i \sim p_1^{d_{i,1}} \cdots p_r^{d_{i,r}}$$

for  $0 \leq d_{i,j} \leq k_j$  ( $1 \leq j \leq r$ ). Thus there are only finitely many non-associated choices for  $a_i$ , and so there exist  $m \neq n$  with  $a_m \sim a_n \implies \langle a_m \rangle = \langle a_n \rangle$ , a contradiction. Hence  $R$  satisfies ACCP.

- (2  $\implies$  3) Let  $r$  be irreducible and suppose  $p \mid ab \in R$ . Then let  $d = \gcd(a, p)$ . Since  $d \mid p$  which is irreducible,  $d \sim 1$  or  $d \sim p$ . If  $d \sim p$  then  $d \mid a \implies p \mid a$ . Otherwise,  $d \sim 1$  so  $1 \sim \gcd(a, p) \implies b \sim \gcd(ab, pb)$ , where  $p \mid ab$  and  $p \mid pb$ , so  $p \mid b$ .
- (3  $\implies$  1)  $R$  satisfies ACCP, so for  $a \neq 0 \in R$  not a unit,  $a$  is a product of irreducibles, so it suffices to prove such factorizations are unique. Suppose we have

$$p_1 \cdots p_r \sim q_1 \cdots q_s$$

where each  $p_i, q_j$  is irreducible. Since  $p_1$  is prime by assumption, we have  $p_1 \mid q_j$  for some  $j$ , say wlog  $p_1 \mid q_1$ . Thus  $p_1 \sim q_1$ . Since  $p_1 \sim q_1$  we can divide out and repeat inductively to get  $p_1 \cdots p_r \sim q_1 \cdots q_s$  has  $r = s$  and  $p_i \sim q_i$  ( $1 \leq i \leq r$ ). Thus the factorization is unique.  $\square$

## 2.4 Principal ideal domains

**Definition (PID):** An integral domain  $R$  is a **principal ideal domain** (PID) if every ideal in  $R$  is principal (singly-generated).

*Example:*  $\mathbb{Z}$  and  $F[x]$  are PIDs, as are fields. Note that although all ideals in  $\mathbb{Z}_n$  are principal,  $\mathbb{Z}_n$  is not an integral domain, so is not a PID.

**Proposition 2.8:** Let  $R$  be a PID and  $a_1, \dots, a_n \neq 0$ . Then  $d \sim \gcd(a_1, \dots, a_n)$  exists, and there exist  $r_1, \dots, r_n \in R$  so that

$$\gcd(a_1, \dots, a_n) \sim r_1 a_1 + \dots + r_n a_n.$$

*Proof:* Let  $A = \langle a_1, \dots, a_n \rangle = \{r_1 a_1 + \dots + r_n a_n : r_i \in R\}$  so  $A$  is an ideal, hence principal i.e. there is  $d \in R$  so  $A = \langle d \rangle$ . In particular,

$$d = r_1 a_1 + \dots + r_n a_n$$

for some  $r_i \in R$  as  $d \in A$ . We claim  $d \sim \gcd(a_1, \dots, a_n)$ . For each  $i \in [n]$ ,  $a_i \in \langle d \rangle$  so  $a_i = qd$  for some  $q$ , hence  $d \mid a_i$ . Also, if  $r \mid a_i$  for all  $i$ , then  $r \mid (r_1 a_1 + \dots + r_n a_n) \iff r \mid d$ , so  $d \sim \gcd(a_1, \dots, a_n) \sim r_1 a_1 + \dots + r_n a_n$  by definition.  $\square$

**Theorem 2.9** (PIDs are UFDs): Every PID is a UFD.

*Proof:* If  $R$  is a PID, by [Theorem 2.7](#) and [Proposition 2.8](#) it suffices to show  $R$  satisfies ACCP. Suppose

$$\{0\} \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots$$

Let  $A = \bigcup_{i \in \mathbb{N}} \langle a_i \rangle$ , which is an ideal, so  $\langle a \rangle = A$  for some  $a \in R$ . Then as  $a \in A$ , there is  $n \in \mathbb{N}$  so  $a \in \langle a_n \rangle$ . Thus  $a \in \langle a_m \rangle$  for all  $m \geq n$ , so  $\langle a \rangle \subseteq \langle a_m \rangle \subseteq \langle a \rangle \implies \langle a \rangle = \langle a_m \rangle$ , so the chain stabilizes. Thus  $R$  satisfies ACCP, so is a UFD.  $\diamond$

*Example:* We claim  $\mathbb{Z}[x]$  is not a PID. Consider

$$A := \{2n + xf(x) : n \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$$

i.e. those polynomials with even constant term. Suppose  $A = \langle g(x) \rangle$  for some  $g(x) \in \mathbb{Z}[x]$ . Since  $2 \in A$ ,  $g(x) \mid 2$ , so  $g(x) \sim 1$  or  $g(x) \sim 2$ . In the former case,  $1 \in A \implies A = \mathbb{Z}[x]$  is a contradiction, and in the latter case,  $A = \{2f(x) : f(x) \in \mathbb{Z}[x]\}$  which is also a contradiction, since e.g.  $x \in A$ . Therefore there exist ideals that are not principal.

**Theorem 2.10:** Let  $R$  be a PID. If  $0 \neq p \in R$  is not a unit, TFAE:

- (1)  $p$  is prime
- (2)  $R/\langle p \rangle$  is a field (iff  $\langle p \rangle$  is a maximal ideal)
- (3)  $R/\langle p \rangle$  is an integral domain (iff  $\langle p \rangle$  is a prime ideal)

*Proof:*

(1  $\implies$  2) Let  $p$  be prime and let  $0 + \langle p \rangle \neq a + \langle p \rangle \in R/\langle p \rangle$  for some  $a \in R$  such that  $p \nmid a$ . We wish to show  $(a + \langle p \rangle)^{-1}$  exists. Consider the ideal

$$A = \langle a, p \rangle = \{ra + sp : r, s \in R\}.$$

Since  $R$  is a PID,  $A = \langle d \rangle$  for some  $d \in R$ . Since  $p \in A$  we have  $d \mid p$ , but as  $p$  is prime hence irreducible,  $d \sim 1$  or  $d \sim p$ . Notice if  $d \sim p$  then  $\langle p \rangle = \langle d \rangle = A$  where  $a \in A$ , so then  $p \mid a$ , a contradiction.

Thus we have  $d \sim 1$ , so  $A = \langle d \rangle = \langle 1 \rangle = R$ . Hence  $1 = ba + cp$  for some  $b, c \in R$ , giving

$$\begin{aligned} (a + \langle p \rangle)(b + \langle p \rangle) &= ab + \langle p \rangle \\ &= (1 - cp) + \langle p \rangle \\ &= 1 + \langle p \rangle. \end{aligned}$$

Therefore  $(a + \langle p \rangle)^{-1}$  exists, so  $R/\langle p \rangle$  is a field.

(2  $\implies$  3) Every field is an integral domain.

(3  $\implies$  1) Suppose  $p \mid ab \in R$ . Then

$$(a + \langle p \rangle)(b + \langle p \rangle) = ab + \langle p \rangle = 0 + \langle p \rangle$$

because  $p \mid ab \implies ab \in \langle p \rangle$ . Since  $R/\langle p \rangle$  is an integral domain, one of  $a + \langle p \rangle, b + \langle p \rangle$  is  $0 + \langle p \rangle$ , so one of  $a, b \in \langle p \rangle$  i.e.  $p \mid a$  or  $p \mid b$ , so  $p$  is prime.  $\diamond$

*Remark:* The proofs for (2  $\implies$  3) and (3  $\implies$  1) work for integral domains, only (1  $\implies$  2) leverages that  $R$  is a PID.

**Note:** We have the following relations between algebraic structures:

$$\text{Field} \subsetneq \text{PID} \subseteq \text{UFD} \subsetneq \text{ACCP} \subsetneq \text{ID} \subsetneq \text{Comm Ring} \subseteq \text{Ring}$$

$$\mathbb{Q} \quad \mathbb{Z} \quad \mathbb{Z}[x] \quad \mathbb{Z}[\sqrt{-5}] \quad A \quad \mathbb{Z}_n \quad M_n(\mathbb{R}).$$

where  $A = \{n + xf : n \in \mathbb{Z}, f \in \mathbb{Q}[x]\}$ .

We don't yet know if the  $\text{PID} \subseteq \text{UFD}$  containment is proper, but we will show  $\mathbb{Z}[x]$  is a UFD eventually.

*Remark:* [Theorem 2.10](#) fails for UFDs. Consider  $\langle x \rangle \in \mathbb{Z}[x]$ , then  $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$  which is an integral domain but not a field, i.e.  $\langle x \rangle$  is a prime ideal but not a maximal ideal.

In a PID, non-zero proper ideals are prime iff they are maximal. In general, only maximal implies prime.

In a UFD, non-zero non-units are prime iff they are irreducible. In general, only prime implies irreducible.

## 2.5 Polynomials

Consider  $2x + 4$ , which is irreducible in  $\mathbb{Q}[x]$ , but factors as  $2(x + 4)$  in  $\mathbb{Z}[x]$  where 2 is not a unit, so it is reducible in  $\mathbb{Z}[x]$ . This motivates the following definition:

**Definition** (Content, primitive): If  $R$  is a UFD and  $0 \neq f(x) \in R[x]$ , a greatest common divisor of all coefficients of  $f$  is called a **content** of  $f$ , denoted  $c(f)$ . If  $c(f) \sim 1$ , we say  $f$  is a **primitive** polynomial.

*Example:* In  $\mathbb{Z}[x]$ ,  $c(6 + 10x^2 + 15x^3) \sim \gcd(6, 10, 15) \sim 1$  so this is primitive. However,  $c(6 + 9x^2 + 15x^3) \sim \gcd(6, 9, 15) \sim 3$ , so this is not primitive.

**Lemma 2.11:** Let  $R$  be a UFD and  $0 \neq f(x) \in R[x]$ .

- $f(x)$  can be written as  $f(x) = c(f)f_1(x)$  for some primitive  $f_1(x) \in R[x]$
- if  $0 \neq b \in R$ , then  $c(bf) \sim bc(f)$ .

*Proof:* Let  $f(x) = a_m x^m + \dots + a_0$ . Let  $c(f) \sim \gcd(a_m, \dots, a_0)$  and write  $a_i = c(f)b_i$  for all  $i$ , so

$$f(x) = c(f)f_1(x), \text{ where } f_1(x) = b_m x^m + \dots + b_0.$$

We show  $f_1$  is primitive. Indeed,

$$c(f) \sim \gcd(a_m, \dots, a_0) \sim \gcd(c(f)b_m, \dots, c(f)b_0) \sim c(f) \gcd(b_m, \dots, b_0).$$

Hence  $1 \sim \gcd(b_m, \dots, b_0) \iff c(f_1) \sim 1$ , so  $f_1$  is primitive. Furthermore, the coefficients of  $bf$  for  $b \neq 0$  are  $ba_m, \dots, ba_0$ , so

$$c(bf) \sim \gcd(ba_m, \dots, ba_0) \sim b \gcd(a_m, \dots, a_0) \sim bc(f).$$

Thus  $c(bf) \sim bc(f)$ . ◇

**Lemma 2.12:** Let  $R$  be a UFD and  $\ell(x) \in R[x]$  be irreducible with  $\deg(\ell) \geq 1$ . Then  $c(\ell) \sim 1$ .

*Proof:* Write  $\ell(x) = c(\ell)\ell_1(x)$  with  $\ell_1$  primitive and  $\deg(\ell_1) = \deg(\ell) = 1$ . Since  $\ell$  is irreducible one of  $c(\ell), \ell_1$  must be a unit but clearly  $\ell_1$  cannot be, so  $c(\ell) \sim 1$ . ◇

**Theorem 2.13** (Gauss' Lemma): Let  $R$  be a UFD. If  $f, g \neq 0 \in R[x]$  then  $c(fg) \sim c(f)c(g)$ . In particular, the product of primitive polynomials is again primitive.

*Proof:* Let  $f = c(f)f_1$  and  $g = c(g)g_1$  with  $f_1, g_1$  primitive. Then

$$c(fg) \sim c(c(f)f_1c(g)g_1) \sim c(f)c(g)c(f_1g_1).$$

It suffices then to prove a product of primitives is primitive. Suppose bwoc  $f, g$  are primitive but  $fg$  is not. Write

$$\begin{aligned} f(x) &= a_0 + \dots + a_m x^m \\ g(x) &= b_0 + \dots + b_n x^n. \end{aligned}$$

Since  $R$  is a UFD, there is a prime  $p$  dividing each coefficient of  $fg$ . Since  $f, g$  are primitive, there is some  $k, s$  so  $p \nmid a_k, b_s$ . Let  $k$  and  $s$  be the minimum such values. Then

- $p \nmid a_k$  but  $p \mid a_i$  for  $i = 0, \dots, k - 1$
- $p \nmid b_s$  but  $p \mid b_j$  for  $j = 0, \dots, s - 1$

Now the coefficient  $c_{k+s}$  of  $x^{k+s}$  in  $fg$  is

$$\begin{aligned} c_{k+s} &= \sum_{i+j=k+s} a_i b_j \\ &= a_0 b_{k+s} + \dots + a_{k-1} b_{s+1} + a_k b_s + a_{k+1} b_{s-1} + \dots + a_{k+s} b_0. \end{aligned}$$

Now  $p$  divides every term on the left of  $a_k b_s$  and every term on the right of it. However, it does not divide  $a_k b_s$ , hence cannot divide the sum, i.e.  $p \nmid c_{k+s}$ , a contradiction. Thus  $fg$  is primitive.  $\square$

**Theorem 2.14:** Let  $R$  be a UFD whose field of fractions  $F$  is

$$F = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}.$$

Regard  $R$  as a subring of  $F$ . If  $\ell(x) \in R[x]$  is irreducible in  $R[x]$ , then  $\ell(x)$  is irreducible in  $F[x]$ .

*Proof:* Let  $\ell(x) \in R[x]$  be irreducible. Suppose  $\ell(x) = g(x)h(x) \in F[x]$ . If  $a, b$  are the products of the denominators of the coefficients of  $g(x)$  and  $h(x)$ , then  $g_1(x) = ag(x) \in R[x]$  and  $h_1(x) = bh(x) \in R[x]$ . Notice that  $ab\ell(x) = g_1(x)h_1(x)$  is a factorization in  $R[x]$ . Since  $\ell(x)$  is irreducible,  $c(\ell) \sim 1$ . Also, by Gauss' lemma, we have

$$ab \sim abc(\ell) \sim c(ab\ell) \sim c(g_1 h_1) \sim c(g_1)c(h_1). \quad (\star)$$

Now, write  $g_1(x) = c(g_1)g_2(x)$  and  $h_1(x) = c(h_1)h_2(x)$  where  $g_2(x), h_2(x)$  are primitive in  $R[x]$ . Then

$$ab\ell(x) = g_1(x)h_1(x) = c(g_1)c(h_1)g_2(x)h_2(x).$$

By  $(\star)$  we have  $\ell(x) \sim g_2(x)h_2(x)$  in  $R[x]$ . Since  $\ell(x)$  is irreducible, it follows that  $h_2(x) \sim 1$  or  $g_2(x) \sim 1$ .

If  $g_2(x) \sim 1$ , then  $ag(x) = g_1(x) = c(g_1)g_2(x)$ . Thus  $g(x) = a^{-1}c(g_1)g_2(x)$  with  $g_2(x) \sim 1$  is a unit in  $F[x]$ . Similarly if  $h_2(x) \sim 1$ , we can show  $h(x)$  is a unit in  $F[x]$ . Thus  $\ell(x) = g(x)h(x)$  in  $F[x]$  implies that either  $g(x)$  or  $h(x)$  is a unit in  $F[x]$ , so  $\ell(x)$  is irreducible in  $F[x]$ .  $\square$

Recall the converse is false:  $2x + 4$  is irreducible in  $\mathbb{Q}[x]$  but reducible in  $\mathbb{Z}[x]$ . What's notable about this example is the content of  $2x + 4$  is not a unit. One might wonder if this is the only such restriction preventing an iff statement. Indeed it is.

**Proposition 2.15:** Let  $F$  be a UFD whose field of fractions is  $F$ . Let  $f(x) \in R[x]$  with  $\deg(f) \geq 1$ . TFAE:

- (1)  $f(x)$  is irreducible in  $R[x]$ .
- (2)  $f(x)$  is primitive and irreducible in  $F[x]$ .

*Proof:*

(1  $\implies$  2) Follows from [Lemma 2.12](#) and [Theorem 2.14](#).

(2  $\implies$  1) Suppose  $f(x)$  is primitive and irreducible in  $F[x]$  but reducible in  $R[x]$ . Then a nontrivial factorization of  $f(x)$  in  $R[x]$  must be of the form  $f(x) = dg(x)$  with  $d \in R$  and  $d \not\sim 1$  (if both factors have degree  $\geq 1$ , then it would be a nontrivial factorization in  $F[x]$ ). Since  $d \mid f(x)$ ,  $d \not\sim 1$  divides each coefficient of  $f(x)$ , contradicting the fact that  $f(x)$  is primitive. Thus  $f(x)$  is irreducible in  $R[x]$ .  $\square$

Notice that primitive guarantees irreducibility in  $R[x]$  iff  $F[x]$ . Only the  $R[x] \implies F[x]$  direction holds for general polynomials.

