PMATH 348 Fields and Galois Theory

University of Waterloo - Winter 2025

4th April 2025

Instructor: Yu-Ru Liu

LaTeX : Xing Liu

Contents

1 Review of Ring Theory **3**

1.1 Introduction to Galois Theory . . . 3

1.2 Review of Ring Theory . . . 4

2 Integral Domains **8**

2.1 Irreducibles and Primes . . . 8

2.2 Ascending Chain Condition . . . 11

2.3 Unique Factorization Domains and Principal Ideal Domains . . . 13

2.4 Gauss' Lemma . . . 18

3 Field Extensions **24**

3.1 Degree of Extensions . . . 24

3.2 Algebraic and Transcendental Extensions . . . 25

4 Splitting Fields **32**

4.1 Existence of Splitting Fields . . . 32

4.2 Uniqueness of Splitting Fields . . . 34

4.3 Degrees of Splitting Fields . . . 35

5 More Field Theory **37**

5.1 Prime Fields . . . 37
5.2 Formal Derivatives and Repeated Roots . . . 38
5.3 Finite Fields . . . 40

6 Solvable Groups and Automorphism Groups **45**
6.1 Solvable Groups . . . 45
6.2 Automorphism Groups . . . 49
6.3 Automorphism Groups of Splitting Fields . . . 50

7 Separable Extensions and Normal Extensions **53**
7.1 Separable Extensions . . . 53
7.2 Normal Extensions . . . 55

8 Galois Correspondence **60**
8.1 Galois Extensions . . . 60
8.2 The Fundamental Theorem . . . 64

9 Cyclic Extensions **72**

10 Solvability by Radicals **77**
10.1 Radical Extensions . . . 77
10.2 Radical Solutions . . . 78

11 Cyclotomic Extensions **82**

1 Review of Ring Theory

Lecture 1, 2025/01/06

1.1 Introduction to Galois Theory

Polynomial Equations

Linear Equations: Let $ax + b = 0$ with $a, b \in \mathbb{R}$ and $a \neq 0$. The solution is $x = -\frac{b}{a}$.

Quadratic Equations (about 1600 BC): Let $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{R}$ and $a \neq 0$. Its solutions are $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Definition 1.1 (**Radical**). An expression involving only $+, -, \times, \div, \sqrt[n]{\cdot}$ is called a **radical**.

Cubic Equations (Tartaglia, del Ferro, Fertana (1535)): After a linear transformation, all cubic equations can be reduced to

$$x^3 + px = q.$$

A solution of the above equation is of the form (Cardanos formula)

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Quartic Equations (Ferrari): reduced to a cubic equation (see Bonus 1).

Quintic Equations:

- This question was attempted by Euler, Bezout, Lagrange without success.
- In 1799, Ruffini gave a 516-page proof about the insolvability of quintic equations (in radicals). His proof was "almost right".
- In 1824, Abel filled in the gap in Ruffini's proof.

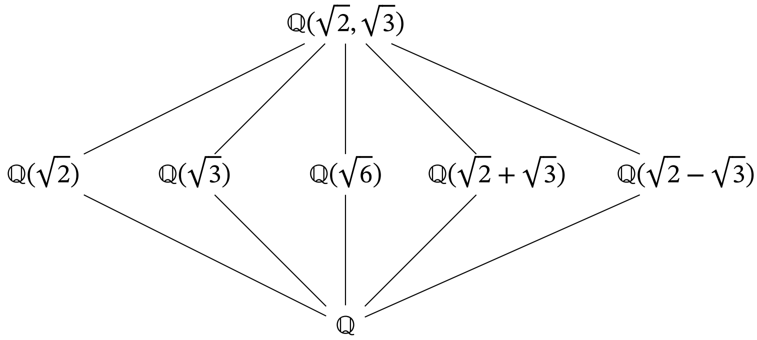
Question: Given a quintic equation, is it solvable by radicals?

Reverse Question: Suppose that a radical solution exits. How does its associated quintic equation look like?

Two main steps of the Galois Theory

(1) Link a root of a quintic equation, say α, to $\mathbb{Q}(\alpha)$, the smallest field containing $\mathbb{Q}$ and α.

- $\mathbb{Q}(\alpha)$ is a field, so it has more structures to be played with than α.
- However, our knowledge of $\mathbb{Q}(\alpha)$ is limited. For example, consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, the smallest field containing $\mathbb{Q}, \sqrt{2}, \sqrt{3}$. We do not know many intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.



(2) Link the field $\mathbb{Q}(\alpha)$ to a group. More precisely, we associate the field extension ${}^{\mathbb{Q}(\alpha)}\!/_{\mathbb{Q}}$ to the group

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha) \text{ an isomorphism and } \varphi|_{\mathbb{Q}} = 1_{\mathbb{Q}}\}.$$

- It can be shown that if α is "good". $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is a finite group.
- Moreover, there is a one-to-one correspondence between the intermediate fields of ${}^{\mathbb{Q}(\alpha)}\!/_{\mathbb{Q}}$ and the subgroups of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$.

Galois Theory (in short): the interplay between fields and groups.

1.2 Review of Ring Theory

Definition 1.2 (**Ring**). A set R is a (unitary) **ring** if it has 2 operations, addition $+$ and multiplication $\cdot$, such that $(R, +)$ is an abelian group and $(R, \cdot)$ satisfies closure, associativity and identity properties of a group, in addition to the distributive law.
More precisely, if R is a ring, then for all $a, b, c \in R$, we have

(1) $a + b \in R$.

(2) $a + b = b + a$.

(3) $a + (b + c) = (a + b) + C$.

(4) There exists $0 \in R$ s.t. $a + 0 = a = 0 + a$, 0 is called the zero of R.

(5) There exists $-a \in R$ s.t. $a + (-a) = 0 = (-a) + a$, $-a$ is called the inverse of a.

(6) $ab := a \cdot b \in R$.

(7) $a(bc) = (ab)c$.

(8) There exists $1 \in R$ s.t. $a1 = a = 1a$, 1 is called the unity of R.