**Theorem 2.16:** If  $R$  is a UFD, then so is  $R[x]$ .

Let  $R$  be a UFD and  $x_1, \dots, x_n$  be  $n$  commutative variables and define the ring  $R[x_1, \dots, x_n]$  of polynomials in  $n$  variables inductively by

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

**Corollary 2.17:** If  $R$  is a UFD, then for all  $n \in \mathbb{Z}^+$ ,  $R[x_1, \dots, x_n]$  is a UFD.

Since  $\mathbb{Z}$  is a UFD,  $\mathbb{Z}[x]$  and  $\mathbb{Z}[x_1, \dots, x_n]$  are UFDs. With this, we can say that PID  $\subsetneq$  UFD because  $\mathbb{Z}[x]$  is a UFD but not a PID.

**Theorem 2.18** (Eisenstein's criterion): Let  $R$  be a UFD with field of fractions  $F$ . Let  $h(x) = c_n x^n + \dots + c_1 x + c_0 \in R[x]$  with  $n \geq 1$ . Let  $\ell \in R$  be irreducible. If:

- $\ell \nmid c_n$
- $\ell \mid c_i$  for all  $i = 0, \dots, n-1$
- $\ell^2 \nmid c_0$

Then  $h$  is irreducible in  $F[x]$ .

*Proof:* By contradiction. If  $h(x)$  is reducible in  $F[x]$ , by Gauss' lemma there are  $r(x), s(x) \in R[x]$  of degree at least 1 so  $h(x) = s(x)r(x)$ . Write

$$\begin{aligned}s(x) &= a_0 + \dots + a_m x^m \\ r(x) &= b_0 + \dots + b_k x^k.\end{aligned}$$

where  $1 \leq m, k < n$ . Since  $h(x) = s(x)r(x)$  we have

$$c_0 = a_0 b_0, \dots, c_{k+s} = \sum_{i+j=k+s} a_i b_j.$$

Consider the constant term. Since  $\ell \mid c_0$ , we have  $\ell \mid a_0 b_0$ . Since  $\ell$  is irreducible and  $R$  is a UFD,  $\ell$  is prime, hence  $\ell \mid a_0$  or  $\ell \mid b_0$ . Wlog, suppose  $\ell \mid a_0$ . Since  $\ell^2 \nmid c_0$ , we have  $\ell \nmid b_0$ .

If we consider the coefficient of  $x$ , since  $\ell \mid c_1$  we have  $\ell \mid (a_0 b_1 + a_1 b_0)$  where  $\ell \mid a_0$  but  $\ell \nmid b_0$ , hence  $\ell \mid a_1 b_0 \implies \ell \mid a_1$ .

By repeating the above argument, conditions on coefficients of  $h(x)$  imply that  $\ell \mid a_i$  for all  $1 \leq i \leq m-1$ . However,  $\ell \nmid a_m$  since  $\ell \nmid c_m$ . Consider the reduction  $\bar{h}(x) = \bar{s}(x)\bar{r}(x) \in (R/\langle \ell \rangle)[x]$ . By the assumption on the coefficients of  $h$ , we have  $\bar{h}(x) = \bar{c}_n x^n$ . However, since  $\bar{s}(x) = \bar{a}_m x^m$  and  $\ell \nmid b_0$ ,  $\bar{s}(x)\bar{r}(x)$  contains the term  $\bar{a}_m \bar{b}_0 x^m$ , which is a contradiction. Thus  $h(x)$  is irreducible in  $F[x]$ .  $\square$

*Example:* Consider  $2x^7 + 3x^4 + 6x^2 + 12$ , where for  $p = 3$  by Eisenstein's criterion this is irreducible in  $\mathbb{Q}[x]$ .

*Example:* Let  $p$  be prime and  $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$  be a  $p^{\text{th}}$  root of unity. Now  $\zeta_p$  is a root of the  $p^{\text{th}}$  cyclotomic polynomial

$$\begin{aligned}\Phi_p(x) &= \frac{x^p - 1}{x - 1} \\ &= x^{p-1} + x^{p-2} + \dots + x + 1.\end{aligned}$$

Eisenstein's does not work directly here, but  $\Phi_p(x+1)$  is irreducible iff  $\Phi_p(x)$  is, so

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \dots + \binom{p}{p-2} x + \binom{p}{p-1} \in \mathbb{Z}[x].\end{aligned}$$

Then  $p \mid \binom{p}{i}$  for  $i = 1, \dots, p-1$ , but  $p \nmid 1$  and  $p^2 \nmid \binom{p}{p-1} = p$ . Thus by Eisenstein's criterion  $\Phi_p(x+1)$  is irreducible iff  $\Phi_p(x)$  is irreducible in  $\mathbb{Q}[x]$ . Furthermore, observe  $\Phi_p(x)$  is primitive, so by [Proposition 2.15](#) it is irreducible in  $\mathbb{Z}[x]$  as well.

## 3 Field Extensions

### 3.1 Basics

**Definition** (Field extension): If  $E$  is a field containing another field  $F$ , we say  $E$  is a **field extension** of  $F$ , denoted  $E/F$ .

*Remark:*  $E/F$  does *not* mean a quotient ring, as the only ideals are  $\{0\}$  and  $E$ .

If  $E/F$  is a field extension, we can view  $E$  as a vector space over  $F$  with the obvious addition and scaling.

**Definition** (Degree): The dimension of  $E$  over  $F$  is called the **degree** of  $E$  over  $F$ , denoted  $[E : F]$ . If  $[E : F] < \infty$  we say  $E/F$  is a finite extension, and otherwise it is an infinite extension.

*Example:*  $[\mathbb{C} : \mathbb{R}] = 2$  is a finite extension.

*Example:* Let  $F$  be a field and let  $F(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x], g(x) \neq 0 \right\}$ . Then  $[F(x) : F]$  is an infinite extension since  $\{1, x, x^2, \dots\}$  is linearly independent over  $F$ .

**Theorem 3.1** (Intermediate field extensions): If  $E/K$  and  $K/F$  are finite field extensions then  $E/F$  is a finite field extension with

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

In particular, if  $K$  is an intermediate field of a finite extension  $F$ , then  $[K : F] \mid [E : F]$ .

*Proof:* Suppose  $[E : K] = m$  and  $[K : F] = n$ . Let  $\{a_1, \dots, a_m\}$  and  $\{b_1, \dots, b_n\}$  be bases for  $E/K$  and  $K/F$  respectively. It suffices to show  $\{a_i b_j\}$  is a basis for  $E/F$ .

For  $e \in E$  we have

$$e = \sum_{i=1}^m k_i a_i$$

for some  $k_i \in K$ , and for each  $k_i$  we have

$$k_i = \sum_{j=1}^n c_{i,j} b_j$$

with each  $c_{i,j} \in F$ . Hence

$$e = \sum_{i=1}^m \sum_{j=1}^n c_{i,j} b_j a_i \in \text{Span}_F \{a_i b_j\}.$$

Next, we have

$$\begin{aligned} \sum_{i=1}^m \sum_{j=1}^n c_{i,j} a_i b_j &= 0 \\ \implies \sum_{i=1}^m a_i \sum_{j=1}^n c_{i,j} b_j &= 0. \end{aligned}$$

Since the  $a_i$  are LI in  $E/K$  with each sum term in  $K$ , by linear independence of the  $a_i$  over  $K$  we have

$$\sum_{j=1}^n c_{i,j} b_j = 0$$

for each  $i$ . Then by the linear independence of the  $b_j$  over  $K/F$ , we have each  $c_{i,j} = 0$ , so the  $\{a_i b_j\}$  are LI.  $\square$

**Definition** (Algebraic, transcendental): Let  $E/F$  be a field extension and  $\alpha \in E$ . We say  $\alpha$  is **algebraic over  $F$**  if there is  $f(x) \in F[x] \setminus \{0\}$  such that  $f(\alpha) = 0$ . Otherwise,  $\alpha$  is **transcendental over  $F$** .

*Example:*  $q \in \mathbb{Q}$  and  $\sqrt{2}$  are algebraic over  $\mathbb{Q}$ , but  $e$  and  $\pi$  are transcendental over  $\mathbb{Q}$ .

*Example:* Claim:  $\alpha = \sqrt{2} + \sqrt{3}$  is algebraic over  $\mathbb{Q}$ .

$$\begin{aligned} (\alpha - \sqrt{2})^2 &= 3 \\ \alpha^2 - 1 &= 2\sqrt{2}\alpha \\ \alpha^4 - 10\alpha^2 + 1 &= 0 \end{aligned}$$

So  $\alpha$  is a root of  $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ , so is algebraic over  $\mathbb{Q}$ .

Notation: Let  $E/F$  be a field extension and  $\alpha \in E$ . Then  $F[\alpha]$  denotes the smallest subring of  $E$  containing  $F$  and  $\alpha$ , and  $F(\alpha)$  denotes the smallest subfield of  $E$  containing  $F$  and  $\alpha$ . For  $\alpha, \beta \in E$  we define  $F[\alpha, \beta]$  and  $F(\alpha, \beta)$  similarly.

### 3.2 Simple extensions

**Definition** (Simple extension): If  $E = F(\alpha)$  for some  $\alpha \in E$ , we say  $E$  is a **simple extension** of  $F$ .

We would like to know what  $[F(\alpha) : F]$  is.

**Definition** ( $F$ -homomorphism): Let  $R, R_1$  be two rings containing a field  $F$ . A ring hom  $\varphi : R \rightarrow R_1$  is called an  $F$ -homomorphism if  $\varphi|_F = \text{id}$ .

**Theorem 3.2:** Let  $E/F$  be a field extension and  $\alpha \in E$ . If  $\alpha$  is transcendental over  $F$ , then  $F[\alpha] \cong F[x]$  and  $F(\alpha) \cong F(x)$ . In particular,  $F[\alpha] \neq F(\alpha)$ .

*Proof:* Define  $\psi : F(x) \rightarrow F(\alpha)$  as the unique  $F$ -hom mapping  $x \mapsto \alpha$ . Then for  $f(x), g(x) \in F[x]$  with  $g(x) \neq 0$ ,

$$\psi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)}.$$

Notice this is well-defined as  $\alpha$  is transcendental, so  $g(\alpha) \neq 0$ . Now  $\text{Ker } \psi$  is an ideal of  $F(x)$ , so  $\psi$  is injective as  $x \notin \text{Ker } \psi$ . Also, since  $F(x)$  is a field, so too is  $\text{Im } \psi$ , which contains  $F$  and  $\alpha$ , so  $F(\alpha) \subseteq \text{Im } \psi$ . Thus  $F(\alpha) = \text{Im } \psi$  and by the first isomorphism theorem,  $F(x)/\text{Ker } \psi \cong F(x) \cong \text{Im } \psi = F(\alpha)$ . As  $F[x]$  and  $F[\alpha]$  are subrings of these fields, they too are isomorphic.  $\square$

**Theorem 3.3:** Let  $E/F$  be a field extension with  $\alpha \in E$ . If  $\alpha$  is algebraic over  $F$ , there is a unique monic irreducible  $p(x) \in F[x]$ , called the **minimal polynomial of  $\alpha$  over  $F$** , such that there is an  $F$ -isomorphism  $\varphi : F[x]/\langle p(x) \rangle \rightarrow F[\alpha]$  with  $\varphi(x) = \alpha$  from which we conclude  $F[\alpha] = F(\alpha)$ .

*Remark:* Since  $\alpha$  is algebraic, the map in the proof of [Theorem 3.2](#) is not well-defined.

*Proof:* Consider the unique  $F$ -homomorphism  $\varphi : F[x] \rightarrow F[\alpha]$  sending  $x \mapsto \alpha$ . Since  $F[x]$  is a ring,  $\text{Im } \varphi$  is a ring containing  $F$  and  $\alpha$ , so  $F[\alpha] \subseteq \text{Im } \varphi$  gives  $\text{Im } \varphi = F[\alpha]$ .

Let  $I = \text{Ker } \varphi = \{f(x) \in F[x] : f(\alpha) = 0\}$ . Since  $\alpha$  is algebraic,  $I \neq \{0\}$ , where  $I$  is an ideal of  $F[x]$ . Since  $F[x]/I \cong \text{Im } \varphi = F[\alpha]$  is an integral domain,  $I$  is a prime ideal. As  $F[x]$  is a PID, there is a unique monic irreducible  $p(x)$  so that  $I = \langle p(x) \rangle$ . Since  $I$  is a prime ideal and therefore a maximal ideal,  $F[x]/\langle p(x) \rangle$  is a field by [Theorem 2.10](#).

Then,  $F[x]/\langle p(x) \rangle \cong F[\alpha]$  is a field containing  $F$  and  $\alpha$ , so  $F(\alpha) \subseteq F[\alpha]$ . The reverse containment is obvious, so  $F[\alpha] = F(\alpha)$ .  $\square$

*Remark:* If  $p(x)$  is the minimal polynomial of  $\alpha$  over  $F$ , we have  $\langle p(x) \rangle = \{f(x) \in F[x] : f(\alpha) = 0\}$ . In particular, if  $f(x) \in F[x]$  satisfies  $f(\alpha) = 0$ , then  $p(x) \mid f(x)$ .

As a direct consequence of these theorems, we have the following result:

**Theorem 3.4** (Degree of a simple extension): Let  $E/F$  be a field extension,  $\alpha \in E$ .

- (1)  $\alpha$  is transcendental over  $F$  iff  $[F(\alpha) : F]$  is infinite.
- (2)  $\alpha$  is algebraic over  $F$  iff  $[F(\alpha) : F]$  is finite. Moreover, if  $p(x)$  is the minimal polynomial of  $\alpha$  over  $F$ ,  $[F(\alpha) : F] = \deg(p)$  and  $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$  is a basis for  $F(\alpha)/F$ .

*Proof:* Notice (1) and (2) are equivalent contrapositives, so it suffices to just prove the forwards direction of each.

- (1) ( $\Rightarrow$ ) By [Theorem 3.2](#) we have  $F(x) \cong F(\alpha)$ . In  $F(x)$ , the elements  $\{1, x, x^2, \dots\}$  are linearly independent over  $F$ , so  $[F(\alpha) : F] = \infty$ .
- (2) ( $\Rightarrow$ ) By [Theorem 3.3](#),  $F(\alpha) \cong F[x]/\langle p(x) \rangle$ . Note that

$$F[x]/\langle p(x) \rangle = \{r(x) \in F[x] : \deg(r) < \deg(p)\}$$

so  $\{1, x, x^2, \dots, x^{\deg(p)-1}\}$  is a basis of  $F[x]/\langle p(x) \rangle$ .  $\square$

*Example:* Let  $p$  be a prime and  $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$  be a root of  $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \dots + x + 1$ . We know  $\Phi_p(x)$  is irreducible, so it is the minimal polynomial of  $\zeta_p$ . Thus by [Theorem 3.4](#),  $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ .

*Example:*  $\alpha = \sqrt{2} + \sqrt{3}$  is algebraic, as a root of  $x^4 - 10x^2 + 1$ . We would like to show that this is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  by showing  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ . Notice

$$(\alpha - \sqrt{2})^2 = \sqrt{3} \implies \sqrt{2} = \frac{\alpha^2 - 1}{2\alpha},$$

so  $\sqrt{2} \in \mathbb{Q}(\alpha)$ . We have the following diagram:

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

Since  $\sqrt{2}$  is a root of  $x^2 - 2$ , which is irreducible, we have  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ . Also,  $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ , giving  $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \geq 2$ . Since  $\alpha \in \mathbb{Q}(\alpha) \setminus \mathbb{Q}(\sqrt{2})$ , it follows that  $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 4$ . However,  $\alpha$  is a root of a degree 4 polynomial, so  $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 4$ , so we have equality, and thus  $x^4 - 10x^2 + 1$  is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ .

*Exercise 3.1:* Show that  $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ . ▶

*Exercise 3.2:* Can we show that  $x^4 - 10x^2 + 1$  is irreducible in  $\mathbb{Q}[x]$  by Eisenstein's? ▶

### 3.3 Finite extensions and the algebraic closure

It turns out that to understand finite field extensions, it suffices to understand simple ones.

**Theorem 3.5:** Let  $E/F$  be a field extension. If  $[E : F] < \infty$ , there exist  $\alpha_1, \dots, \alpha_n \in E$  such that

$$F \subsetneq F(\alpha_1) \subsetneq \dots \subsetneq F(\alpha_1, \dots, \alpha_n) = E.$$

*Proof:* By induction on  $[E : F]$ . If  $[E : F] = 1$ , then  $E = F$  and we are done. Suppose  $[E : F] > 1$  and the statement holds for all field extensions  $E_1/F_1$  with  $[E_1 : F_1] < [E : F]$ . Let  $\alpha_1 \in E \setminus F$  so by [Theorem 3.1](#) we have

$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F].$$

Since  $[F(\alpha_1) : F] > 1$ , we have  $[E : F(\alpha_1)] < [E : F]$  so by the IH, there are  $a_2, \dots, a_n \in E$  such that

$$F(\alpha_1) \subsetneq F(a_1, \alpha_2) \subsetneq \dots \subsetneq F(\alpha_1, \alpha_2, \dots, \alpha_n) = E.$$

Therefore placing  $F \subsetneq F(\alpha_1)$  at the start of this chain gives the desired result.  $\diamond$

**Definition** (Algebraic field extension): A field extension  $E/F$  is **algebraic** if every  $\alpha \in E$  is algebraic over  $F$ . Otherwise, it is **transcendental**.

**Theorem 3.6:** Let  $E/F$  be a field extension. If  $[E : F] < \infty$ , then  $E/F$  is algebraic.

*Proof:* Suppose  $[E : F] = n$ . For  $\alpha \in E$ , the elements  $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$  are not linearly independent over  $F$ , so there exist  $c_i \in F$  not all zero such that

$$\sum_{i=0}^n c_i \alpha^i = 0$$

i.e. that  $\alpha$  is a root of  $c_0 + \dots + c_n x^n \in F[x]$ , so  $\alpha$  is algebraic over  $F$ .  $\diamond$

**Theorem 3.7** (Algebraic closure): Let  $E/F$  be a field extension. Define

$$L := \{\alpha \in E : [F(\alpha) : F] < \infty\}.$$

Then  $L$ , called the **algebraic closure of  $F$  in  $E$** , is an intermediate field of  $E/F$ .

*Proof:* Certainly  $F \subseteq L$ , so if  $\alpha, \beta \in L$  we need to show  $\alpha \pm \beta, \alpha\beta$ , and  $\frac{\alpha}{\beta}$  for  $\beta \neq 0$  are all in  $L$ . By definition,  $[F(\alpha) : F], [F(\beta) : F] < \infty$ .

Consider the field  $F(\alpha, \beta)$ . Notice the minimal polynomial of  $\alpha$  over  $F$ , say  $p(x) \in F[x]$ , is also an element of  $F(\beta)[x]$  with  $p(\alpha) = 0$ . Therefore the minimal polynomial of  $\alpha$  over  $F(\beta)$  divides the minimal polynomial of  $\alpha$  over  $F$ , so the former has at most the degree of the latter. It follows by [Theorem 3.1](#) that

$$\begin{aligned} [F(\alpha, \beta) : F(\beta)] &\leq [F(\alpha) : F] \\ [F(\alpha, \beta) : F] &= [F(\alpha, \beta) : F(\beta)][F(\beta) : F] \leq [F(\alpha) : F][F(\beta) : F] < \infty. \end{aligned}$$

Now since  $\alpha \pm \beta \in F(\alpha, \beta)$ , we have  $[F(\alpha \pm \beta) : F] \leq [F(\alpha, \beta) : F] < \infty$ , so  $\alpha \pm \beta \in L$ . Similarly, we can show  $\alpha\beta, \frac{\alpha}{\beta} \in L$ , so  $L$  is a field.  $\diamond$

**Definition** (Algebraically closed): A field  $F$  is **algebraically closed** if for any algebraic extension  $E/F$ , we have  $E = F$ .

*Example:* By the fundamental theorem of algebra,  $\mathbb{C}$  is algebraically closed. Moreover,  $\mathbb{C}$  is the algebraic closure of  $\mathbb{R}$  in  $\mathbb{C}$ .

*Example:* Let  $\overline{\mathbb{Q}}$  be the algebraic closure of  $\mathbb{Q}$  in  $\mathbb{C}$ , i.e.

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

For a prime  $p$ , since  $\zeta_p \in \overline{\mathbb{Q}}$  as  $\zeta_p$  is a root of its minimal polynomial  $\Phi_p(x)$ , we have

$$[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

As there are infinitely many primes,  $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ . In particular, this example shows that an algebraic extension need not be finite, i.e. the converse of [Theorem 3.6](#) is false.

## 4 Splitting Fields

### 4.1 Existence

**Definition** (Splits over): Let  $E/F$  be a field extension. We say  $f(x) \in F[x]$  splits over  $E$  if  $E$  contains all roots of  $f(x)$ , i.e.  $f$  can be written as a product of linear factors in  $E[x]$ .

**Definition** (Splitting field): Let  $\tilde{E}/F$  be a field extension,  $f(x) \in F[x]$ , and  $F \subseteq E \subseteq \tilde{E}$ . If

- $f(x)$  splits over  $E$  and
- $f(x)$  does not split over any proper subfield of  $E$

we say that  $E$  is a splitting field of  $f(x)$  in  $\tilde{E}$ .

**Theorem 4.1:** Let  $p(x) \in F[x]$  be irreducible. The quotient ring  $F[x]/\langle p(x) \rangle$  is a field containing  $F$  and a root of  $p(x)$ .

*Proof:* Since  $p(x)$  is irreducible,  $I := \langle p(x) \rangle$  is a prime ideal. Since  $F[x]$  is a PID,  $I$  is maximal iff  $E := F[x]/I$  is a field. Consider the map

$$\begin{aligned}\varphi : F &\rightarrow E \\ a &\mapsto a + I.\end{aligned}$$

Since  $F$  is a field and  $\varphi \neq 0$ ,  $\varphi$  is injective. Thus by identifying  $F$  with  $\varphi(F)$ , we view  $F$  as a subfield of  $E$ . We claim  $\alpha := x + I$  is a root of  $p(x)$ . Write

$$\begin{aligned}p(x) &= a_0 + a_1x + \dots + a_nx^n \in F[x] \\ &= (a_0 + I) + (a_1 + I)x + \dots + (a_n + I)x^n \in E[x].\end{aligned}$$

We have

$$\begin{aligned}p(\alpha) &= a_0 + I + (a_1 + I)\alpha + \dots + (a_n + I)\alpha^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + \dots + (a_n + I)(x + I)^n \\ &= (a_0 + a_1x + \dots + a_nx^n) + I \\ &= p(x) + I = 0 + I = I.\end{aligned}$$

Thus  $\alpha = x + I \in E$  is a root of  $p(x)$ .  $\diamond$

**Theorem 4.2** (Kronecker's theorem): Let  $f(x) \in F[x]$ . There exists a field  $E$  containing  $F$  such that  $f(x)$  splits over  $E$ .

*Proof:* By induction on  $\deg(f)$  with any field. If  $\deg(f) = 1$ , we let  $E = F$  and are done. If  $\deg(f) > 1$ , write  $f(x) = p(x)h(x)$  with  $p(x)$  irreducible in  $F[x]$ . By [Theorem 4.1](#), there is a field  $K$  with  $F \subseteq K$  containing a root of  $p(x)$ , say  $\alpha$ . Thus

$$\begin{aligned}p(x) &= (x - \alpha)q(x) \\ \Rightarrow f(x) &= (x - \alpha)q(x)h(x)\end{aligned}$$

where  $q(x) \in K[x]$ . Since  $\deg(qh) < \deg(f)$ , by induction there is a field  $E$  containing  $K$  over which  $q(x)h(x)$  splits. It follows that  $f(x)$  splits over  $E$ .  $\diamond$

**Theorem 4.3** (Splitting fields are finite extensions): Every  $f(x) \in F[x]$  has a splitting field which is a finite extension of  $F$ .

*Proof:* For  $f(x) \in F[x]$ , by [Theorem 4.2](#) there is a field extension  $E/F$  over which  $f(x)$  splits. Say  $\alpha_1, \dots, \alpha_n$  are the roots of  $f(x)$  in  $E$ . Consider  $L := F(\alpha_1, \dots, \alpha_n)$ , which is the smallest subfield of  $E$  containing all roots of  $f(x)$ , so  $f(x)$  does not split over any proper subfield of  $L$ . Thus  $L/F$  is a splitting field of  $f(x)$  in  $E$ . In addition, since the  $\alpha_i$  are all algebraic in  $L$ ,  $[L : F]$  is finite.  $\diamond$

*Example:* Consider  $x^3 - 2 \in \mathbb{Q}[x]$ . We know  $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta_3)(x - \sqrt[3]{2}\zeta_3^2)$  where  $\zeta_3 = \exp\left(\frac{2\pi i}{3}\right)$ . Hence the splitting field of  $x^3 - 2$  over  $\mathbb{Q}$  is

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3).$$

## 4.2 Uniqueness

**Question:** If we have two field extensions  $E/F$  and  $E_1/F$ , what is the relation between the splitting field of  $f(x)$  in  $E$  and in  $E_1$ ?

**Definition** (Homomorphism extension): Let  $\varphi : R \rightarrow R_1$  be a ring homomorphism, and  $\Phi : R[x] \rightarrow R_1[x]$  be the unique ring homomorphism satisfying  $\Phi|_R = \varphi$  and  $\Phi(x) = x$ . We say  $\Phi$  **extends**  $\varphi$ .

More generally, if  $R \subseteq S$  and  $R_1 \subseteq S_1$  are all rings and  $\Phi : S \rightarrow S_1$  is a ring homomorphism with  $\Phi|_R = \varphi$ , we say  $\Phi$  extends  $\varphi$ .

**Theorem 4.4:** Let  $\varphi : F \rightarrow F_1$  be a field isomorphism and  $f(x) \in F[x]$ . Let  $\Phi : F[x] \rightarrow F_1[x]$  extend  $\varphi$ . Let  $f_1(x) = \Phi(f(x))$  and  $E/F, E_1/F_1$  be splitting fields of  $f(x)$  and  $f_1(x)$  respectively. Then there is an isomorphism  $\psi : E \rightarrow E_1$  which extends  $\varphi$ .

*Proof:* By induction on  $[E : F]$ . If  $[E : F] = 1$ , then  $f(x)$  is a product of linear factors in  $F[x]$ , and so is  $f_1(x)$  in  $F_1[x]$ . Thus  $E = F, E_1 = F_1$ , so let  $\psi = \varphi$  and we are done.

Suppose  $[E : F] > 1$  and the statement holds for all  $\tilde{E}/\tilde{F}$  with  $[\tilde{E} : \tilde{F}] < [E : F]$ . Let  $p(x) \in F[x]$  be an irreducible factor of  $f(x)$  with  $\deg(p) \geq 2$ . Such a  $p$  exists, as otherwise all the irreducible factors of  $f$  are degree 1, giving  $[E : F] = 1$ . Define  $p_1(x) := \Phi(p(x))$ .

Let  $\alpha \in E$  and  $\alpha_1 \in E_1$  be roots of  $p(x)$  and  $p_1(x)$  respectively. From [Theorem 3.3](#), we have the  $F$  and  $F_1$ -isomorphisms

$$\begin{aligned} F(\alpha) &\cong F[x]/\langle p(x) \rangle, \quad \alpha \mapsto x + \langle p(x) \rangle \\ F_1(\alpha_1) &\cong F_1[x]/\langle p_1(x) \rangle, \quad \alpha_1 \mapsto x + \langle p_1(x) \rangle. \end{aligned}$$

Consider the isomorphism  $\Phi : F[x] \rightarrow F_1[x]$  extending  $\varphi$ . Since  $p_1(x) = \Phi(p(x))$ , there is a field isomorphism  $\tilde{\Phi}$  given by

$$\begin{aligned} \tilde{\Phi} : F[x]/\langle p(x) \rangle &\rightarrow F_1[x]/\langle p_1(x) \rangle \\ x + \langle p(x) \rangle &\mapsto x + \langle p_1(x) \rangle \end{aligned}$$

which extends  $\varphi$ . It follows from the commutative diagram below that there exists a field isomorphism  $\tilde{\varphi} : F(\alpha) \rightarrow F_1(\alpha_1), \alpha \mapsto \alpha_1$  extending  $\varphi$ .

$$\begin{array}{ccccc} & & \psi & & \\ E & \xrightarrow{\quad} & E_1 & & \\ | & \nearrow \sim & \downarrow & \searrow \sim & | \\ F(\alpha) & \xrightarrow{\tilde{\Phi}} & F_1[x]/\langle p_1(x) \rangle & \xrightarrow{\sim} & F_1(\alpha_1) \\ | & \searrow \tilde{\varphi} & & \nearrow & | \\ F & \xrightarrow{\quad} & F_1 & \xrightarrow{\quad} & F_1 \end{array}$$

Notice since  $\deg(p) \geq 2$ , we have  $[E : F(\alpha)] < [E : F]$ . Since  $E$  (resp.  $E_1$ ) is the splitting field of  $f(x) \in F(\alpha)[x]$  (resp.  $f_1(x) \in F_1(\alpha_1)[x]$ ) over  $F(\alpha)$  (resp.  $F_1(\alpha_1)$ ), by induction there is an isomorphism  $\psi : E \rightarrow E_1$  which extends  $\tilde{\varphi}$ . Therefore  $\psi$  extends  $\varphi$ .  $\square$

**Corollary 4.5** (Uniqueness of splitting fields): Any two splitting fields of  $f(x) \in F[x]$  over  $F$  are isomorphic, and so we can say *the* splitting field of  $f(x)$  over  $F$ .

*Proof:* Let  $\varphi : F \rightarrow F$  be the identity map, and apply [Theorem 4.4](#).  $\diamond$

**Theorem 4.6:** Let  $F$  be a field,  $f(x) \in F[x]$  with  $\deg(f) = n \geq 1$ . If  $E/F$  is the splitting field of  $f(x)$ , then  $[E : F] \mid n!$ .

*Proof:* By induction on  $\deg(f)$ . If  $\deg(f) = 1$ , choose  $E = F$  and we have  $[E : F] \mid 1!$ . Suppose  $\deg(f) > 1$  and the statement holds for all  $g(x)$  with  $\deg(g) < \deg(f)$ . Two cases:

*Case 1.*  $f(x)$  is irreducible in  $F[x]$ . Let  $\alpha \in E$  be a root of  $f(x)$ , and by [Theorem 3.3](#)

$$\begin{aligned} F(\alpha) &\cong F[x]/\langle f(x) \rangle \\ \text{and } [F(\alpha) : F] &= \deg(f) = n \end{aligned}$$

since  $f$  is the minimal polynomial of  $\alpha$ . Write  $f(x) = (x - \alpha)g(x)$  with  $g(x) \in F(\alpha)[x]$  and  $\deg(g) \leq n - 1$ . Since  $E$  is the splitting field of  $g(x)$  over  $F(\alpha)$ , by induction  $[E : F(\alpha)] \mid (n - 1)!$  which gives

$$[E : F] = [E : F(\alpha)][F(\alpha) : F] = n \cdot [E : F(\alpha)] \implies [E : F] \mid n!.$$

*Case 2.*  $f(x)$  is reducible in  $F[x]$ . Write  $f(x) = g(x)h(x)$  with  $g(x), h(x) \in F[x]$  and  $\deg(g) = m, \deg(h) = k, m + k = n$ , and  $1 \leq m, k < n$ . Let  $K$  be the splitting field of  $g(x)$  over  $F$ . Since  $\deg(g) = m$ , by induction  $[K : F] \mid m!$ . Since  $E$  is the splitting field of  $h(x)$  over  $K$ , by induction  $[E : K] \mid k!$ . Therefore  $[E : F] \mid m!k!$  which is a factor of  $n!$  since  $\binom{n}{m} = \frac{n!}{m!k!}$  is an integer.

Aside:  $E$  is the splitting field of  $h(x)$  over  $K$  because certainly  $h(x)$  splits over  $E$ , and if  $L/K$  were to be a splitting field for  $h(x)$  with  $L \subsetneq E$ , then  $f(x)$  would split over  $L$  as well. However,  $E$  is the splitting field of  $f(x)$  over  $F$ , a contradiction.  $\diamond$

## 5 More Field Theory

### 5.1 Prime fields

**Definition** (Prime field): The **prime field** of a field  $F$  is the intersection of all subfields of  $F$ .

**Theorem 5.1:** If  $F$  is a field, its prime field is isomorphic to either  $\mathbb{Q}$  or  $\mathbb{Z}_p$  for a prime  $p$ .

**Definition** (Character): Given a field  $F$ , if its prime field is isomorphic to  $\mathbb{Q}$  (resp.  $\mathbb{Z}_p$ ), we say  $F$  has characteristic 0 (resp.  $p$ ), denoted  $\text{ch}(F) = 0$  (resp.  $\text{ch}(F) = p$ ).

*Remark:* When  $\text{ch}(F) = p$ , for  $a, b \in F$ ,

$$\begin{aligned} (a+b)^p &= a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} a b^{p-1} + \binom{p}{p} b^p \\ &= a^p + b^p \end{aligned}$$

since  $p \mid \binom{p}{i}$  for each  $i = 1, \dots, p-1$ .

*Proof of Theorem 5.1:* Let  $F_1$  be a subfield of  $F$ . Consider the map

$$\begin{aligned} \chi : \mathbb{Z} &\rightarrow F_1 \\ n &\mapsto n \cdot 1 \end{aligned}$$

where  $1 \in F_1 \subseteq F$ . Let  $I = \text{Ker } \chi$ . Since  $\mathbb{Z}/I \cong \text{Im } \chi$ , a subring of  $F_1$ ,  $\mathbb{Z}/I$  is an integral domain. Thus  $I$  is a prime ideal.

- If  $I = \langle 0 \rangle$ , then  $\mathbb{Z} \subseteq F_1$ . Since  $F_1$  is a field,  $\mathbb{Q} = \text{Frac}(\mathbb{Z}) \subseteq F_1$ .
- If  $I = \langle p \rangle$  for a prime  $p$ ,  $\mathbb{Z}_p \cong \mathbb{Z}/\langle p \rangle \cong \text{Im } \chi \subseteq F_1$ .  $\square$

**Proposition 5.2:** Let  $F$  be a field with  $\text{ch}(F) = p$  and  $n \in \mathbb{N}$ . Then  $\varphi : F \rightarrow F, u \mapsto u^{p^n}$  is an injective  $\mathbb{Z}_p$ -homomorphism of fields. In particular if  $F$  is finite, then  $\varphi$  is a  $\mathbb{Z}_p$ -isomorphism.