(9) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ (distributive law).

The ring R is called a commutative ring if is also satisfy:

(10) $ab = ba$.

Note. Properties $(1) - (5)$ is equivalent to say that $(R, +)$ is an abelian group. Properties $(6) - (8)$ is equivalent to say that $(R, \cdot)$ is almost a group.

Note. We only consider commutative rings in PMATH 348.

Lecture 2, 2025/01/08

Definition 1.3 (Unit). Let R be a commutative ring. We say that $u \in \mathbb{R}$ is a **unit** if u has a multiplicative inverse in R, denoted by u^{-1}, i.e. $uu^{-1} = 1 = u^{-1}u$.
Let R^* denote the set of all units in R. Note that $(R^*, \cdot)$ is a group.

Definition 1.4 (Field). A commutative ring $R \neq \{0\}$ with $R^* = R \setminus \{0\}$ is a **field**.

Definition 1.5 (Integral Domain). A commutative ring $R \neq \{0\}$ is an **integral domain** if for $a, b \in R$, $ab = 0$ implies that $a = 0$ or $b = 0$.

Example. $\mathbb{Z}$ is an integral domain, while $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Proposition 1.1. Every subring of a field (including the field itself) is an integral domain.

Definition 1.6 (Ideal). A subset I of a commutative ring R is an **ideal** if $0 \in I$ and for $a, b \in I$ and $r \in R$, we have $a - b \in I$ and $ra \in I$.

Example. Let I be an ideal of a commutative ring R. If $1_R \in I$, then $I = R$.

Example. The only ideals of a field F are $\{0\}$ and F.

The ring of integers $\mathbb{Z}$

- $\mathbb{Z}$ is an integral domain.
- The units of $\mathbb{Z}$ are $\{\pm 1\}$.
- Division Algorithm in $\mathbb{Z}$: for $a, b \in \mathbb{Z}$ with $a \neq 0$, we can write $b = aq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < |a|$.
- Using the division algorithm in $\mathbb{Z}$, we can prove that an ideal I of $\mathbb{Z}$ is of the form $I = \langle n \rangle = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Note that if $n > 0$, then the generator is unique.
- Consider all fields containing $\mathbb{Z}$. Their intersection (the smallest field containing $\mathbb{Z}$) is the set of rational numbers $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$.

The polynomial ring $F[x]$ (F: a field)

Define $F[x] = \{f(x) = a_0 + a_1 x + \cdots + a_m x^m : a_i \in F\ (0 \leq i \leq m)\}$.

- If $a_m = 1$, we say that $f(x)$ is <u>monic</u>.
- If $a_m \neq 0$, we define the <u>degree</u> of $f(x)$, $\deg(f(x)) = m$.Also, $\deg(0) = -\infty$.
- Product Rule: for $f(x), g(x) \in F[x]$, $\deg(fg) = \deg(f) + \deg(g)$.
- $F[x]$ is an integral domain.
- The units of $F[x]$ are $F^* = F \setminus \{0\}$.
- Division Algorithm in $F[x]$: for $f(x), g(x) \in F[x]$ with $f(x) \neq 0$, we can write $g(x) = f(x)q(x) + r(x)$ with $q(x), r(x) \in F[x]$ and $\deg(r) < \deg(f)$.
- Using the division algorithm in $F[x]$, we can prove that an ideal I of $F[x]$ is of the form $I = \langle f(x) \rangle = f(x)F[x]$ for some $f(x) \in F[x]$. Note that if $f(x)$ is monic, then it is unique.

- Consider all fields containing $F[x]$. Their intersection is the set of rational functions

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

Definition 1.7 (Quotient Ring). Let I be an ideal of a ring R. We recall that the additive quotient group R/I is a ring with the multiplication $(r+I)(s+I) = rs + I$. The unity of R/I is $1 + I$. This is the **quotient ring** of R by I.

Theorem 1.2 (First Isomorphism Theorem).
Let $\theta : R \to S$ be a ring homomorphism. Then the kernel of θ, $\operatorname{Ker}\theta$, is an ideal of R. Also, we have

$$R/\operatorname{Ker}\theta \cong \operatorname{im}\theta.$$

Example. Let F be a field and S be a ring and let $\phi : F \to S$ be a ring homomorphism. Since the only ideals of F are $\{0\}$ and F, either ϕ is injective or $\phi = 0$.

Definition 1.8 (Prime Ideal). Let R be a commutative ring. An ideal $P \neq R$ of R is a **prime ideal** if whenever $r, s \in R$ satisfy $rs \in P$, then $r \in P$ or $s \in P$.

Definition 1.9 (Maximal Ideal). Let R be a commutative ring. An ideal $M \neq R$ of R is a **maximal ideal** if whenever A is an ideal such that $M \subseteq A \subseteq R$, then $A = M$ or $A = R$.

Proposition 1.3. Every maximal ideal if a prime ideal.

Theorem 1.4. Let I be an ideal of a ring R and $I \neq R$. Then

(1) I is a maximal ideal $\iff$ R/I is a field.

(2) I is a prime ideal $\iff$ R/I is an integral domain.

2 Integral Domains

2.1 Irreducibles and Primes

Definition 2.1 (Divides). Let R be an integral domain and $a, b \in R$. We say that a **divides** b, denoted by $a \mid b$, if $b = ca$ for some $c \in R$.

Proposition 2.1. Let R be an integral domain. For $a, b \in R$, the following are equivalent:

(1) $a \mid b$ and $b \mid a$.

(2) $a = ub$ for some unit $u \in R$.

(3) $\langle a \rangle = \langle b \rangle$.

Proof.

(1) $\implies$ (2): If $a \mid b$ and $b \mid a$, write $b = ua$ and $a = vb$ for some $u, v \in R$. If $a = 0$, then $b = 0$ and thus $a = 1b$. If $a \neq 0$, then $a = v(ua) = (vu)a$. This implies that $uv = 1$ since R is an integral domain. Thus, u is a unit.