*Proof:* By (a slight modification of) the previous remark,  $\varphi(a+b) = \varphi(a) + \varphi(b)$  and multiplicativity is obvious, so  $\varphi$  is indeed a hom. Also,  $1 \notin \text{Ker}(\varphi)$ , so  $\text{Ker}(\varphi) \neq F \implies \text{Ker}(\varphi) = \{0\}$  since  $F$  is a field, hence  $\varphi$  is injective. For  $a \in \mathbb{Z}_p$ , we have  $a = a \cdot 1 \implies \varphi(a) = a\varphi(1) = a1 = a$  and so  $\varphi$  is a  $\mathbb{Z}_p$ -hom.  $\square$

### 5.2 Formal derivatives and repeated roots

**Definition** (Formal derivative): If  $F$  is a field, the monomials  $\{1, x, x^2, \dots\}$  form an  $F$ -basis for  $F[x]$ . Define the linear operator

$$\begin{aligned} D : F[x] &\rightarrow F[x] \\ 1 &\mapsto 0 \\ x^i &\mapsto ix^{i-1}, \forall i \in \mathbb{N}. \end{aligned}$$

Notice that  $D(f+g) = D(f) + D(g)$  and  $D(fg) = D(f)g + fD(g)$ . We call  $D(f) =: f'$  the **formal derivative** of  $f$ .

**Theorem 5.3:** Let  $F$  be a field,  $f(x) \in F[x]$ .

- (1) If  $\text{ch}(F) = 0$ , then  $f'(x) = 0 \iff f(x) = c$  for some  $c \in F$ .
- (2) If  $\text{ch}(F) = p$ , then  $f'(x) = 0 \iff f(x) = g(x^p)$  for some  $g(x) \in F[x]$ .

*Proof:*

(1) ( $\Leftarrow$ ) is clear. For ( $\Rightarrow$ ), say  $f(x) = a_0 + \dots + a_n x^n$ . Then

$$f'(x) = a_1 + 2a_2 x + \dots + na_n x^{n-1} = 0$$

implies that each  $ia_i = 0$  for all  $i = 1, \dots, n$ . Since  $\text{ch}(F) = 0$  we have  $i \neq 0$ , and so each  $a_i = 0$ . Therefore  $f(x) = a_0$ .

(2) ( $\Leftarrow$ ) Write  $g(x) = b_0 + b_1x + \dots + b_mx^m \in F[x]$ . Then

$$\begin{aligned} f(x) &= g(x^p) = b_0 + b_1x^p + \dots + b_mx^{pm} \\ \implies f'(x) &= b_1px^{p-1} + \dots + b_mpmx^{pm-1}. \end{aligned}$$

Since  $\text{ch}(F) = p$ , we have  $p = 0$  so  $f'(x) = 0$ .

( $\Rightarrow$ ) For  $f(x) = a_0 + \dots + a_nx^n$ ,

$$f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1} = 0$$

implies  $ia_i = 0$ . Since  $\text{ch}(F) = p$ ,  $ia_i = 0$  gives  $a_i = 0$  unless  $p \mid i$ . Thus

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots + a_{mp} x^{mp} = g(x^p)$$

where  $g(x) = a_0 + a_p x + \dots + a_{mp} x^m$ .  $\diamond$

**Definition** (Repeated root): Let  $E/F$  be a field extension,  $f(x) \in F[x]$ . We say  $\alpha \in E$  is a **repeated root** of  $f(x)$  if  $f(x) = (x - \alpha)^2 g(x)$  for some  $g(x) \in E[x]$ .

**Theorem 5.4:** Let  $E/F$  be a field extension,  $f(x) \in F[x]$ ,  $\alpha \in E$ . Then  $\alpha$  is a repeated root of  $f(x)$  iff  $x - \alpha$  divides both  $f$  and  $f'$ , i.e.  $(x - \alpha) \mid \text{gcd}(f, f')$ .

*Proof:* ( $\Rightarrow$ ) Suppose  $f(x) = (x - \alpha)^2 g(x)$ . Then

$$\begin{aligned} f'(x) &= 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x) \\ &= (x - \alpha)[2g(x) + (x - \alpha)g'(x)], \end{aligned}$$

so  $(x - \alpha) \mid f, f'$ .

( $\Leftarrow$ ) Suppose  $(x - \alpha) \mid f, f'$ . Write  $f(x) = (x - \alpha)h(x)$  with  $h(x) \in E[x]$ . Then

$$\begin{aligned} f'(x) &= h(x) + (x - \alpha)h'(x) \\ \implies h(\alpha) &= f'(\alpha) - (\alpha - \alpha)h'(\alpha) = 0, \end{aligned}$$

since  $(x - \alpha) \mid f'$ . So  $\alpha$  is a root of  $h$ , giving  $(x - \alpha) \mid h$ , hence  $f(x) = (x - \alpha)^2 g(x)$  for some  $g(x) \in E[x]$ .  $\diamond$

**Definition** (Separable): Let  $F$  be a field,  $f(x) \in F[x] \setminus \{0\}$ . We say  $f(x)$  is **separable over  $F$**  if it has no repeated roots in any extension of  $F$ .

*Example:*  $f(x) = (x - 4)(x - 9)$  is separable in  $\mathbb{Q}[x]$ .

**Corollary 5.5:** Let  $F$  be a field and  $f(x) \in F[x]$ .  $f(x)$  is separable iff  $\text{gcd}(f, f') = 1$ .

*Remark:* The condition of repeated roots depends on the extension of  $F$  while  $\text{gcd}$  involves only  $F$ .

*Proof:* Note  $\text{gcd}(f, f') \neq 1 \iff (x - \alpha) \mid \text{gcd}(f, f')$  for some  $\alpha$  in some extension of  $F$ . By [Theorem 5.4](#), the result follows.  $\diamond$

**Corollary 5.6:** If  $\text{ch}(F) = 0$ , then every irreducible  $r(x) \in F[x]$  is separable.

*Proof:* Let  $r(x) \in F[x]$  be irreducible. Then

$$\text{gcd}(r, r') = \begin{cases} 1 & \text{if } r' \neq 0 \\ r & \text{if } r' = 0 \end{cases}$$

If  $r'(x) = 0$ , then  $r(x) = c$  for  $c \in F$ , but  $\deg(r) \geq 1$  as  $r$  is irreducible, so we must have  $\text{gcd}(r, r') = 1$  and the result follows by [Corollary 5.5](#).  $\diamond$

**Example:**  $\Phi_p(x) = 1 + x + \dots + x^{p-1} = \frac{x^p - 1}{x - 1}$  is irreducible, hence separable. Recall the roots of  $\Phi_p(x)$  are  $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$  which are all distinct.

### 5.3 Finite fields

Given a field  $F$ , define  $F^\times := F \setminus \{0\}$  (the group of units).

**Proposition 5.7:** If  $F$  is a finite field, then  $\text{ch}(F) = p$  for some prime  $p$  and  $|F| = p^n$  for some  $n \in \mathbb{N}$ .

*Proof:* Since  $F$  is finite, by [Theorem 5.1](#) its prime field is  $\mathbb{Z}_p$  for some prime  $p$ . Since  $F$  is a finite dimensional vector space over  $\mathbb{Z}_p$ ,  $F \cong \mathbb{Z}_p^n$  where  $n = [F : \mathbb{Z}_p]$ . Therefore  $|F| = |\mathbb{Z}_p|^n = p^n$ .  $\square$

**Theorem 5.8:** Let  $F$  be a field and  $G$  a finite subgroup of  $F^\times$ . Then  $G$  is cyclic. In particular, the group of units of a finite field is cyclic.

*Proof:* Wlog we assume  $G \neq \{1\}$ . Since  $G$  is abelian, by the classification of finite abelian groups

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_r}$$

where each  $n_i | n_{i+1}$  and  $n_i > 1$  since  $G \neq \{1\}$ . Notice every  $g \in G$  must then satisfy  $g^{n_r} = 1$ , so is a root of  $x^{n_r} - 1 \in F[x]$ . Since  $x^{n_r} - 1$  has at most  $n_r$  distinct roots in  $F$ , we have  $|G| \leq n_r$ , where the above isomorphism gives  $|G| = n_1 \times n_2 \times \dots \times n_r$ , so it must be that  $r = 1$  and  $G \cong \mathbb{Z}_{n_1}$  is a cyclic group.  $\square$

**Corollary 5.9:** If  $F$  is a finite field, then  $F$  is a simple extension of  $\mathbb{Z}_p$ .

*Proof:* By taking  $u \in F$  to be a generator of  $F^\times$ , we have  $F = \mathbb{Z}_p(u)$ .  $\square$

**Theorem 5.10:** Let  $p$  be a prime and  $n \in \mathbb{N}$ .

- (1)  $F$  is a finite field with  $|F| = p^n$  iff  $F$  is the splitting field of  $x^{p^n} - x$  over  $\mathbb{Z}_p$ .
- (2) Let  $F$  be a finite field with  $|F| = p^n$ , let  $m \in \mathbb{N}$  with  $m | n$ . Then  $F$  contains a unique subfield  $K$  with  $|K| = p^m$ .

*Proof:*

(1) ( $\Rightarrow$ ) Suppose  $|F| = p^n$ . Then  $|F^\times| = p^n - 1$ , so every  $u \in F^\times$  satisfies  $u^{p^n-1} = 1$ , thus is a root of  $f(x) := x(x^{p^n-1} - 1) = x^{p^n} - x \in \mathbb{Z}_p[x]$ . Also,  $0 \in F$  is a root of  $f(x)$ , so every element of  $F$  is a root of  $f(x)$  which therefore has  $p^n$  distinct roots in  $F$ . Clearly  $f(x)$  cannot split over any smaller field, so  $F$  must be the splitting field of  $f(x)$  over  $\mathbb{Z}_p$ .

( $\Leftarrow$ ) Suppose  $F$  is the splitting field of  $f(x) := x^{p^n} - x$  over  $\mathbb{Z}_p$ . Since  $\text{ch}(F) = p$ , we have

$$f'(x) = p^n x^{p^n-1} - 1 = -1.$$

Thus  $\gcd(f, f') = 1$ , so by [Corollary 5.5](#)  $f(x)$  has  $p^n$  distinct roots in  $F$ . Let  $E$  be the set of all roots of  $f(x)$  in  $F$  and define

$$\begin{aligned} \varphi : F &\rightarrow F \\ u &\mapsto u^{p^n}. \end{aligned}$$

Notice  $u \in F$  satisfies  $u \in E$  iff  $\varphi(u) = u$ . This equality condition is closed under  $+, -, \times, /$ , and so  $E$  is a subfield of  $F$  of order  $p^n$ . Since  $F$  is a splitting field, it is generated over  $\mathbb{Z}_p$  by the roots of  $f(x)$  i.e. the elements of  $E$ , so  $F = \mathbb{Z}_p(E) = E$ , giving  $|F| = p^n$ .

- (2) Let  $\alpha \neq 0$  be a root of  $x^{p^m} - x$ , so  $\alpha$  must be a root of  $x^{p^m-1} - 1$ , giving  $\alpha^{p^m-1} = 1$ . We recall

$$x^{ab} - 1 = (x^a - 1)(x^{ab-a} + x^{ab-2a} + \dots + 1)$$

so as  $m | n \Leftrightarrow n = mk$  for  $k \in \mathbb{Z}$ , we have

$$p^n - 1 = p^{mk} - 1 = (p^m - 1)M$$

for some  $M \in \mathbb{Z}$ , and so

$$\alpha^{p^n-1} = \alpha^{(p^m-1)M} = (\alpha^{p^m-1})^M = 1^M = 1.$$

Therefore  $\alpha$  is a root of  $x^{p^n-1} - 1$ , and so every root of  $x^{p^m} - x$  is a root of  $x^{p^n} - x$ . Since  $x^{p^n} - x$  splits over  $F$ , so does  $x^{p^m} - x$ . Let

$$K := \{u \in F : u^{p^m} - u = 0\}.$$

Then  $|K| = p^m$  since the roots of  $x^{p^m} - x$  are distinct and by (1),  $K$  is a field. Now if  $\tilde{K} \subseteq F$  is a subfield with  $|\tilde{K}| = p^m$ , then  $\tilde{K} \subseteq K$ , since all elements  $v \in \tilde{K}$  satisfy  $v^{p^m} - v = 0$ . Therefore  $\tilde{K} = K$ , so  $K$  is unique.  $\square$

**Corollary 5.11** (E.H. Moore): Let  $p$  be a prime and  $n \in \mathbb{N}$ . Then any two finite fields of order  $p^n$  are isomorphic. We denote such a field by  $\mathbb{F}_{p^n}$ .

*Proof:* Follows by [Theorem 5.10](#) and uniqueness of splitting fields.  $\square$

**Definition** ( $F^p$ ): Let  $F$  be a field with  $\text{ch}(F) = p$ . Define  $F^p := \{b^p : b \in F\}$ .

*Remark:*  $F^p$  is a subfield of  $F$  as  $(a+b)^p = a^p + b^p$  and multiplicativity is obvious.

**Theorem 5.12:** Let  $F$  be a finite field with  $\text{ch}(F) = p$ .

- (1)  $F = F^p$ .
- (2) Every irreducible  $r(x) \in F[x]$  is separable.

*Proof:*

- (1) Clearly  $F^p \subseteq F$ . Every finite field  $F = \mathbb{F}_p^n$  is the splitting field of  $x^{p^n} - x$  over  $\mathbb{Z}_p$  for some prime  $p$  and  $n \in \mathbb{Z}^+$ . Thus for any  $a \in F$ ,

$$a = a^{p^n} = (a^{p^{n-1}})^p \in F^p.$$

- (2) Let  $r(x) \in F[x]$  be irreducible. Now  $\gcd(r, r')$  divides  $r(x)$ , so

$$\gcd(r, r') = \begin{cases} 1 & \text{if } r' \neq 0 \\ r & \text{if } r' = 0 \end{cases}$$

Supposing  $r' = 0$ , by [Theorem 5.3](#)  $r(x) = g(x^p)$  for some  $g(x) \in F[x]$ , but then

$$r(x) = a_0 + a_1 x^p + \dots + a_m x^{mp}$$

and since  $F = F^p$ , each  $a_i = b_i^p$  for some  $b_i \in F$ , giving

$$\begin{aligned} r(x) &= b_0^p + b_1^p x^p + \dots + b_m^p x^{mp} \\ &= (b_0 + b_1 x + \dots + b_m x_m)^p, \end{aligned}$$

so  $r(x)$  is reducible, a contradiction. Therefore  $\gcd(r, r') = 1$ , so by [Corollary 5.5](#) we have  $r(x)$  is separable.  $\square$

*Example:* We now know that irreducible implies separable in the following cases:

- $\text{ch}(F) = 0$ .
- $\text{ch}(F) = p$  and  $F$  is finite.

However, this is not true if  $\text{ch}(F) = p$  and  $F$  is infinite. Let  $F$  be a field with  $\text{ch}(F) = p$  and consider  $f(x) = x^p - a \in F[x]$ . Since  $f'(x) = px^{p-1} = 0$  we have  $\gcd(f, f') \neq 1$ , so by [Corollary 5.5](#)  $f(x)$  is not separable. Furthermore:

- (1) If  $a \in F^p$ , say  $a = b^p$ . Then  $f(x) = x^p - b^p = (x - b)^p$  and so  $f(x)$  is reducible.

(2) If  $a \notin F^p$ , let  $E/F$  be a field extension where  $x^p - a$  has a root  $\beta \in E$ . Then  $\beta^p = a$ , and since  $a \notin F^p$  we have  $\beta \notin F$ , so

$$f(x) = x^p - \beta^p = (x - \beta)^p$$

which is not separable. However, in this situation  $x^p - a$  is actually irreducible in  $F[x]$ .

*Proof:* Write  $x^p - a = g(x)h(x)$  for monic  $g(x), h(x) \in F[x]$ . We have

$$\begin{aligned} (x - \beta)^p &= g(x)h(x) \\ \Rightarrow g(x) &= (x - \beta)^r, \quad h(x) = (x - \beta)^s \end{aligned}$$

for some  $0 \leq r, s$  with  $r + s = p$ . Write

$$g(x) = x^r + r\beta x^{r-1} + \dots \in F[x],$$

so  $r\beta \in F$ . However  $\beta \notin F$  so it must be that  $r = 0 \in F$ . As an integer, then,  $r = 0$  or  $r = p$ . Either way,  $g(x) = 1$  or  $h(x) = 1$  (one is a unit), so  $f(x)$  is irreducible in  $F[x]$ .  $\square$

## 6 Solvable and Automorphism Groups

### 6.1 Solvable groups

**Definition** (Solvable): A group  $G$  is **solvable** if there is a tower

$$G = G_0 \supseteq G_1 \subseteq G_2 \supseteq \dots \supseteq G_m = \{1\}$$

with  $G_{i+1} \trianglelefteq G_i$  and  $G_i/G_{i+1}$  abelian for all  $i = 0, \dots, m-1$ .

*Remark:*  $G_{i+1}$  is not necessarily a normal subgroup of  $G$ , but if it is then we get  $G_{i+1} \trianglelefteq G_i$  for free.

*Example:* Consider  $S_4$ . Let  $V := \mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ . Note  $A_4$  and  $V$  are normal subgroups of  $S_4$ , and we have

$$S_4 \supseteq A_4 \supseteq V \supseteq \{e\}.$$

Since  $S_4/A_4 \cong \mathbb{Z}_2$ ,  $A_4/V \cong \mathbb{Z}_3$ , and  $V/\{e\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$  are all abelian,  $S_4$  is solvable.

Recall from group theory:

**Theorem 6.1** (Second isomorphism theorem): Let  $H, K \leq G$  with  $K \trianglelefteq G$ . Then  $HK \leq G$  and  $K \trianglelefteq HK$  and  $H \cap K \trianglelefteq H$  and  $HK/K \cong H/H \cap K$ .

**Theorem 6.2** (Third isomorphism theorem): Let  $K \leq H \leq G$  with  $K, H \trianglelefteq G$ . Then  $H/K \trianglelefteq G/K$  and  $(G/K)/(H/K) \cong G/H$ .

**Theorem 6.3:** Let  $G$  be a solvable group. If  $H \leq G$ , then

- (1)  $H$  is solvable.
- (2) Let  $N \trianglelefteq G$ . Then  $G/N$  is solvable.

*Proof:* As  $G$  is solvable there is a tower

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = \{1\}$$

with  $G_{i+1} \trianglelefteq G_i$  and  $G_i/G_{i+1}$  abelian.

- (1) Define  $H_i = H \cap G_i$ . Since  $G_{i+1} \trianglelefteq G_i$ , the tower

$$H = H_0 \supseteq G_1 \supseteq \dots \supseteq H_m = \{1\}$$

satisfies  $H_{i+1} \trianglelefteq H_i$ . Note that both  $H_i$  and  $G_{i+1}$  are subgroups of  $G_i$  and

$$H_{i+1} = H \cap G_{i+1} = H_i \cap G_{i+1}.$$

By the second isomorphism theorem:

$$H_i/H_{i+1} = H_i/(H_i \cap G_{i+1}) \cong H_i G_{i+1}/G_{i+1} \leq G_i/G_{i+1}.$$

Since  $G_i/G_{i+1}$  is abelian, so is  $H_i/H_{i+1}$ , hence  $H$  is solvable.

- (2) Consider the towers

$$\begin{aligned} G &= G_0 N \supseteq G_1 N \supseteq \dots \supseteq G_m N = N \\ G/N &= G_0 N/N \supseteq G_1 N/N \supseteq \dots \supseteq G_m N/N = N/N = \{1\}. \end{aligned}$$

Since  $G_{i+1} \trianglelefteq G_i$  and  $N \trianglelefteq G$ , we have  $G_{i+1}N \trianglelefteq G_iN$  which implies  $G_{i+1}N/N \trianglelefteq G_iN/N$ . By the third isomorphism theorem,

$$(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N.$$

Notice that as  $G_{i+1} \subseteq G_i$ ,

$$G_iG_{i+1}N = \{g_1g_2n : g_1 \in G_i, g_2 \in G_{i+1}, n \in N\} = \{g_1n : g_1 \in G_i, n \in N\} = G_iN,$$

so by the second isomorphism theorem,

$$G_i N / G_{i+1} N = G_i G_{i+1} N / G_{i+1} N \cong G_i / (G_i \cap G_{i+1} N).$$

Consider the natural quotient map

$$G_i \rightarrow G_i / (G_i \cap G_{i+1} N)$$

which is surjective, and since  $G_{i+1} \subseteq G_i \cap G_{i+1} N$ , induces a surjective map

$$\varphi : G_i / G_{i+1} \rightarrow G_i / (G_i \cap G_{i+1} N)$$

by the universal property of groups. Since  $G_i / G_{i+1}$  is abelian, so is  $G_i / (G_i \cap G_{i+1} N) = \text{Im } \varphi$ . Therefore

$$(G_i N / N) / (G_{i+1} N / N)$$

is abelian. It follows that  $G/N$  is solvable.  $\square$

*Example:* Since  $S_4$  is solvable, so are  $S_3$  and  $S_2$ .

**Theorem 6.4:** Let  $N \trianglelefteq G$ . If  $N$  and  $G/N$  are both solvable, then  $G$  is solvable. In particular, a direct product of finitely many solvable groups is solvable.

*Proof:* Since  $N$  is solvable, we have a tower

$$N = N_0 \supseteq N_1 \supseteq \dots \supseteq N_m = \{1\}$$

with  $N_{i+1} \trianglelefteq N_i$  and  $N_i / N_{i+1}$  abelian. For a subgroup  $H \leq G$  with  $N \leq H$ , write  $\overline{H} = H/N$ . Since  $G/N$  is solvable, we have a tower

$$G/N = \overline{G} = \overline{G_0} \supseteq \overline{G_1} \supseteq \dots \supseteq \overline{G_r} = N/N = \{1\}$$

with  $\overline{G_{i+1}} \trianglelefteq \overline{G_i}$  and  $\overline{G_i} / \overline{G_{i+1}}$  abelian. Let  $\text{Sub}_N(G) := \{H \leq G : N \leq H\}$  and  $\text{Sub}(G)$  be the set of all subgroups of  $G$ . Consider the map<sup>1</sup>

$$\begin{aligned} \sigma : \text{Sub}_N(G) &\rightarrow \text{Sub}(G/N) \\ H &\mapsto H/N. \end{aligned}$$

For all  $i = 0, \dots, r$ , define  $G_i = \sigma^{-1}(\overline{G_i})$ . Since  $N \trianglelefteq G$  and  $\overline{G_{i+1}} \trianglelefteq \overline{G_i}$ , we have (see Piazza)  $G_{i+1} \trianglelefteq G_i$ . Moreover, by the third isomorphism theorem,

$$G_i / G_{i+1} \cong \overline{G_i} / \overline{G_{i+1}}.$$

It follows that

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_r = N = N_0 \supseteq N_1 \supseteq \dots \supseteq N_m = \{1\}.$$

with  $G_{i+1} \trianglelefteq G$ ,  $N_{i+1} \trianglelefteq N_i$ , and  $G_i / G_{i+1}, N_i / N_{i+1}$  are all abelian. Therefore  $G$  is solvable.  $\square$

**Definition (Simple):** A group  $G$  is **simple** if  $G \neq \{1\}$  and its only normal subgroups are  $\{1\}$  and  $G$ .

*Example:* One can show  $A_5$  is simple, so its only tower is  $A_5 \supseteq \{1\}$ . As  $A_5 / \{1\} = A_5$  is not abelian,  $A_5$  is not solvable, so by [Theorem 6.3](#)  $S_5$  cannot be solvable ( $A_5 \leq S_5$ ). Moreover, since all  $S_n$  for  $n \geq 5$  contains a subgroup isomorphic to  $S_5$ , [Theorem 6.3](#) gives that  $S_n$  is not solvable.

**Corollary 6.5:** Let  $G$  be a finite solvable group. Then there is a tower

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = \{1\}$$

with  $G_{i+1} \trianglelefteq G_i$  and  $G_i / G_{i+1}$  a *cyclic* group.

<sup>1</sup>This map is a bijection: see [https://en.wikipedia.org/wiki/Correspondence\\_theorem](https://en.wikipedia.org/wiki/Correspondence_theorem)

*Proof:* We know in such a tower each  $G_i/G_{i+1}$  is abelian, so by the classification of finite abelian groups for each  $A_i := G_i/G_{i+1}$ ,

$$A_i \cong C_{k_1} \times \dots \times C_{k_r}$$

where  $C_k$  is a cyclic group of order  $k$ , so the result follows.

**TODO: why?**

◇

*Remark:* In the above proof, given a finite cyclic group  $C$  by the Chinese remainder theorem

$$C \cong \mathbb{Z}/\langle p_1^{\alpha_1} \rangle \times \dots \times \mathbb{Z}/\langle p_r^{\alpha_r} \rangle$$

where the  $p_i$  are distinct primes. Also, for a cyclic group whose order is a prime power, say  $\mathbb{Z}/\langle p^\alpha \rangle$ , we have a tower of subgroups

$$\mathbb{Z}/\langle p^\alpha \rangle \supseteq \mathbb{Z}/\langle p^{\alpha-1} \rangle \supseteq \dots \supseteq \mathbb{Z}/\langle p \rangle \supseteq \{1\}$$

so we can further require the quotient  $G_i/G_{i+1}$  in [Corollary 6.5](#) to be a cyclic group of prime order.

## 6.2 Automorphism groups

**Definition** ( $\text{Aut}_F(E)$ ): Let  $E/F$  be a field extension. If  $\psi : E \rightarrow E$  is an automorphism and  $\psi|_F = \text{id}$  we say  $\psi$  is an  $F$ -automorphism of  $E$ . Under composition, the set of  $F$ -automorphisms of  $E$  is a group called the **automorphism group of  $E/F$**  denoted

$$\text{Aut}_F(E) := \{\psi : E \rightarrow E : \psi|_F = \text{id}\}.$$

**Lemma 6.6:** Let  $E/F$  be a field extension,  $f(x) \in F[x]$ , and  $\psi \in \text{Aut}_F(E)$ . If  $\alpha \in E$  is a root of  $f(x)$ , then  $\psi(\alpha)$  is a root of  $f(x)$ .

*Proof:* Write  $f(x) = a_0 + \dots + a_n x^n \in F[x]$  so

$$\begin{aligned} f(\psi(\alpha)) &= a_0 + \dots + a_n \psi(\alpha)^n \\ &= \psi(a_0) + \dots + \psi(a_n) \psi(\alpha)^n \quad (a_i \in F, \psi|_F = \text{id}) \\ &= \psi(a_0 + \dots + a_n \alpha^n) \quad (\psi \text{ is a hom}) \\ &= \psi(f(\alpha)) = \psi(0) = 0. \end{aligned}$$

◇

**Lemma 6.7:** Let  $E = F(\alpha_1, \dots, \alpha_n)$  be a field extension of  $F$ . For  $\psi_1, \psi_2 \in \text{Aut}_F(E)$ , if  $\psi_1(\alpha_i) = \psi_2(\alpha_i)$  for all  $i = 1, \dots, n$  then  $\psi_1 = \psi_2$ .

*Proof:* For  $\alpha \in E$  there exist  $f, g \in F[x_1, \dots, x_n]$  such that

$$\alpha = \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}$$

and by the same manipulation as in the proof of [Lemma 6.6](#),

$$\begin{aligned} \psi_1(\alpha) &= \psi_1\left(\frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}\right) \\ &= \frac{f(\psi_1(\alpha_1), \dots, \psi_1(\alpha_n))}{g(\psi_1(\alpha_1), \dots, \psi_1(\alpha_n))} \\ &= \frac{f(\psi_2(\alpha_1), \dots, \psi_2(\alpha_n))}{g(\psi_2(\alpha_1), \dots, \psi_2(\alpha_n))} \\ &= \psi_2(\alpha) \end{aligned}$$

so  $\psi_1 = \psi_2$ .

◇

**Corollary 6.8:** If  $E/F$  is a finite extension then  $\text{Aut}_F(E)$  is a finite group.

*Proof:* Since  $E/F$  is finite by [Theorem 3.5](#) there are  $\alpha_1, \dots, \alpha_n \in E$  so  $E = F(\alpha_1, \dots, \alpha_n)$  with each  $\alpha_i$  algebraic over  $F$ . For  $\psi \in \text{Aut}_F(E)$  by [Lemma 6.6](#) we have  $\psi(\alpha_i)$  is a root of the minimal polynomial of  $\alpha_i$  over  $F$ . Thus there are only finitely many choices for the value of  $\psi(\alpha_i)$ . By [Lemma 6.7](#)  $\psi$  is completely determined by its values at each  $\alpha_i$ , so there are only finitely many  $\psi$ , hence  $\text{Aut}_F(E)$  is finite.  $\square$

*Example:* The converse of [Corollary 6.8](#) is false, for example  $\mathbb{R}/\mathbb{Q}$  is an infinite extension but  $\text{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{\text{id}\}$  and in fact  $\text{Aut}(\mathbb{R}) = \{\text{id}\}$ .

### 6.3 Automorphism groups of splitting fields

**Definition** ( $\text{Aut}$  group of  $f(x)$ ): Let  $F$  be a field,  $f(x) \in F[x]$ . The **automorphism group of  $f(x)$  over  $F$**  is defined to be  $\text{Aut}_F(E)$  where  $E$  is the splitting field of  $f(x)$  over  $F$ .

Recall by the proof of [Theorem 4.4](#) we can show the number of such extensions in its statement is at most  $[E : F]$ , and one can show equality holds iff every irreducible factor of  $f(x)$  is separable over  $F$ .

*Exercise 6.1:* Prove the above statement. 

**Theorem 6.9:** Let  $E/F$  be the splitting field of  $0 \neq f(x) \in F[x]$ . Then  $|\text{Aut}_F(E)| \leq [E : F]$  with equality iff every irreducible factor of  $f(x)$  is separable.

*Proof:* In the proof of the previous exercise we count the number of extensions as those extending maps  $F(\alpha) \rightarrow F_1(\alpha_1)$  mapping a root of an irreducible factor to a corresponding root, where each resulting extension  $\psi$  is an element of  $\text{Aut}_F(E)$ , and the set of all such extensions accounts for all of  $\text{Aut}_F(E)$  (the  $F$ -automorphisms permuting the roots in valid ways) so the result follows.  $\square$

**Theorem 6.10:** If  $f(x) \in F[x]$  has  $n$  distinct roots in its splitting field  $E$ , then  $\text{Aut}_F(E)$  is isomorphic to a subgroup of  $S_n$ . In particular,  $|\text{Aut}_F(E)| \mid n!$ .

*Proof:* Let  $X := \{\alpha_1, \dots, \alpha_n\}$  be the distinct roots of  $f(x)$  in  $E$ . By [Lemma 6.6](#) if  $\psi \in \text{Aut}_F(E)$  then  $\psi(X) = X$ . Let  $\psi|_X$  be the restriction of  $\psi$  to  $X$ , so that

$$\begin{aligned} f : \text{Aut}_F(E) &\rightarrow \text{Sym}(X) \cong S_n \\ \psi &\mapsto \psi|_X \end{aligned}$$

is a group homomorphism. Moreover by [Lemma 6.7](#),  $f$  is injective so  $\text{Aut}_F(E) \cong \text{Im}(f) \leq S_n$ .  $\square$

*Example:* Consider  $f(x) = x^3 - 2 \in \mathbb{Q}[x]$  and let  $E/\mathbb{Q}$  be the splitting field of  $f(x)$  over  $\mathbb{Q}$ . Then

$$E := \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \text{ and } [E : \mathbb{Q}] = 6.$$

Since  $\text{ch}(\mathbb{Q}) = 0$  and  $f(x)$  is irreducible,  $f(x)$  is separable. By [Theorem 6.9](#) we know

$$|\text{Aut}_{\mathbb{Q}}(E)| = [E : F] = 6$$

and by [Theorem 6.10](#) since  $f$  has 3 distinct roots in  $E$  we know  $\text{Aut}_{\mathbb{Q}}(E)$  is a subgroup of  $S_3$ , which forces  $\text{Aut}_{\mathbb{Q}}(E) \cong S_3$ .

*Example:* Let  $F$  be a field with  $\text{ch}(F) = p$  and  $f(x) = x^p - a$  where  $a \in F^p \neq F$ . Then  $f(x)$  is irreducible over  $F$  and if  $\beta$  is a root of  $f(x)$  we have  $f(x) = (x - \beta)^p$  with  $\beta \notin F$ . Then the splitting field of  $f(x)$  over  $F$  is  $E = F(\beta)$  and  $\text{Aut}_F(E) = \{\text{id}\}$  since the only choice is  $\beta \mapsto \beta$ . In this case we have

$$1 = |\text{Aut}_F(E)| \neq [E : F] = \deg f = p$$

which is fine, since  $f$  is not separable (in fact it is completely inseparable).

**Definition** (Fixed field): Let  $E/F$  be a field extension and  $\psi \in \text{Aut}_F(E)$ . Define

$$E^\psi := \{a \in E : \psi(a) = a\}$$

which is a subfield of  $E$  containing  $F$ , called the **fixed field of  $\psi$** . If  $G \leq \text{Aut}_F(E)$ , the **fixed field of  $G$**  is defined as

$$E^G := \bigcap_{\psi \in G} E^\psi = \{a \in E : \psi(a) = a, \forall \psi \in G\}.$$

**Theorem 6.11:** Let  $f(x) \in F[x]$  be a polynomial whose irreducible factors are separable. Let  $E/F$  be the splitting field of  $f(x)$ . Then  $E^G = F$  where  $G := \text{Aut}_F(E)$ .

*Proof:* Write  $L := E^G$ . Since  $F \subseteq L$ , if  $\psi$  fixes  $L$  then it fixes  $F$ , so  $\text{Aut}_L(E) \leq \text{Aut}_F(E)$ . On the other hand if  $\psi \in \text{Aut}_F(E)$  then by definition of  $E^G$ , for all  $a \in L$ ,  $\psi(a) = a$  gives  $\psi \in \text{Aut}_L(E)$ , so  $\text{Aut}_F(E) = \text{Aut}_L(E)$ . Note that since all the irreducible factors of  $f(x)$  are separable over  $F$  and  $f(x)$  splits over  $E$ ,  $f(x)$  is also separable over  $L$  and has  $E$  as its splitting field over  $L$ . Thus by [Theorem 6.9](#) we have

$$[E : F] = |\text{Aut}_F(E)| = |\text{Aut}_L(E)| = [E : L]$$

where  $[E : F] = [E : L][L : F]$  gives  $[L : F] = 1$ , and so  $L = E^G = F$ .  $\square$

## 7 Separable and Normal Extensions

### 7.1 Separable extensions

**Definition** (Separable extension): Let  $E/F$  be an algebraic extension. For  $\alpha \in E$ , let  $p(x) \in F[x]$  be its minimal polynomial. We say  $\alpha$  is **separable** over  $F$  if  $p(x)$  is separable. If this holds for all  $\alpha \in E$ , we say  $E/F$  is a **separable extension**.