(2) $\implies$ (3): If $a = ub$, then $\langle a \rangle \subseteq \langle b \rangle$. Since u is a unit, and $b = u^{-1}a$, we have $\langle b \rangle \subseteq \langle a \rangle$. It follows that $\langle a \rangle = \langle b \rangle$.

(3) $\implies$ (1): If $\langle a \rangle = \langle b \rangle$, then $a \in \langle a \rangle = \langle b \rangle$. Thus, $a = ub$ for some $u \in R$, i.e. $b \mid a$. Similarly, since $b \in \langle a \rangle$, we have $a \mid b$. □

Lecture 3, 2025/01/10

Definition 2.2 (Associated). Let R be an integral domain. For $a, b \in R$, we say a is **associated** to b, denoted by $a \sim b$, if $a \mid b$ and $b \mid a$. From Proposition 2.1, $\sim$ is an equivalence relation in R. More precisely,

(1) $a \sim a$, $\forall a \in R$.

(2) If $a \sim b$, then $b \sim a$.

(3) If $a \sim b$ and $b \sim c$, then $a \sim c$.

Remark. Also, we can show (see Piazza):

(1) If $a \sim a'$ and $b \sim b'$, then $ab \sim a'b'$.

(2) If $a \sim a'$ and $b \sim b'$, then $a \mid b \iff a' \mid b'$.

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

Definition 2.3 (Irreducible, Reducible).
Let R be an integral domain. We say $p \in R$ is **irreducible** if $p \neq 0$ is not a unit, and if $p = ab$ with $a, b \in R$, then either a or b is a unit in R. An element that is not irreducible is called **reducible**.

Example. Let $R = \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ and $p = 1 + \sqrt{-5}$.

Claim. p is irreducible in R.

For $d = m + n\sqrt{-5}$, the norm of d is defined to be $N(d) = (m + n\sqrt{-5})(m - n\sqrt{-5}) = m^2 + 5n^2 \in \mathbb{N} \cup \{0\}$. One can check that $N(ab) = N(a)N(b)$ for $a, b \in R$ (see Piazza) and $N(d) = 1 \iff d$ is a unit (see A1).

Proof of Claim. Suppose that $p = ab \in R$. Then,

$$6 = N(p) = N(a)N(b).$$

Note that $6 = 1 \cdot 6 = 2 \cdot 3$. If $N(d) = m^2 + 5n^2 = 2$ with $m, n \in \mathbb{Z}$, then $n = 0$. However, $m^2 \neq 2$. Hence $N(d) \neq 2$. Similarly, $N(d) \neq 3$. Thus, we have either $N(a) = 1$ or $N(b) = 1$, i.e. either a or b is a unit in R. Thus, p is irreducible.

Another way to show $m^2 + 5n^2 \neq 2$ is to consider the equation $m^2 + 5n^2 \equiv 2 \pmod 5$. It has no solutions since for $m \equiv 0, 1, 2, 3, 4 \pmod 5$, we have $m^2 \equiv 0, 1, 4 \pmod 5$. □

Proposition 2.2. Let R be an integral domain and let $p \in R$ with $p \neq 0$, not a unit. The following are equivalent:

(1) p is irreducible.

(2) If $d \mid p$, then $d \sim 1$ or $d \sim p$.

(3) If $p \sim ab$ in R, then $p \sim a$ or $p \sim b$.

(4) If $p = ab$ in R, then $p \sim a$ or $p \sim b$.

As a consequence, if $p \sim q$, then p is irreducible $\iff$ q is irreducible.

Proof.

(1) $\implies$ (2): If $p = ad$ for some $a \in R$, then by (1), either d or a is a unit. Thus, $d \sim 1$ or $d \sim p$.

(2) $\implies$ (3): If $p \sim ab$, then $b \mid p$. By (2), either $b \sim 1$ or $b \sim p$. If $b \sim p$, then we are done. If $b \sim 1$, then $a \sim p$.

(3) $\implies$ (4): This is clear.

(4) $\implies$ (1): If $p = ab$, then by (4), either $p \sim a$ or $p \sim b$. If $p \sim a$, write $a = up$ for some unit u. Since R is commutative, we have $p = ab = (up)b = p(ub)$. Since R is an integral domain and $p \neq 0$, we have $1 = ub$. Thus, b is a unit. Similarly, $p \sim b$ implies that a is a unit. Thus (1) follows. □

Definition 2.4 (**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 $p \mid ab$ with $a, b \in R$, then $p \mid a$ or $p \mid b$.

Remark. If $p \sim q$, then p is prime $\iff$ q is prime (exercise). Also, by induction, if p is a prime and $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.

Proposition 2.3. Let R be an integral domain and $p \in R$. If p is prime, then p is irreducible.

Proof. Let $p \in R$ be prime. If $p = ab$ in R, then $p \mid a$ or $p \mid b$. If $p \mid a$, write $a = dp$ for some $d \in R$. Since R is commutative, we have $a = dp = d(ab) = a(db)$. Since R is an integral domain and $a \neq 0$, we have $1 = db$. Thus, b is a unit. Similarly, if $p \mid b$, then a is a unit. If follows that p is irreducible. □

Example. The converse of Proposition 2.3 is not true. Consider

$$R = \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\} \quad \text{and} \quad p = 1 + \sqrt{-5}.$$

Claim. p is not prime in R.

Proof. We recall that for $d = m + n\sqrt{-5}$, $N(d) = m^2 + 5n^2 \in \mathbb{N} \cup \{0\}$. Note that $2 \cdot 3 = 6 =$

$(1+\sqrt{-5})(1-\sqrt{-5})$ in R. If p is prime, since $p \mid 2 \cdot 3$, then $p \mid 2$ or $p \mid 3$. Suppose $p \mid 2$, say $2 = qp$ for some $q \in R$. If follows that

$$4 = N(2) = N(q)N(p) = 6N(q)$$

which is not possible since $N(q) \in \mathbb{N} \cup \{0\}$. Similarly, $p \mid 3$ is not possible. Thus p is not prime.