*Example:* If  $\text{ch}(F) = 0$ , by [Corollary 5.5](#) every irreducible  $p(x) \in F[x]$  is separable, so any algebraic extension  $E/F$  is separable.

**Theorem 7.1:** Let  $E/F$  be the splitting field of  $f(x) \in F[x]$ . If every irreducible factor of  $f(x)$  is separable, then  $E/F$  is separable.

*Proof:* Let  $\alpha \in E$  and  $p(x) \in F[x]$  be its minimal polynomial. Let  $\alpha = \alpha_1, \dots, \alpha_n$  be the distinct roots of  $p(x)$  in  $E$ . Define

$$\tilde{p}(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

We claim  $\tilde{p}(x) \in F[x]$ . Let  $\psi \in \text{Aut}_F(E)$ . Since  $\psi$  is an automorphism,  $\psi(\alpha_i) \neq \psi(\alpha_j)$  if  $i \neq j$ , so by [Lemma 6.6](#)  $\psi$  permutes  $\{\alpha_1, \dots, \alpha_n\}$ . Therefore by extending  $\psi$  uniquely to  $E[x]$  with  $x \mapsto x$  we have

$$\begin{aligned} \psi(\tilde{p}(x)) &= (x - \psi(\alpha_1)) \cdots (x - \psi(\alpha_n)) \\ &= (x - \alpha_1) \cdots (x - \alpha_n) = \tilde{p}(x). \end{aligned}$$

It follows that  $\tilde{p}(x) \in E^\psi[x]$ , but  $\psi$  was arbitrary, so  $\tilde{p}(x) \in E^{\text{Aut}_F(E)}[x]$ . Since  $E/F$  is the splitting field of  $f(x)$  whose irreducible factors are separable, by [Theorem 6.11](#) we have  $\tilde{p}(x) \in F[x]$ .

Now  $\tilde{p}(x) \in F[x]$  and  $\tilde{p}(\alpha) = 0$ , so  $p \mid \tilde{p}$  since  $p(x)$  is the min poly of  $\alpha$ . By construction  $\tilde{p} \mid p$ , so  $p(x) = \tilde{p}(x)$  since they are both monic. It follows that  $p(x)$  is separable, hence  $E/F$  is separable.  $\square$

**Corollary 7.2:** Let  $E/F$  be a finite extension so  $E = F(\alpha_1, \dots, \alpha_n)$ . If each  $\alpha_i$  is separable over  $F$ , then so is  $E/F$ .

*Proof:* Let  $p_i(x)$  be the minimal polynomial of each  $\alpha_i$  ( $1 \leq i \leq n$ ). Define  $f(x) = p_1(x) \cdots p_n(x)$ , where each  $p_i(x)$  is separable. Let  $L$  be the splitting field of  $f(x)$  over  $F$ . By [Theorem 7.1](#)  $L/F$  is separable as every irreducible factor of  $f(x)$  is separable. Since  $E = F(\alpha_1, \dots, \alpha_n)$  is a subfield of  $L$ , we have that  $E$  is separable.  $\square$

**Corollary 7.3:** Let  $E/F$  be an algebraic extension and  $L \subseteq E$  be all the  $\alpha \in E$  with  $\alpha$  separable over  $F$ . Then  $L$  is a field.

*Proof:* Let  $\alpha, \beta \in L$ . Then  $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$  ( $\beta \neq 0$ )  $\in F(\alpha, \beta)$ . By [Corollary 7.2](#),  $F(\alpha, \beta)$  is separable, so  $F(\alpha, \beta) \subseteq L$ . Thus  $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$  ( $\beta \neq 0$ )  $\in L$ .  $\square$

**Definition** (Primitive element): If  $E = F(\gamma)$  is a simple extension, we say  $\gamma$  is a **primitive element** of  $E/F$ .

**Theorem 7.4** (Primitive element theorem): If  $E/F$  is a finite, separable extension, then  $E = F(\gamma)$  for some  $\gamma \in E$ . In particular, if  $\text{ch}(F) = 0$ , then any finite extension  $E/F$  is a simple extension.

*Example:* We have that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[3]{5}, i, \sqrt{3+i}) = \mathbb{Q}(\beta)$  for some  $\beta$ .

*Proof:* We have seen in [Corollary 5.9](#) that a finite extension of a finite field is always simple, so wlog let  $F$  be an infinite field. Since  $E = F(\alpha_1, \dots, \alpha_n)$  with each  $\alpha_i \in E$  it suffices to consider the case when  $E = F(\alpha, \beta)$  and the general case follows by induction.

Let  $E = F(\alpha, \beta)$  for  $\alpha, \beta \notin F$ . We claim there exists  $\lambda \in F$  such that  $\gamma = \alpha + \lambda\beta$  with  $\beta \in F(\gamma)$ . With this claim, we have

$$\begin{aligned}\alpha = \gamma - \lambda\beta \in F(\gamma) &\implies F(\alpha, \beta) \subseteq F(\gamma) \\ \gamma = \alpha + \lambda\beta \in F(\alpha, \beta) &\implies F(\gamma) \subseteq F(\alpha, \beta).\end{aligned}$$

Thus  $E = F(\alpha, \beta) = F(\gamma)$ .

*Proof of claim:* Let  $a(x), b(x)$  be the minimal polynomials of  $\alpha, \beta$  over  $F$ . Since  $\beta \notin F$ ,  $\deg(b) > 1$  so there is a root  $\tilde{\beta}$  of  $b(x)$  such that  $\tilde{\beta} \neq \beta$ . Choose  $\lambda \in F$  such that

$$\lambda \neq \frac{\tilde{\alpha} - \alpha}{\tilde{\beta} - \beta}$$

for all roots  $\tilde{\alpha}, \tilde{\beta}$  of  $a(x), b(x)$  with  $\tilde{\beta} \neq \beta$  in some splitting field of  $a(x), b(x)$  over  $F$ . This is possible as there are finitely many choices of  $\tilde{\alpha}, \tilde{\beta}$ , but  $F$  is infinite. Define  $\gamma := \alpha + \lambda\beta$ . Consider  $h(x) := a(\gamma - \lambda x) \in F(\gamma)[x]$ . Then

$$h(\beta) = a(\gamma - \lambda x) = a(\alpha) = 0.$$

However, for  $\tilde{\beta} \neq \beta$ , since  $\gamma - \lambda\tilde{\beta} = \alpha + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha}$  by the choice of  $\lambda$ , we have

$$h(\tilde{\beta}) = a(\gamma - \lambda\tilde{\beta}) \neq 0.$$

Thus  $h(x)$  and  $b(x)$  have  $\beta$  as their only common root in any extension of  $F(\gamma)$ . Let  $b_1(x)$  be the minimal polynomial of  $\beta$  over  $F(\gamma)$ . Then  $b_1(x) \mid h(x), b(x)$ . Since  $E/F$  is separable and  $b(x) \in F[x]$  is irreducible,  $b(x)$  has distinct roots and so does  $b_1(x)$ . The roots of  $b_1(x)$  are common to  $h(x)$  and  $b(x)$ , but  $\beta$  being the only common root forces  $b_1(x) = x - \beta$ . Since  $b_1(x) \in F(\gamma)[x]$  we get  $\beta \in F(\gamma)$  and this completes the proof.  $\diamond$

## 7.2 Normal extensions

**Definition** (Normal extension): Let  $E/F$  be an algebraic extension. We say  $E/F$  is a **normal extension** if for any irreducible  $p(x) \in F[x]$ , either  $p(x)$  has no roots or all roots in  $E$ . Equivalently, if  $p(x)$  has a root in  $E$  then  $p(x)$  splits over  $E$ .

**Theorem 7.5:** A finite extension  $E/F$  is normal iff it is the splitting field of some  $f(x) \in F[x]$ .

*Proof:* ( $\implies$ ) Suppose  $E/F$  is normal. Write  $E = F(\alpha_1, \dots, \alpha_n)$  and let  $p_i(x) \in F[x]$  be the minimal polynomial of  $\alpha_i$  ( $1 \leq i \leq n$ ) and  $f(x) = p_1(x) \cdots p_n(x)$ . Since  $E/F$  is normal, each  $p_i(x)$  splits over  $E$ . Let

$$\alpha_i = \alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,r_i} \quad (1 \leq i \leq n)$$

be the roots of  $p_i(x)$  in  $E$ . Then

$$\begin{aligned}E &= F(\alpha_1, \dots, \alpha_n) \\ &= F(\alpha_{1,1}, \dots, \alpha_{1,r_1}, \dots, \alpha_{n,1}, \dots, \alpha_{n,r_n})\end{aligned}$$

which is the splitting field of  $f(x)$  over  $F$ .

( $\impliedby$ ) Suppose  $E/F$  is the splitting field of  $f(x) \in F[x]$ . Let  $p(x) \in F[x]$  be irreducible with a root  $a \in E$ . Let  $K/E$  be the splitting field of  $p(x)$  over  $E$ , say

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where  $\alpha = \alpha_1 \in E$  and  $\alpha_2, \dots, \alpha_n \in K = E(\alpha_1, \alpha_2, \dots, \alpha_n)$ . Since

$$F(\alpha) \cong F[x]/\langle p(x) \rangle \cong F(\alpha_2)$$

we have an  $F$ -isomorphism  $\theta : F(\alpha) \rightarrow F(\alpha_2)$ ,  $\alpha \mapsto \alpha_2$ . Note  $f(x)p(x) \in F[x] \subseteq F(\alpha)[x], F(\alpha_2)[x]$ , so we can view  $K$  as the splitting field of  $f(x)p(x)$  over both  $F(\alpha)$  and  $F(\alpha_2)$ . Then by [Theorem 4.4](#) there is an isomorphism  $\psi : K \rightarrow K$  extending  $\theta$ . In particular,  $\psi \in \text{Aut}_F(K)$ , so  $\psi$  permutes the roots

of  $f(x)$ . Since  $E$  is generated over  $F$  by these roots, by [Lemma 6.6](#) we have  $\psi(E) = E$ . It follows that  $\alpha_2 = \psi(\alpha) \in E$  since  $\alpha \in E$ . Similarly, we can prove  $\alpha_i \in E$  ( $3 \leq i \leq n$ ). Thus  $K = E$  and  $p(x)$  splits over  $E$ , so  $E/F$  is normal.  $\square$

**Example:** We claim every quadratic extension is normal. Let  $E/F$  be a field extension with  $[E : F] = 2$ . For  $\alpha \in E \setminus F$ , we have  $E = F(\alpha)$ . Let  $p(x) = x^2 + ax + b$  be the minimal polynomial of  $\alpha$  over  $F$ . If  $\beta$  is another root of  $p(x)$ , then  $p(x) = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$  so  $\beta = -a - \alpha = \frac{b}{\alpha} \in E$ . Hence  $E/F$  is normal.

**Example:** Consider  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ . This is not a normal extension since  $x^4 - 2$  is irreducible but has non-real roots. Notice something strange: the extension  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$  is made up of two quadratic extensions:

$$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}) \text{ and } \mathbb{Q}(\sqrt{2})/\mathbb{Q}$$

which are both normal, but their “composition” is not.

The previous example shows if  $K/F$  and  $E/K$  are normal, then  $E/F$  is not necessarily normal. However, a sort of converse statement does hold.

**Proposition 7.6:** If  $E/F$  is a normal extension and  $K$  is an intermediate field, then  $E/K$  is normal.

*Proof:* Let  $p(x) \in K[x]$  be irreducible with a root  $\alpha \in E$ . Let  $f(x) \in F[x] \subseteq K[x]$  be the minimal polynomial of  $\alpha$  over  $F$ . Then  $p(x) \mid f(x)$ , and since  $E/F$  is normal  $f(x)$  splits over  $E$ , hence so does  $p(x)$ , thus  $E/K$  is normal.  $\square$

*Remark:* Note that  $K/F$  in [Proposition 7.6](#) may not be normal. Consider  $F := \mathbb{Q}, K := \mathbb{Q}(\sqrt[4]{2}), E := \mathbb{Q}(\sqrt[4]{2}, i)$ . Then  $E/F$  is the splitting field of  $x^4 - 2$  hence normal, and  $E/K$  is normal, but  $K/F$  is not normal.

**Proposition 7.7:** Let  $E/F$  be a finite normal extension and  $\alpha, \beta \in E$ . TFAE:

- (1) There exists  $\psi \in \text{Aut}_F(E)$  with  $\psi(\alpha) = \beta$ .
- (2)  $\alpha$  and  $\beta$  have the same minimal polynomial over  $F$ .

In this case we say  $\alpha$  and  $\beta$  are **conjugate over  $F$** .

*Proof:*

(1  $\implies$  2) Let  $p(x)$  be the minimal polynomial of  $\alpha$  over  $F$  and  $\psi \in \text{Aut}_F(E)$  with  $\psi(\alpha) = \beta$ . By [Lemma 6.6](#)  $\beta$  is also a root of  $p(x)$ , but  $p(x)$  is monic and irreducible over  $F$ , so it must be the minimal polynomial of  $\beta$  over  $F$ .

(2  $\implies$  1) Suppose  $\alpha, \beta$  have the same minimal polynomial  $p(x)$  over  $F$ . Since

$$F(\alpha) \cong F[x]/\langle p(x) \rangle \cong F(\beta)$$

we have an  $F$ -isomorphism  $\theta : F(\alpha) \rightarrow F(\beta), \alpha \mapsto \beta$ . Since  $E/F$  is a finite normal extension, by [Theorem 7.5](#)  $E$  is the splitting field of some  $f(x)$  over  $F$ . We can also view  $E$  as the splitting field of  $f(x)$  over  $F(\alpha)$  and  $F(\beta)$ , so by [Theorem 4.4](#) there is an isomorphism  $\psi : E \rightarrow E$  extending  $\theta$ , giving  $\psi \in \text{Aut}_F(E)$  with  $\psi(\alpha) = \beta$ , so we are done.  $\square$

We have seen not every field extension is normal, but we would like to work with these, which motivates the following definition.

**Definition** (Normal closure): A **normal closure** of a finite extension  $E/F$  is a finite normal extension  $N/F$  satisfying

- $E$  is a subfield of  $N$
- For any intermediate field  $L$  of  $N/E$ , if  $L$  is normal over  $F$ , then  $L = N$

That is,  $N$  is the smallest field containing  $E$  such that  $N/F$  is normal.

*Example:* The normal closure of  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  is  $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ .

**Theorem 7.8:** Every finite extension  $E/F$  has a normal closure  $N/F$  that is unique up to  $E$ -isomorphism

*Proof:* Write  $E = F(\alpha_1, \dots, \alpha_n)$  and let  $p_i(x)$  be the minimal polynomial of each  $\alpha_i$  over  $F$ . Write  $f(x) := p_1(x) \cdots p_n(x)$  and let  $N/E$  be the splitting field of  $f(x)$  over  $E$ . Since  $\alpha_1, \dots, \alpha_n$  are roots of  $f(x)$ ,  $N$  is also the splitting field of  $f(x)$  over  $F$ , so by [Theorem 7.5](#)  $N/F$  is normal.

Let  $L \subseteq N$  be a subfield containing  $E$ . Then  $L$  contains all the  $\alpha_i$  and if  $L$  is normal over  $F$ , each  $p_i(x)$  then splits over  $L$ , so  $f(x)$  splits over  $L$ , giving  $N \subseteq L \implies L = N$ .

For uniqueness, let  $N/E$  be the splitting field of  $f(x)$  over  $E$  as above. Let  $N_1/F$  be another normal closure of  $E/F$ . Since  $N_1$  is normal over  $F$  and contains each  $\alpha_i$ ,  $f(x)$  splits over  $N_1$ , so  $N_1$  contains a splitting field  $\tilde{N}$  of  $f(x)$  over  $F$ , thus over  $E$ . By [Corollary 4.5](#)  $N$  and  $\tilde{N}$  are  $E$ -isomorphic. Since  $\tilde{N}$  is a splitting field of  $f(x)$  over  $F$ , by [Theorem 7.5](#),  $\tilde{N}$  is normal over  $F$ , so  $N_1 \subseteq \tilde{N} \implies \tilde{N} = N_1 \cong N$ .  $\square$

## 8 Galois Correspondence

### 8.1 Galois extensions

Recall for a finite extension  $E/F$  we have shown

- [Theorem 7.5](#):  $E$  is the splitting field of some  $f(x) \in F[x]$  iff  $E$  is normal
- [Theorem 7.1](#): If  $E$  is the splitting field of some  $f(x) \in F[x]$  whose irreducible factors are separable then  $E/F$  is separable.

**Definition** (Galois group): An algebraic extension  $E/F$  is **Galois** if it is normal and separable. If  $E/F$  is a Galois extension, we define the **Galois group of  $E/F$**  as  $\text{Gal}_F(E) := \text{Aut}_F(E)$ .

*Remark:*

- (1) By [Theorem 7.1](#) and [Theorem 7.5](#), a finite Galois extension  $E/F$  is the splitting field of some  $f(x) \in F[x]$  whose irreducible factors are separable.
- (2) If  $E/F$  is a finite Galois extension, by [Theorem 6.9](#)  $|\text{Gal}_F(E)| = [E : F]$ .
- (3) If  $E/F$  is the splitting field of a separable polynomial  $f(x) \in F[x]$  with degree  $n$ , by [Theorem 6.10](#)  $\text{Gal}_F(E)$  is a subgroup of  $S_n$ .

**Example:** Let  $E$  be the splitting field of  $(x^2 - 2)(x^2 - 3)(x^2 - 5)$  over  $\mathbb{Q}$ . Then  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  and  $[E : F] = 8$ .

**Exercise 8.1:** Prove the above. ▶

For  $\psi \in \text{Gal}_{\mathbb{Q}}(E)$ , we have

$$\begin{aligned}\psi(\sqrt{2}) &= \pm\sqrt{2} \\ \psi(\sqrt{3}) &= \pm\sqrt{3} \\ \psi(\sqrt{5}) &= \pm\sqrt{5}.\end{aligned}$$

Since  $|\text{Gal}_{\mathbb{Q}}(E)| = [E : F] = 8$ , we have  $\text{Gal}_{\mathbb{Q}}(E) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ .

**Theorem 8.1** (E. Artin): Let  $E$  be a field,  $G$  a finite subgroup of  $\text{Aut}(E)$ . Then  $E/E^G$  is a finite Galois extension and  $\text{Gal}_{E^G}(E) = G$ . In particular,  $[E : E^G] = |G|$ .

*Proof:* Let  $n = |G|$  and  $F := E^G$ . For  $\alpha \in E$ , consider the  $G$ -orbit of  $\alpha$ , i.e.

$$\{\psi(\alpha) : \psi \in G\} = \{\alpha = \alpha_1, \alpha_2, \dots, \alpha_n\}$$

where the  $\alpha_i$  are distinct and  $m \leq n$ . Consider  $f(x) = (x - \alpha_1)\cdots(x - \alpha_m)$ . For any  $\psi \in G$ ,  $\psi$  permutes the roots of  $f(x)$ . Since the coefficients of  $f(x)$  are symmetric w.r.t each  $\alpha_i$ ,  $f(x) \in E^G[x] = F[x]$ . To show  $f(x)$  is the minimal polynomial of  $\alpha$  over  $F$ , consider a factor  $g(x) \in F[x]$  of  $f(x)$ . Wlog, we can write

$$g(x) = (x - \alpha_1)\cdots(x - \alpha_\ell).$$

If  $\ell < m$ , since each  $\alpha_i$  are in the  $G$ -orbit of  $\alpha$ , there is  $\psi \in G$  such that

$$\{\alpha_1, \dots, \alpha_\ell\} \neq \{\psi(\alpha_1), \dots, \psi(\alpha_\ell)\}.$$

It follows that

$$\psi(g(x)) = (x - \psi(\alpha_1))\cdots(x - \psi(\alpha_\ell)) \neq g(x)$$

so  $g(x) \notin F[x]$ . Therefore  $\ell = m$ , so  $g(x) = f(x)$  and so  $f(x)$  is the minimal polynomial of  $\alpha$  over  $F$ . Since  $f(x)$  is separable and splits over  $E$ ,  $E/F$  is separable, hence a Galois extension.

**Claim:**  $[E : F] \leq n$ .

Assume the claim is true. We have shown  $E/F$  is a finite Galois extension, so  $E$  is the splitting field of some polynomial whose irreducible factors are separable over  $F$ . Since

$$F = E^G = \{\alpha \in E : \psi(\alpha) = \alpha \forall \psi \in G\},$$

$G$  is a subgroup of  $\text{Gal}_F(E)$ . By [Theorem 6.9](#) we have

$$n = |G| \leq |\text{Gal}_F(E)| = [E : F] \leq n.$$

Therefore  $\text{Gal}_F(E) = G$  and  $[E : F] = n$ .

*Proof of claim:* Suppose bwoc  $[E : F] > n = |G|$ . We can choose  $\beta_1, \dots, \beta_{n+1} \in E$  that are linearly independent over  $F$ . Consider the system

$$\psi(\beta_1)v_1 + \dots + \psi(\beta_{n+1})v_{n+1} = 0 \quad \forall \psi \in G$$

of  $n$  linear equations in  $n+1$  variables  $v_i$ . This must have a non-zero solution in  $E$ , so let

$$\gamma := (\gamma_1, \dots, \gamma_{n+1})$$

be such a solution with the *minimum* number of non-zero entries, say  $r$ . Notice  $r \geq 2$  as if there is only one such entry, the sum cannot be 0. Wlog, we can assume  $\gamma_1 = \dots = \gamma_r \neq 0$  and  $\gamma_{r+1} = \dots = \gamma_{n+1} = 0$ . Therefore

$$\psi(\beta_1)\gamma_1 + \dots + \psi(\beta_r)\gamma_r = 0 \quad \forall \psi \in G \quad (1)$$

and by dividing the solution by  $\gamma_r$ , we can assume  $\gamma_r = 1$ . Also, since  $\beta_1, \dots, \beta_r$  are linearly independent over  $F$  and  $\beta_1\gamma_1 + \dots + \beta_r\gamma_r = 0$  (take  $\psi = \text{id}$  in (1)) there is at least one  $\gamma_i \notin F$  (if each  $\gamma_i \in F$ , they must all be 0). Since  $r \geq 2$ , wlog we can assume  $\gamma_1 \notin F$ . Choose  $\varphi \in G$  with  $\varphi(\gamma_1) \neq \gamma_1$ . Applying  $\varphi$  to (1) we get

$$(\varphi \circ \psi)(\beta_1)\varphi(\gamma_1) + \dots + (\varphi \circ \psi)(\beta_r)\varphi(\gamma_r) = 0 \quad \forall \psi \in G.$$

Notice since  $\psi$  runs through all of  $G$ , so does  $\varphi \circ \psi$  (the left action is a permutation), so we can rewrite the above as

$$\psi(\beta_1)\varphi(\gamma_1) + \dots + \psi(\beta_r)\varphi(\gamma_r) \quad \forall \psi \in G. \quad (2)$$

Subtracting (2) from (1),

$$\psi(\beta_1)(\gamma_1 - \varphi(\gamma_1)) + \dots + \psi(\beta_r)(\gamma_r - \varphi(\gamma_r)) = 0 \quad \forall \psi \in G.$$

Since  $\gamma_r = 1$  we have  $\gamma_r - \varphi(\gamma_r) = 0$ , and since  $\gamma_1 \notin F$  we have  $\gamma_1 - \varphi(\gamma_1) \neq 0$ . Therefore

$$(\gamma_1 - \varphi(\gamma_1), \dots, \gamma_{r-1} - \varphi(\gamma_{r-1}), 0, \dots, 0)$$

is a solution of the system with fewer non-zero entries than  $\gamma$ , a contradiction of our choice.  $\diamond$

*Remark:* Let  $E$  be a field and  $G$  finite subgroup of  $\text{Aut}(E)$ . For  $\alpha \in E$ , let  $\{\alpha = \alpha_1, \dots, \alpha_n\}$  be the  $G$ -orbit of  $\alpha$  in the set of all conjugates of  $\alpha$ . Then we see in the proof of [Theorem 8.1](#) that the minimal polynomial of  $\alpha$  over  $E^G$  is

$$(x - \alpha_1) \cdots (x - \alpha_n) \in E^G[x].$$

**Definition** (Symmetric functions): Let  $t_1, \dots, t_n$  be variables. We define the **elementary symmetric functions** in  $t_1, \dots, t_n$  as

$$\begin{aligned} s_1 &= t_1 + \dots + t_n \\ s_2 &= \sum_{1 \leq i < j \leq n} t_i t_j \\ &\vdots \\ s_n &= t_1 \cdots t_n. \end{aligned}$$

This gives  $f(x) = (x - t_1)\cdots(x - t_n) = x^n - s_1x^{n-1} + s_2x^{n-1} + \dots + (-1)^ns_n$ .

*Example:* Let  $E = F(t_1, \dots, t_n)$  be the function field in  $n$  variables  $t_1, \dots, t_n$  over a field  $F$ . Consider the symmetric group  $G := S_n$  as the subgroup of  $\text{Aut}(E)$  which permutes the variables  $t_1, \dots, t_n$  and fixes  $F$ . We are interested in finding  $E^G$ .

From the proof of [Theorem 8.1](#), the coefficients of the minimal polynomial of  $t_1$  lie in  $E^G$ . The  $G$ -orbit of  $t_1$  is  $\{t_1, \dots, t_n\}$ . By the above remark, we see

$$\begin{aligned} f(x) &= (x - t_1)\cdots(x - t_n) \\ &= x^n - s_1x^{n-1} + s_2x^{n-1} + \dots + (-1)^ns_n \in L[x] \end{aligned}$$

is the minimal polynomial of  $t_1$  over  $E^G$ , where  $L := F(s_1, \dots, s_n)$ . Notice that  $L \subseteq E^G$ .

**Claim:**  $L = E^G$ .

*Proof:* Notice  $E$  is the splitting field of  $f(x)$  over  $L$ . Since  $\deg(f) = n$ , by [Theorem 4.6](#)

$$[E : L] \leq n!.$$

On the other hand, by [Theorem 8.1](#)

$$[E : E^G] = |G| = |S_n| = n!.$$

Since  $L \subseteq E^G$ ,  $n! = [E : E^G] \leq [E : L] \leq n!$  and so  $L = E^G$ .  $\square$

## 8.2 The fundamental theorem

Notation: Let  $\text{Int}(E/F)$  denote the set of intermediate fields of  $E/F$  and  $\text{Sub}(G)$  the set of all subgroups of  $G$ .

**Theorem 8.2** (The fundamental theorem of Galois theory): Let  $E/F$  be a finite Galois extension and  $G = \text{Gal}_F(E)$ . Then the maps

$$\begin{aligned} \text{Int}(E/F) &\rightarrow \text{Sub}(G) & L &\mapsto L^* := \text{Gal}_L(E) \\ \text{Sub}(G) &\rightarrow \text{Int}(E/F) & H &\mapsto H^* := E^H \end{aligned}$$

are inverses of each other and reverse the inclusion relation. In particular, for  $L_1, L_2 \in \text{Int}(E/F)$  with  $L_2 \subseteq L_1$  and  $H_1, H_2 \in \text{Sub}(G)$  with  $H_2 \subseteq H_1$ , we have

$$[L_1 : L_2] = [L_2^* : L_1^*] \quad \text{and} \quad [H_1 : H_2] = [H_2^* : H_1^*].$$

We have the following diagram:

$$\begin{array}{ccc} E & \longrightarrow & \{1\} = \text{Gal}_E(E) \\ \uparrow & & \downarrow \\ L_1 & & L_1^* = \text{Gal}_{L_1}(E) \\ \uparrow & & \downarrow \\ L_2 & & L_2^* = \text{Gal}_{L_2}(E) \\ \uparrow & & \downarrow \\ F & & G = \text{Gal}_F(E) \end{array}$$

*Proof:* Let  $L \in \text{Int}(E/F)$  and  $H \in \text{Sub}(G)$ . Recall [Theorem 6.11](#): if  $G_1 = \text{Gal}_{F_1}(E_1)$  then  $E_1^{G_1} = F_1$ , therefore

$$(L^*)^* = (\text{Gal}_L(E))^* = E^{\text{Gal}_L(E)} = L.$$

Similarly by [Theorem 8.1](#) if  $G_1 \subseteq \text{Aut}(E_1)$  then  $\text{Gal}_{E_1^{G_1}}(E_1) = G_1$ , so

$$(H^*)^* = (E^H)^* = \text{Aut}_{E^H}(E) = H.$$

Therefore the maps are bijections and inverses of each other.

Let  $L_1, L_2 \in \text{Int}(E/F)$ . Since  $E/F$  is the splitting field of some polynomial  $f(x) \in F[x]$  whose irreducible factors are separable,  $E/L_1$  and  $E/L_2$  are also Galois extensions since  $E$  is also the splitting field of  $f(x)$  over  $L_1$  and  $L_2$ .

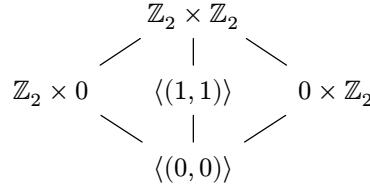
We have  $L_2 \subseteq L_1 \implies \text{Gal}_{L_1}(E) \subseteq \text{Gal}_{L_2}(E)$  as if an automorphism fixes  $L_1$  then it will fix  $L_2$ , so  $L_2 \subseteq L_1 \implies L_1^* \subseteq L_2^*$ . Also,

$$[L_1 : L_2] = \frac{[E : L_2]}{[E : L_1]} = \frac{|\text{Gal}_{L_2}(E)|}{|\text{Gal}_{L_1}(E)|} = \frac{|L_2^*|}{|L_1^*|} = [L_2^* : L_1^*].$$

For  $H_1 \in H_2 \in \text{Sub}(G)$ , note  $H_2 \subseteq H_1 \implies E^{H_1} \subseteq E^{H_2} \implies H_1^* \subseteq H_2^*$ . Also,

$$[H_1 : H_2] = \frac{|H_1|}{|H_2|} = \frac{|\text{Gal}_{E^{H_1}}(E)|}{|\text{Gal}_{E^{H_2}}(E)|} = \frac{[E : E^{H_1}]}{[E : E^{H_2}]} = [E^{H_2} : E^{H_1}] = [H_2^* : H_1^*]. \quad \diamond$$

*Remark:* Consider  $E/\mathbb{Q}$  where  $E := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Recall  $|\text{Gal}_{\mathbb{Q}}(E)| = 4$  so the Galois group is either  $\mathbb{Z}_4$  or  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , but the automorphisms are of order 2, so  $\text{Gal}_{\mathbb{Q}}(E) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . Consider the subgroups:



Since there are finitely many subgroups of  $\text{Gal}_{\mathbb{Q}}(E)$ , there are finitely many intermediate fields between  $\mathbb{Q}$  and  $E$ .

We recall that if  $E/F$  is a finite Galois extension and  $L \in \text{Int}(E/F)$  then  $L/F$  is *not* necessarily Galois. When is this true?

$$\begin{array}{c} E \leftrightarrow \{1\} = \text{Gal}_E(E) \\ \uparrow \qquad \downarrow \\ L \leftrightarrow L^* = \text{Gal}_L(E) \\ \uparrow \qquad \downarrow \\ F \leftrightarrow G = \text{Gal}_F(E) \end{array}$$

From the above picture, if  $L/F$  is Galois, the corresponding group is  $G/L^*$  which is well-defined iff  $L^* \trianglelefteq G$ . We will work towards showing  $L/F$  is Galois iff  $L^* \trianglelefteq G$ .

**Proposition 8.3:** Let  $E/F$  be a finite Galois extension and  $G = \text{Gal}_F(E)$ . Let  $L \in \text{Int}(E/F)$ . For  $\psi \in G$ , we have  $\text{Gal}_{\psi(L)}(E) = \psi \text{Gal}_L(E) \psi^{-1}$ .