$\square$

Lecture 4, 2025/01/13

We recall that for a prime $p \in \mathbb{Z}$, we have $p = \pm 1, \pm p$ are the only factorizations of p (i.e. p is irreducible). Also, we can prove Euclid's lemma, which states that if $p \mid ab$, then $p \mid a$ or $p \mid b$ (i.e. p is prime). The same thing holds if we replace $\mathbb{Z}$ with $F[x]$ for a field F.

Question: What is the additional property in $\mathbb{Z}$ or $F[x]$ that allows us to get "irreducible $\implies$ prime"?

Exercise: Construct another element that is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$.

2.2 Ascending Chain Condition

Definition 2.5 (**Ascending Chain Condition on Principal Ideals (ACCP)**).
An integral domain R is said to satisfy the **ascending chain conditions on principal ideals (ACCP)** if for any ascending chain $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$ of principal ideals in R, $\exists n \in \mathbb{N}$ s.t.

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

Example.

Claim. $\mathbb{Z}$ satisfies ACCP.

Proof. If $\{0\} \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$ in $\mathbb{Z}$, then $a_2 \mid a_1$, $a_3 \mid a_2$, and so on. Taking absolute values gives $|a_1| \geq |a_2| \geq |a_3| \geq \cdots$. Since each $|a_i| \geq 0$ is an integer, we get $|a_n| = |a_{n+1}| = \cdots$ for some $n \in \mathbb{N}$. It implies that $a_{i+1} = \pm a_i$ for all $i \geq n$. Thus, $\langle a_i \rangle = \langle a_{i+1} \rangle$ for all $i \geq n$. $\square$

Theorem 2.4. Let R be an integral domain satisfying the ACCP. If $a \in R$ with $a \neq 0$ is not a unit, then a can be written as a product of irreducible elements of R.

Proof. Suppose that $\exists 0 \neq a \in R$ with a is not a unit, which is not a product of irreducible elements. Since a is not irreducible, by Proposition 2.2, we can write $a = x_1 a_1$ with $a \nsim x_1$ and $a \nsim a_1$. Note that at least one of x_1 and WLOG suppose a_1 is not a product of irreducible elements (if both are, so is a). Suppose that a_1 is not a product of irreducible elements. Then, as before, we can write $a_1 = x_2 a_2$ with $a_1 \nsim x_2$ and $a_1 \nsim a_2$. This process continues infinitely and we have an ascending chain of principal ideals

$$\langle a \rangle \subseteq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots .$$

Since $a \nsim a_1$, $a_1 \nsim a_2$, ..., by Proposition 2.1, we have

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

which contradicts ACCP. Thus, such an a does not exist. □

Theorem 2.5. If R is an integral domain satisfying the ACCP, so is $R[x]$.

Proof. Suppose that $R[x]$ does not satisfy ACCP. Then, there exists a chain of principal ideals $\{0\} \subsetneq \langle f_1 \rangle \subsetneq \langle f_2 \rangle \subsetneq \cdots$ in $R[x]$. Thus, we have $f_{i+1} \mid f_i$ for all $i \in \mathbb{N}$. Let a_i denote the leading coefficient of f_i for each i. Since $f_{i+1} \mid f_i$, we have $a_{i+1} \mid a_i$ for each i. Thus, $\{0\} \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$ in R. Since R satisfies ACCP, we have $\langle a_n \rangle = \langle a_{n+1} \rangle = \cdots$ for some $n \geq 1$, i.e. $a_n \sim a_{n+1} \sim \cdots$. For $m \geq n$, let $f_m = g f_{m+1}$ for some $g(x) \in R[x]$. If b is the leading coefficient of $g(x)$, then $a_m = b a_{m+1}$. Since $a_m \sim a_{m+1}$, then b is a unit in R. However, $g(x)$ is not a unit in $R[x]$ since $\langle f_m \rangle \neq \langle f_{m+1} \rangle$. Thus, $g(x) \neq b$ and we have $\deg(g) \geq 1$. By the product formula for $R[x]$, it implies that $\deg(f_m) > \deg(f_{m+1})$ and it is true for all $m \geq n$. Thus, we have

$$\deg(f_n) > \deg(f_{n+1}) > \cdots$$

which leads to a contradiction since $\deg(f_i) \geq 0$. Thus, $R[x]$ satisfies ACCP. □

Example. Since $\mathbb{Z}$ satisfies ACCP, so does $\mathbb{Z}[x]$ by Theorem 2.5.

Example. Consider $R = \{n + xf : n \in \mathbb{Z}, f \in \mathbb{Q}[x]\}$, the set of polynomials in $\mathbb{Q}[x]$ whose constant term is in $\mathbb{Z}$. Then, R is an integral domain (exercise), but we have

$$\langle x \rangle \subsetneq \left\langle \frac{1}{2}x \right\rangle \subsetneq \left\langle \frac{1}{2^2}x \right\rangle \subsetneq \cdots \quad \text{in } R.$$

Thus, R does not satisfy ACCP.

2.3 Unique Factorization Domains and Principal Ideal Domains

Definition 2.6 (**Unique Factorization Domain (UFD)**).
An integral domain R is called a **unique factorization domain** (**UFD**) if it satisfies the following conditions:

(1) If $a \in R$ with $a \neq 0$ is not a unit, then a is a product of irreducible elements in R.

(2) If $p_1 p_2 \cdots p_r \sim q_1 q_2 \cdots q_s$, where p_i and q_i are irreducible, then $r = s$ and after possible reordering, $p_i \sim q_i$ for all i.

Example. $\mathbb{Z}$ and $F[x]$ (F is a field) are UFDs.

Example. A field is a UFD.

Proposition 2.6. 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 $p \mid ab$, with $a, b \in R$, write $ab = pd$ for some $d \in R$. Since R is a UFD, we can factor a, b and d into irreducible elements, say $a = p_1 \cdots p_k$, $b = q_1 \cdots q_l$, and $d = r_1 \cdots r_m$ (here we allow k, l, or m to be 0 to take care of the case when a, b, or d is a unit). Since $pd = ab$, we have $pr_1 \cdots r_m = p_1 \cdots p_k q_1 \cdots q_l$. Since p is irreducible, it implies that $p \sim p_i$ for some i or $p \sim q_j$ for some j. Thus, $p \mid a$ or $p \mid b$. $\square$

Example. Since $\mathbb{Z}$ is a UFD, a prime $p \in \mathbb{Z}$ satisfies Euclid's lemma: $p \mid ab \implies p \mid a$ or $p \mid b$. A similar statement holds if we replace $\mathbb{Z}$ by $F[x]$.

Example. Consider $R = \mathbb{Z}[\sqrt{-5}]$ and $p = 1 + \sqrt{-5} \in R$. We have seen before that p is irreducible in R but not prime. By Proposition 2.6, R is not a UFD. For example,

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

where $1 \pm \sqrt{-5}, 2, 3$ are all irreducible in R. However, $1 + \sqrt{-5} \nsim 2$ and $1 + \sqrt{-5} \nsim 3$. Since $N(1 + \sqrt{-5}) = 6$ while $N(2) = 4$ and $N(3) = 9$ (note that $u \in R$ is a unit $\iff N(u) = 1$).

Example.

Claim. $R = \mathbb{Z}[\sqrt{-5}]$ satisfies the ACCP.

Proof. If $\{0\} \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$ in R, then $a_2 \mid a_1$, $a_3 \mid a_2$, and so on. Taking the norms gives $N(a_1) \geq N(a_2) \geq N(a_3) \geq \cdots$. Since each $N(a_i) \geq 0$ is an integer, we get $N(a_n) = N(a_{n+1}) = \cdots$ for some $n \in \mathbb{N}$. Since $N(d) = 1 \iff d$ is a unit in R, it follows that $a_{i+1} \sim a_i$ for all $i \geq n$. Thus, $\langle a_i \rangle = \langle a_{i+1} \rangle$ for all $i \geq n$. $\square$

Definition 2.7 (**Greatest Common Divisor**).

Let R be an integral domain and $a, b \in R$. We say $d \in R$ is a **greatest common divisor** (note that it is no longer unique) of a, b, denoted by $\gcd(a, b)$, if it satisfies the following conditions:

(1) $d \mid a$ and $d \mid b$.

(2) If $e \in R$ with $e \mid a$ and $e \mid b$, then $e \mid d$.

One can prove the following (see Piazza).

Proposition 2.7. Let R be a UFD and $a, b \in R \setminus \{0\}$. If $p_1, \ldots, p_k$ are non-associated primes dividing a and b, say $a \sim p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b \sim p_1^{\beta_1} \cdots p_k^{\beta_k}$ with $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$, then

$$\gcd(a, b) \sim p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}.$$

Remark. If R is a UFD and $d, a_1, \dots, a_m \in R$, we have (exercise) $\gcd(da_1, \dots, da_m) = d\gcd(a_1, \dots, a_m)$.

Theorem 2.8. Let R be an integral domain, the following are equivalent:

(1) R is a UFD.

(2) R satisfies ACCP and $\gcd(a, b)$ exists for all non-zero $a, b \in R$.

(3) R satisfies ACCP and every irreducible element in R is prime.

Lecture 6, 2025/01/17

Proof of Theorem 2.8.

(1) $\implies$ (2): By Proposition 2.7, $\gcd(a, b)$ exists. Suppose that $\exists \{0\} \neq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$ in R. Since $\langle a_1 \rangle \neq \{0\}$, we know that $a_1 \neq 0$ is not a unit, and write $a_1 = p_1^{k_1} \cdots p_r^{k_r}$ 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 $0 \le d_{i,j} \le k_j$ with $1 \le j \le r$. Thus, there are only finitely many non-associated choices for a_i and so there exists $m \pm n$ with $a_m \sim a_n$. This implies that $\langle a_m \rangle = \langle a_n \rangle$, which is a contradiction. Thus, R satisfies ACCP.

(2) $\implies$ (3): Let $p \in R$ be irreducible and suppose that $p \mid ab$. By (2), let $d \sim \gcd(a, p)$. Then, $d \mid p$. Since p is irreducible, we have $d \sim p$ or $d \sim 1$. In the first case, since $d \sim p$ and $d \mid a$, we have $p \mid a$. In the second case, since $d \sim \gcd(a, p) \mid 1$, then $\gcd(ab, pb) \sim b$. Since $p \mid ab$ and $p \mid pb$, we have $p \mid \gcd(ab, pb)$ i.e. $p \mid b$. Thus, p is prime.

(3) $\implies$ (1): If R satisfies ACCP, by Theorem 2.4, for $a \in R$ with $a \neq 0$ not a unit, a is a product of irreducible elements of R. Thus, it suffices to show that such factorization is unique. Suppose we have $p_1 \cdots p_r \sim q_1 \cdots q_s$, where p_1 and q_j are irreducible. Since p_1 is a prime, then $p_1 \mid q_j$ for some j, say q_1. By Proposition 2.2, we have $p_1 \sim q_1$. Since $p_i \sim q_i$ with $1 \le i \le r$. Thus, the factorization is unique. $\square$

Definition 2.8 (Principal Ideal Domain (PID)).
An integral domain R is called a **principal ideal domain (PID)** if every ideal is principal, i.e. every ideal is of the form $\langle a \rangle = aR$ for some $a \in R$.

Example. $\mathbb{Z}$ and $F[x]$ with F being a field, are PIDs.

Example. A field F is a PID, since its only ideals are $\{0\}$ and F.

Example. Let $n \in \mathbb{N}$ with n not a prime Although all ideals of $\mathbb{Z}_n$ are principal (exercise), $\mathbb{Z}_n$ is not a PID, since $\mathbb{Z}_n$ is not an integral domain.

Proposition 2.9. Let R be a PID and let $a_1, \dots, a_n$ be non-zero elements in R. Then $d \sim \gcd(a_1, \dots, a_n)$ exists and $\exists r_1, \dots, r_n \in R$ s.t.

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

Proof. Let $A = \langle a_1, \dots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\}$ which is an ideal of R. Since R is a PID, $\exists d \in R$ s.t. $A = \langle d \rangle$. Thus, $d = r_1 a_1 + \cdots + r_n a_n$ for some $r_i \in R$.

Claim. $d \sim \gcd(a_1, \dots, a_n)$.

Proof of Claim. Since $A = \langle d \rangle$ and $a_i \in A$, we have $d \mid a_i$ for all i. Also, if $r \mid a_i$ for all i, then $r \mid (r_1 a_i + \cdots + r_n a_n)$, i.e. $r \mid d$. By the definition of gcd, we have $d \sim \gcd(a_1, \dots, a_n)$. □

□

Theorem 2.10. Every PID is a UFD.

Proof. If R is a PID, by Theorem 2.8 and Proposition 2.9, it suffices to show that R satisfies the ACCP. If $\{0\} \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$ in R, write $A = \langle a_1 \rangle \cup \langle a_2 \rangle \cup \cdots$. Then, A is an ideal (exercise). Since R is a PID, we can write $A = \langle a \rangle$ for some $a \in R$. Then, $a \in \langle a_n \rangle$ for some n and hence

$$\langle a \rangle \subseteq \langle a_n \rangle \subseteq \langle a_{n+1} \rangle \subseteq \cdots \subseteq A = \langle a \rangle .$$

Thus, $\langle a_n \rangle = \langle a_{n+1} \rangle = \cdots = \langle a \rangle$, i.e. R satisfies ACCP. It follows that R is a UFD. □

Example.

Claim. $\mathbb{Z}[x]$ is not a PID.

Proof. Consider $A = \{2n + xf(x) : n \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$ which is an ideal of $\mathbb{Z}[x]$ (exercise).

Suppose $A = \langle g(x)\rangle$ for some $g(x) \in \mathbb{Z}[x]$. Since $2 \in A$, we have $g(x) \mid 2$. It follows that $g(x) \sim 1$ or $g(x) \sim 2$. If $g(x) \sim 1$, then $1 \in A$ and hence $A = \mathbb{Z}[x]$. If $g(x) \sim 2$, then $2 \in A$ and hence $A = \langle 2\rangle$. However, $x \in A$ but $x \notin \langle 2\rangle$. Thus, $A \neq \langle 2\rangle$. Thus, $\mathbb{Z}[x]$ is not a PID. □

Lecture 7, 2025/01/20

Theorem 2.11. Let R be a PID. If $0 \neq p \in R$ is not a unit, then the following are equivalent:

(1) p is a prime.

(2) $R/\langle p\rangle$ is a field.

(3) $R/\langle p\rangle$ is an integral domain.

Note. By Theorem 1.4, we see from (2) and (3) that in a PID, every non-zero prime ideal is maximal.

Proof.

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

(3) $\implies$ (1): Suppose that $p \mid ab$ with $a, b \in R$. Then,

$$\begin{aligned}(a + \langle p\rangle)(b + \langle p\rangle) &= ab + \langle p\rangle \\ &= 0 + \langle p\rangle \quad \text{in } R/\langle p\rangle.\end{aligned}$$

Since $R/\langle p\rangle$ is an integral domain, we have $a + \langle p\rangle = 0 + \langle p\rangle$ or $b + \langle p\rangle = 0 + \langle p\rangle$ in $R/\langle p\rangle$. It follows that either $p \mid a$ or $p \mid b$. Thus, p is a prime.

(1) $\implies$ (2): Suppose that p is a prime. Consider $a + \langle p\rangle \neq 0 + \langle p\rangle$ in $R/\langle p\rangle$. Then, $a \notin \langle p\rangle$ and thus $p \nmid a$. Consider $A = \{ra + sp : r, s \in R\}$, which is an ideal of R. Since R is a PID, $A = \langle d\rangle$ for some $d \in R$. Since $p \in A$, we have $d \mid p$. Since p is a prime and thus irreducible, we have $d \sim p$ or $d \sim 1$. If $d \sim p$, we have $\langle p\rangle = \langle d\rangle = A$. Since $a \in A$, we have $p \mid a$, which is a contradiction. Thus, we have $d \sim 1$. It follows that $A = \langle 1\rangle = R$. In particular, $1 \in A$, say $1 = ba + cp$ for some $b, c \in R$. Then,

$$(a + \langle p\rangle)(b + \langle p\rangle) = ab + \langle p\rangle = (1 - cp) + \langle p\rangle = 1 + \langle p\rangle \quad \text{in } R/\langle p\rangle.$$

It follows that $R/\langle p\rangle$ is a field. □

Example. $\mathbb{Z}[x]$ is NOT a PID since $A = \{2n + xf(x) : n \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$ is not principal.

Remark. We have the following chain:

$$\text{Fields} \subsetneq \text{PID} \subseteq \text{UFD} \subsetneq \text{ACCP} \subsetneq \text{Integral Domain} \subsetneq \text{Commutative Rings} \subsetneq \text{Rings}.$$

We will see that PID $\subsetneq$ UFD in the next section! An example that is a UFD, but not a PID: $\mathbb{Z}[x]$.

Remark. Theorem 2.11 may fail if we replace PID with UFD. For example, $R = \mathbb{Z}[x]$ is a UFD (see section 2.4). Consider $\langle x \rangle \in R$. Then, $R/\langle x \rangle \cong \mathbb{Z}$, which is an integral domain but not a field. Thus, $\langle x \rangle$ is a prime ideal of $\mathbb{Z}[x]$, but not a maximal ideal.

Remark.

- In a PID, maximal ideal $\iff$ prime ideal (in general, maximal $\implies$ prime).
- In a UFD, prime elements $\iff$ irreducible elements (in general, prime $\implies$ irreducible).

2.4 Gauss' Lemma

Consider $2x + 4$. It is irreducible in $\mathbb{Q}[x]$, but it is reducible in $\mathbb{Z}[x]$ since $2x + 4 = 2(x + 2)$.

Definition 2.9 (Content, Primitive Polynomial).
If R is a UFD and $0 \neq f(x) \in R[x]$, a greatest common divisor of all coefficients of $f(x)$ is called a **content** of $f(x)$ and is denoted by $c(f)$. If $c(f) \sim 1$, we say that $f(x)$ is a **primitive polynomial**.

Example. In $\mathbb{Z}[x]$, $c(6 + 10x^2 + 15x^3) \sim \gcd(6, 10, 15) \sim 1$ and $c(6 + 9x^2 + 15x^3) \sim \gcd(6, 9, 15) \sim 3$. Thus, $6 + 10x^2 + 15x^3$ is primitive while $6 + 9x^2 + 15x^3$ is not.

Lemma 2.12. Let R be a UFD and $0 \neq f(x) \in R[x]$.

(1) $f(x)$ can be written as $f(x) = c(f)f_1(x)$ where $f_1(x)$ is primitive.

(2) If $0 \neq b \in R$, then $c(bf) \sim bc(f)$.

Proof.

(1) For $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in R[x]$, let $c = c(f) \sim \gcd(a_0, \dots, a_m)$. Write $a_i = cb_i$ for all i. Then, $f(x) = cf_1(x)$ where $f_1(x) = b_m x^m + \cdots + b_1 x + b_0$. Then,

$$c \sim \gcd(a_0, \dots, a_m) \sim \gcd(cb_0, \dots, cb_m) \sim c \gcd(b_0, \dots, b_m).$$

It follows that $\gcd(b_0, \dots, b_m) \sim 1$, i.e. $c(f_1) \sim 1$. Hence, $f_1(x)$ is primitive.

(2) If $a_0, \dots, a_m$ are the coefficients of $f(x)$, then the coefficients of $bf(x)$ are $ba_0, \dots, ba_m$. Thus, $c(bf) \sim \gcd(ba_0, \dots, ba_m) \sim b \gcd(a_0, \dots, a_m) \sim bc(f)$.

□

Lemma 2.13. Let R be a UFD and $\ell(x) \in R[x]$ be irreducible with $\deg(\ell) \geq 1$. Then, $c(\ell) \sim 1$, i.e. $\ell(x)$ is primitive.

Lecture 8, 2025/01/22

Proof. By Lemma 2.12, write $\ell(x) = c(\ell)\ell_1(x)$ where $\ell_1(x)$ is primitive. Since $\ell(x)$ is irreducible, either $c(\ell)$ or $\ell_1(x)$ is a unit. Since $\deg(\ell_1) = \deg(\ell) \geq 1$, $\ell_1(x)$ is not a unit. Thus, $c(\ell) \sim 1$. □

Theorem 2.14 (Gauss' Lemma).
Let R be a UFD. If $f(x) \neq 0$ and $g(x) \neq 0$ are in $R[x]$, then

$$c(fg) \sim c(f)c(g).$$

In particular, the product of primitive polynomials is primitive.

Proof. Let $f = c(f)f_1$ and $g = c(g)g_1$ where f_1 and g_1 are primitive. Then by Lemma 2.12,

$$c(fg) \sim c(c(f)f_1 c(g)g_1) \sim c(f)c(g)c(f_1 g_1) \sim c(f)c(g).$$

Thus, it suffices to prove that $f(x)g(x)$ is primitive when $f(x)$ and $g(x)$ are primitive, i.e. $c(f) \sim 1 \sim c(g)$. Suppose $f(x)$ and $g(x)$ are primitive, but $f(x)g(x)$ is not primitive. Since R is a UFD, there exists a prime p dividing each coefficient of $f(x)g(x)$. Write $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ and

$g(x) = b_0 + b_1x + \cdots + b_nx^n$. Since $f(x)$ and $g(x)$ are primitive, then p does not divide every a_i nor every b_j. Thus, $\exists k, s \in \mathbb{N} \cup \{0\}$ such that

(1) $p \nmid a_k$, but $p \mid a_i$ for $0 \le i < k$.

(2) $p \nmid b_s$, but $p \mid b_j$ for $0 \le j < s$.

The coefficients of x^{k+s} in $f(x)g(x)$ is $c_{k+s} = \sum\limits_{i+j=k+s} a_ib_j$. Because of (1) and (2), p divides all a_ib_j with $i + j = k + s$, except a_kb_s. It follows that $p \nmid c_{k+s}$, which is a contradiction. Thus, $f(x)g(x)$ is primitive. □

Theorem 2.15. Let R be a UFD whose field of fractioins is F. Regard $R \subseteq F$ as a subring of F as usual. If $\ell(x) \in R[x]$ is irreducible in $R[x]$, then $\ell(x)$ is irreducible in $F[x]$.

Remark. The converse is false. For example, $2x + 4$ is irreducible in $\mathbb{Q}[x]$, but $2x + 4 = 2(x + 2)$ is reducible in $\mathbb{Z}[x]$.

Proof. Let $\ell(x) \in R[x]$ be irreducible. Suppose that $\ell(x) = g(x)h(x)$ in $F[x]$. If a and b are products of the denominators of the coefficients of $g(x)$ and $h(x)$ respectively, then $g_1(x) = ag(x) \in R[x]$ and $h_1(x) = bh(x) \in R[x]$. Note that $ab\ell(x) = g_1(x)h_1(x)$ is a factorization in $R[x]$. Since $\ell(x)$ is irreducible in $R[x]$, by Lemma 2.13, $c(\ell) \sim 1$. Also, by Gauss' Lemma, we have

$$ab \sim abc(\ell) \sim c(ab\ell(x)) \sim c(g_1(x)h_1(x)) \sim c(g_1)c(h_1). \tag{$*$}$$

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

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

By $(*)$, we have $\ell(x) \sim g_2(x)h_2(x)$. Since $\ell(x)$ is irreducible in $R[x]$, it follows that $h_2(x) \sim 1$ or $g_2(x) \sim 1$. If $g_2(x) \sim 1$ in R, 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 $h_2(x) \sim 1$, then $h(x)$ 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 $F[x]$. It follows that $\ell(x)$ is irreducible in $F[x]$. □

Proposition 2.16. Let R be a UFD whose field of fractions is F. Regard $R \subseteq F$ as a subring of F. Let $f(x) \in R[x]$ with $\deg(f) \ge 1$. The following are equivalent:

(1) $f(x)$ is irreducible in $R[x]$.

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

Proof.

(1) $\implies$ (2): This follows from Lemma 2.13 and Theorem 2.15.

(2) $\implies$ (1): Suppose that $f(x)$ is primitive and irreducible in $F[x]$, but is 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 $d \nsim 1$ (if both factors have deg ≥ 1, then it would be a nontrivial factorization in $F[x]$). Since $d \mid f(x)$ and $d \nmid 1$, we have d divides each coefficient of $f(x)$, which contradicts the fact that $f(x)$ is primitive. Thus, $f(x)$ is irreducible in $R[x]$. □

Theorem 2.17. If R is a UFD, then $R[x]$ is also a UFD.

Proof. Because of Theorem 2.5 (R satisfies ACCP $\implies$ $R[x]$ satisfies ACCP) and 2.8, to prove this result, it suffices to show that every irreducible element $\ell(x)$ in $R[x]$ is prime. Let $\ell(x) \mid f(x)g(x)$ with $f(x), g(x) \in R[x]$. We aim to prove that $\ell(x) \mid f(x)$ or $\ell(x) \mid g(x)$. Note that if $\deg(\ell) = 0$, i.e. ℓ is a constant. Then, $\ell(x) \mid f(x)g(x)$ implies that $\ell \mid c(fg)$ and hence $\ell \mid c(f)c(g)$. Since ℓ is prime in R (by Proposition 2.6 since R is a UFD and ℓ is irreducible), we have $\ell \mid c(f)$ or $\ell \mid c(g)$. So $\ell \mid f(x)$ or $\ell \mid g(x)$. In the following proof, we assume that $\deg(\ell) \geq 1$.

To prove this result, it suffices to prove the following claim.

Claim. If $\ell(x) \mid f_1(x)g_1(x)$ with $f_1(x)$ and $g_1(x)$ are primitive, then $\ell(x) \mid f_1(x)$ or $\ell(x) \mid g_1(x)$.

Proof of Claim. Since $\ell(x) \mid f(x)g(x)$ for some $h(x) \in R[x]$. By Lemma 2.12, write $f(x) = c(f)f_1(x)$ and $g(x) = c(g)g_1(x)$ and $h(x) = c(h)h_1(x)$ where $f_1(x)$, $g_1(x)$, and $h_1(x)$ are primitive in $R[x]$. By Lemma 2.13 (this is where we need $\deg(\ell) \geq 1$), we have $c(\ell) \sim 1$. It follows that $c(h) \sim c(f)c(g)$. Since $c(h)h_1(x)\ell(x) = c(f)c(g)f_1(x)g_1(x)$, it follows that $h_1(x)\ell(x) \sim f_1(x)g_1(x)$. By the assumption, we have $\ell(x) \mid f_1(x)$ or $\ell(x) \mid g_1(x)$. It follows that $\ell(x) \mid f(x)$ or $\ell(x) \mid g(x)$. □

We now assume that $\ell(x) \mid f(x)g(x)$ in $R[x]$, where $f(x), g(x)$ are primitive in $R[x]$. Let F be the field of fractions of R and consider $R \subseteq F$ as a subring of F. Then, we have $\ell(x) \mid f(x)g(x)$ in $F[x]$. Since $\ell(x) \in R[x]$ is irreducible, by Theorem 2.15, $\ell(x)$ is irreducible in $F[x]$. By Euclid's lemma for $F[x]$, we have $\ell(x) \mid f(x)$ or $\ell(x) \mid g(x)$. Suppose that $\ell(x) \mid f(x)$ in $F[x]$, say $f(x) = \ell(x)k(x)$ for some $k(x) \in F[x]$. If $d \in R$ is the product of all denominators of non-zero coefficients of $k(x)$, then

$k_0(x) = dk(x) \in R[x]$ and we have $df(x) = d\ell(x)k(x) = k_0(x)\ell(x)$. Since $f(x)$ is primitive and $\ell(x)$ is irreducible (thus $c(\ell) \sim 1$), by Gauss' Lemma, we have

$$d \sim c(df) \sim c(k_0\ell) \sim c(k_0)c(\ell) \sim c(k_0).$$

If we write $k_0(x) = c(k_0)k_1(x)$ with $k_1(x) \in R[x]$, then $df(x) = k_0(x)\ell(x) = c(k_0)k_1(x)\ell(x)$. Since $d \sim c(k_0)$, it follows that $f(x) \sim k_1(x)\ell(x)$. Thus, $\ell(x) \mid f(x)$ in $R[x]$. Similarly, if $\ell(x) \mid g(x)$ in $F[x]$, then we can show that $\ell(x) \mid g(x)$ in $R[x]$. It follows that $\ell(x)$ is prime and hence $R[x]$ is a UFD. □

Note. Let R be a UFD and $x_1, \dots, x_n$ be n commutative variables, i.e. $x_ix_j = x_jx_i$ for all $i \neq j$. Define the ring $R[x_1, \dots, x_n]$ as polynomials in n variable inductively by

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

Corollary 2.18. If R is a UFD, then for all $n \in \mathbb{N}$, $R[x_1, \dots, x_n]$ is also a UFD.

Since $\mathbb{Z}$ is a UFD, we have the following.

Corollary 2.19. $\mathbb{Z}[x]$ and $\mathbb{Z}[x_1, \dots, x_n]$ are UFDs.

Remark. Hence $\mathbb{Z}[x]$ is a UFD. Since it is not a PID, we have PID $\subsetneq$ UFD.

Theorem 2.20 (**Eisenstein's Criterion**).
Let R be a UFD with the field of fractions F. Let $h(x) = c_nx^n + \cdots + c_1x + c_0 \in R[x]$ with $n \geq 1$. Let $\ell \in R$