*Proof:* For any  $\alpha \in \psi(L)$ ,  $\psi^{-1}(\alpha) \in L$ . If  $\varphi \in \text{Gal}_L(E)$  we then have

$$\varphi(\psi^{-1}(\alpha)) = \psi^{-1}(\alpha) \implies \psi\varphi\psi^{-1}(\alpha) = \alpha.$$

Therefore  $\psi\varphi\psi^{-1} \in \text{Gal}_{\psi(L)}(E)$  for all  $\varphi \in \text{Gal}_L(E)$ . Therefore

$$\psi \text{Gal}_L(E) \psi^{-1} \leq \text{Gal}_{\psi(L)}(E).$$

Since  $\psi \in \text{Aut}_F(E)$  is a vector space isomorphism, it acts as a change of basis over  $E/L$ , so  $[E : L] = [E : \psi(L)]$ . Thus

$$\begin{aligned}
|\psi \text{Gal}_L(E)\psi^{-1}| &= |\text{Gal}_L(E)| \\
&= [E : L] \\
&= [E : \psi(L)] \\
&= |\text{Gal}_{\psi(L)}(E)|,
\end{aligned}$$

so we have  $\psi \text{Gal}_L(E)\psi^{-1} = \text{Gal}_{\psi(L)}(E)$ .  $\square$

**Theorem 8.4:** Let  $E/L$ ,  $L$ ,  $L^*$  be defined as in [Theorem 8.2](#). Then  $L/F$  is a Galois extension iff  $L^* \trianglelefteq \text{Gal}_F(E)$ . In this case,  $\text{Gal}_F(L) \cong \text{Gal}_F(E)/L^*$

*Proof:* We have

$$\begin{aligned}
L/F \text{ normal} &\iff \psi(L) = L, \quad \forall \psi \in \text{Gal}_F(E) \\
&\iff \text{Gal}_{\psi(L)}(E) = \text{Gal}_L(E), \quad \forall \psi \in \text{Gal}_F(E) \\
&\iff \psi \text{Gal}_L(E)\psi^{-1} = \text{Gal}_L(E), \quad \forall \psi \in \text{Gal}_F(E) \\
&\iff \text{Gal}_L(E) = L^* \trianglelefteq \text{Gal}_F(E).
\end{aligned}$$

Now  $L \subseteq E$  where everything in  $E$  is separable over  $F$ , so  $L/F$  is separable. In the case  $L/F$  is normal it is therefore Galois, and the restriction map

$$\begin{aligned}
\text{Gal}_F(E) &\rightarrow \text{Gal}_F(L) \\
\psi &\mapsto \psi|_L
\end{aligned}$$

is well-defined, as  $\psi(L) = L$ . Moreover, it is surjective and its kernel is  $\text{Gal}_L(E)$  (the maps that fix  $L$ ). Therefore  $\text{Gal}_F(E)/L^* \cong \text{Gal}_F(L)$ .  $\square$

*Example:* For a prime  $p$ , let  $q := p^n$ . Consider the finite field  $\mathbb{F}_q$  of  $q$  elements which is an extension of  $\mathbb{F}_p$  of degree  $n$ . Recall the Frobenius automorphism

$$\begin{aligned}
\sigma_p : \mathbb{F}_q &\rightarrow \mathbb{F}_q \\
\alpha &\mapsto \alpha^{p^n}.
\end{aligned}$$

For  $\alpha \in \mathbb{F}_q$ , we have  $\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha$  so  $\sigma_p^n = \text{id}$ . For  $1 \leq m < n$ , we have  $\sigma_p^m(\alpha) = \alpha^{p^m}$ . Since  $x^{p^m} - x$  has at most  $p^m$  roots in  $\mathbb{F}_q$ , there exists  $\alpha \in \mathbb{F}_q$  such that  $\alpha^{p^m} \neq \alpha$ , and so  $\sigma_p^m \neq \text{id}$ . Therefore  $\sigma_p$  has order  $n$  in  $\text{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) =: G$ . It follows that

$$n = |\langle \sigma_p \rangle| \leq |G| = [\mathbb{F}_q : \mathbb{F}_p] = n,$$

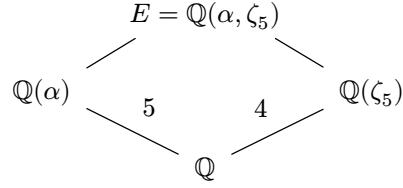
where the last equality is by [Proposition 5.7](#). Thus  $G = \langle \sigma_p \rangle$  is a cyclic group of order  $n$ . Consider a subgroup  $H \leq G$  of order  $d$ . Then  $d \mid n$  and  $[G : H] = \frac{n}{d}$ . By [Theorem 8.2](#),

$$\frac{n}{d} = [G : H] = [H^* : G^*] = [\mathbb{F}_q^H : \mathbb{F}_q^G] = [\mathbb{F}_q^H : \mathbb{F}_p].$$

Therefore  $H^* = \mathbb{F}_q^H = \mathbb{F}_{p^{n/d}}$ . We have:

$$\begin{array}{ccc}
\mathbb{F}_q & \leftrightarrow & \{1\} \\
\uparrow & & \downarrow \\
H^* & \leftrightarrow & H \\
\uparrow & & \downarrow \\
\mathbb{F}_p & \leftrightarrow & G
\end{array}$$

*Example:* Let  $E$  be the splitting field of  $x^5 - 7$  in  $\mathbb{Q}$  over  $\mathbb{C}$ . Then  $E = \mathbb{Q}(\alpha, \zeta_5)$  where  $\alpha = \sqrt[5]{7}$  and  $\zeta_5 = \exp\left(\frac{2\pi i}{5}\right)$ . The minimal polynomials of  $\alpha$  and  $\zeta_5$  over  $\mathbb{Q}$  are  $x^5 - 7$  and  $x^4 + x^3 + x^2 + x + 1$  respectively. We have



Since  $[Q(\alpha) : Q] = 5$  and  $[Q(\zeta_5) : Q] = 4$  are divisors of  $[E : Q]$  we have  $20 \mid [E : Q]$ , so  $[E : Q(\zeta_5)] \geq 5$ . Also,  $E = Q(\zeta_5)(\alpha)$  and the minimal polynomial of  $\alpha$  over  $Q(\zeta_5)$  divides  $x^5 - 7$ , so has degree at most 5. Therefore  $[E : Q(\zeta_5)] = 5$ , giving  $[E : Q] = 20$ . It follows that  $\text{Gal}_Q(E)$  is a group of order 20.

Each  $\psi \in G$  is determined by where it sends  $\alpha$  and  $\zeta_5$ . Write  $\psi_{k,s}$  for the map  $\psi$  that sends

$$\begin{aligned}\psi(\alpha) &= \alpha\zeta_5^k, \quad k \in \mathbb{Z}_5 \\ \psi(\zeta_5) &= \zeta_5^s, \quad s \in \mathbb{Z}_5^*\end{aligned}$$

Define

$$\begin{aligned}\sigma := \psi_{1,1} &= \begin{cases} \alpha \mapsto \alpha\zeta_5 \\ \zeta_5 \mapsto \zeta_5 \end{cases} \\ \tau := \psi_{0,2} &= \begin{cases} \alpha \mapsto \alpha \\ \zeta_5 \mapsto \zeta_5^2 \end{cases}\end{aligned}$$

**Exercise 8.2:** Verify that  $\tau\sigma = \sigma^2\tau$  and  $G = \langle \sigma, \tau : \sigma^5 = \tau^4 = 1, \tau\sigma = \sigma^2\tau \rangle$ .



It follows that  $G = \{\sigma^a\tau^b : a \in \mathbb{Z}_5, b \in \mathbb{Z}_4\}$ . Since  $|G| = 20$ , by Lagrange's theorem a subgroup can only have one of the following orders:

$$1, 2, 4, 5, 10, 20.$$

Let  $n_p$  denote the number of Sylow  $p$ -subgroups. Recall by the third Sylow theorem since  $20 = 2^2 \cdot 5$  that  $n_5 \mid 4$  and  $n_5 \equiv 1 \pmod{5}$ , so the only choice is  $n_5 = 1$ , so there is a unique Sylow 5-subgroup, say  $P_5$ , of order 5. By the Sylow theorems  $P_5 \trianglelefteq G$  and since  $\langle \sigma \rangle$  is a subgroup of order 5, we have that  $P_5 = \langle \sigma \rangle$ .

Also,  $n_2 \mid 5$  and  $n_2 \equiv 1 \pmod{2}$ , so  $n_2 \in \{1, 5\}$ . Now if  $n_2 = 1$ , there is a single Sylow 2-subgroup say  $P_4 = \langle \tau \rangle \cong \mathbb{Z}_4$ , where  $P_4 \trianglelefteq G$ . Since  $|P_4 \cap P_5| = 1$  we have

$$G \cong P_4 \times P_5 \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20},$$

which contradicts that  $G$  is not abelian. Thus there are 5 Sylow 2-subgroups each of order 4. We have seen that  $\tau$  is of order 4, so  $\langle \tau \rangle$  is a Sylow 2-subgroup and the others must be conjugate to  $\langle \tau \rangle$ . Note since all elements of  $G$  are of the form  $\sigma^a\tau^b$  we have

$$\sigma^a\tau^b\tau\tau^{-b}\sigma^{-a} = \sigma^a\tau\sigma^{-a}, \quad a \in \mathbb{Z}_5.$$

Now using  $\tau\sigma = \sigma^2\tau$ ,

$$\langle \sigma^4\tau\sigma^{-4} \rangle = \langle \sigma^{-1}\tau\sigma \rangle = \langle \sigma\tau \rangle = \langle \psi_{1,2} \rangle.$$

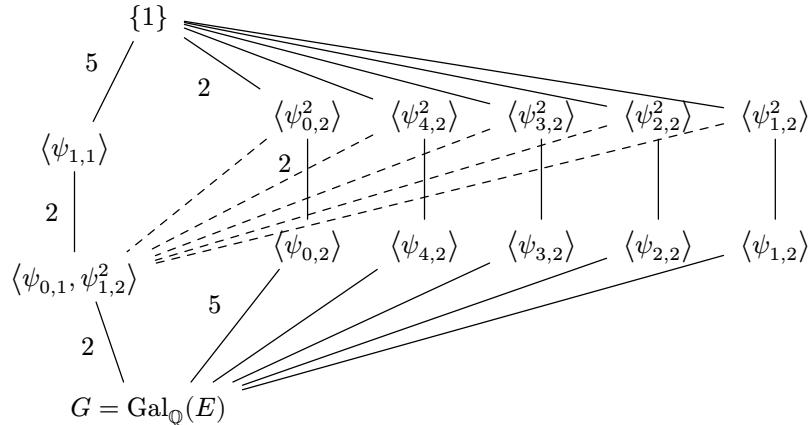
Similarly, we see the Sylow 2-subgroups are

$$\langle \psi_{0,2} \rangle, \langle \psi_{1,2} \rangle, \langle \psi_{2,2} \rangle, \langle \psi_{3,2} \rangle, \langle \psi_{4,2} \rangle.$$

Moreover, since a subgroup of  $G$  of order 2 is contained in a Sylow 2-subgroup,

$$\langle \psi_{0,2}^2 \rangle, \langle \psi_{1,2}^2 \rangle, \langle \psi_{2,2}^2 \rangle, \langle \psi_{3,2}^2 \rangle, \langle \psi_{4,2}^2 \rangle$$

are all the subgroups of  $G$  of order 2. For a subgroup  $H$  of  $G$  with order 10, since  $P_5$  is the only subgroup of order 5 we have  $H \supseteq P_5 = \langle \sigma \rangle$ , so  $\sigma^a\tau^b \in H \iff \tau^b \in H$ . The only element of the form  $\tau^b$  of order 2 is  $\tau^2$ , so  $H = \langle \sigma, \tau^2 \rangle$ . We have now found all subgroups of  $G$ , so combining everything we get the following diagram:



The dotted lines indicate that  $\langle \psi_{0,1}, \psi_{1,2}^2 \rangle$  contains each subgroup of order 2. The edge labels are the index of each subgroup inclusion.

Now for an intermediate field  $L$  of  $E/\mathbb{Q}$ , we consider  $L^* = \text{Gal}_L(E)$ . For example, for  $\mathbb{Q}(\zeta_5)$  note that  $\psi_{1,1}(\zeta_5) = \zeta_5$ , so  $\mathbb{Q}(\zeta_5)^* \supseteq \langle \psi_{1,1} \rangle$ . Since

$$|\langle \psi_{1,1} \rangle| = [\langle \psi_{1,1} \rangle : \{1\}] = 5 = [E : \mathbb{Q}(\zeta_5)] = [\mathbb{Q}(\zeta_5)^* : \{1\}]$$

we have  $\mathbb{Q}(\zeta_5)^* = \langle \psi_{1,1} \rangle$ . Also,

$$\psi_{1,2}(\alpha\zeta_5^r) = \alpha\zeta_5\zeta_5^{2r} = \alpha\zeta_5^{2r+1}.$$

If  $\psi_{1,2}$  fixes  $\alpha\zeta_5^r$ , then  $r \equiv 2r+1 \pmod{5}$  i.e.  $r \equiv 4 \pmod{5}$ . Thus  $\mathbb{Q}(\alpha\zeta_5^4) \supseteq \langle \psi_{1,2} \rangle$ . Since

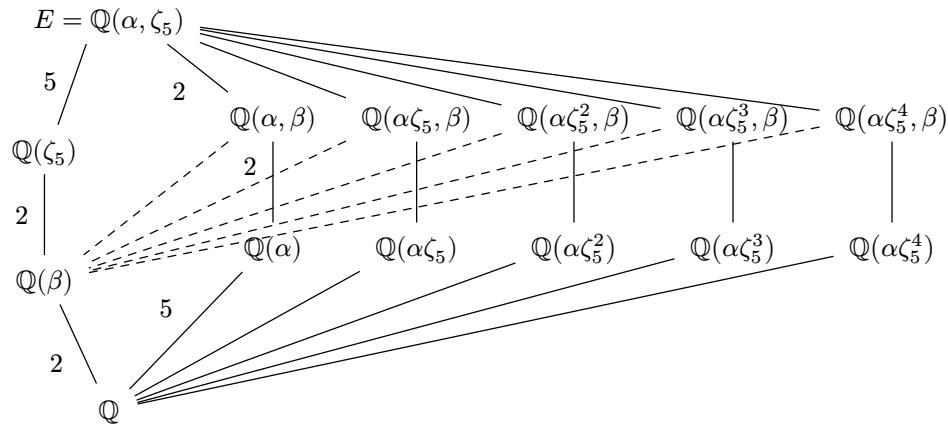
$$|\langle \psi_{1,2} \rangle| = [\langle \psi_{1,2} \rangle : \{1\}] = 4 = [E : \mathbb{Q}(\alpha\zeta_5^4)] = [\mathbb{Q}(\alpha\zeta_5^4)^* : \{1\}]$$

we have  $\mathbb{Q}(\alpha\zeta_5^4)^* = \langle \psi_{1,2} \rangle$ . Using the same argument we can get  $\langle \psi_{r,2} \rangle^*$  for  $r \in \mathbb{Z}_5$ .

Consider  $\beta = \zeta_5 + \zeta_5^{-1} \in \mathbb{R}$ . We have

$$\begin{aligned} \beta^2 + \beta - 1 &= (\zeta_5 + \zeta_5^{-1})^2 + \zeta_5 + \zeta_5^{-1} - 1 \\ &= \zeta_5^2 + \zeta_5^{-2} + 2 + \zeta_5 + \zeta_5^{-1} - 1 \\ &= 1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0 \end{aligned}$$

since the minimal polynomial of  $\zeta_5$  is  $1 + x + x^2 + x^3 + x^4$ . Since  $x^2 + x - 1$  has no rational roots, we have  $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$ , and similarly  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$ . We therefore obtain the following diagram of intermediate fields of  $E/\mathbb{Q}$ :



where the inclusions are reversed compared to the subgroup diagram by [Theorem 8.2](#).

## Appendix A: Solutions to Exercises

2.1:

- (a) Say  $a = ua'$  and  $b = vb'$ ,  $u, v$  units. Then  $ab = uva'b'$  by commutativity of the ring, so  $ab \sim a'b'$ .
- (b) Suppose  $a \mid b$ . Then  $b = ca$  for some  $c \in R$ , so  $vb' = b = ca = cua'$ , giving  $v^{-1}cua' = b'$ , so  $a' \mid b'$ .  
The converse is identical.

2.2: Let  $x = a + b\sqrt{d}$  and  $y = u + v\sqrt{d}$ .

$$\begin{aligned} N(x)N(y) &= (a^2 - db^2)(u^2 - dv^2) \\ &= a^2u^2 - da^2v^2 - db^2u^2 + d^2b^2v^2 \\ N(xy) &= N(au + dbv + (av + bu)\sqrt{d}) \\ &= (au + dbv)^2 - d(av + bu)^2 \\ &= a^2u^2 + 2abuv\sqrt{d} + d^2b^2v^2 - d(a^2v^2 + 2abuv + b^2u^2) \\ &= a^2u^2 - da^2v^2 - db^2u^2 + d^2b^2v^2 = N(x)N(y). \end{aligned}$$

2.3: Take  $R := \mathbb{Q} + x\mathbb{R}[x]$ . Then  $x$  is irreducible in  $R$  and  $x \mid 2x^2$  where  $2x^2 = (\sqrt{2}x)^2$  but  $x \nmid \sqrt{2}x$ . If this were true we'd have  $qx = \sqrt{2}x$  for some  $q \in \mathbb{Q}$ , but  $\sqrt{2} \notin \mathbb{Q}$ .

2.4: Let  $d := p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}$ , where it is clear  $d \mid a, b$ . If  $c \mid a, b$  write

$$c \sim p_1^{\gamma_1} \cdots p_k^{\gamma_k}.$$

Notice this product cannot contain any primes that are not  $p_1, \dots, p_k$  as otherwise we'd have some  $q \mid c$  but  $q \nmid a, b$ . Suppose wlog  $p_1$  with  $\gamma_1 > \min\{\alpha_1, \beta_1\}$ . Then wlog say  $\alpha_1$  is the minimum, so as  $cm = a$  for some  $m \in R$ ,

$$\begin{aligned} p_1^{\gamma_1} \cdots p_k^{\gamma_k} m &= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ \implies p_1^{\gamma_1 - \alpha_1} \cdots p_k^{\gamma_k} m &= p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad (*) \end{aligned}$$

since  $p_1^{\alpha_1} \neq 0$  and  $R$  is an integral domain. Then  $p_1$  divides the LHS of  $(*)$  but not the RHS as the  $p_i$  are pairwise non-associated, a contradiction. Thus each  $\gamma_i \leq \min\{\alpha_i, \beta_i\}$ , so  $c \mid d$ .

3.1: Suppose  $\sqrt{3} = x + y\sqrt{2}$  where  $x, y \in \mathbb{Q}$ . Notice  $y \neq 0$  as otherwise  $x = \sqrt{3} \in \mathbb{Q}$  and  $x \neq 0$  as otherwise  $y = \frac{\sqrt{3}}{\sqrt{2}} \notin \mathbb{Q}$ , so

$$\begin{aligned} 3 &= x^2 + 2xy\sqrt{2} + 2y^2 \\ \implies \frac{3 - x^2 - 2y^2}{2xy} &= \sqrt{2} \end{aligned}$$

where the above LHS is rational but the RHS is not, a contradiction.

3.2:

6.1:

8.1:

| 8.2:

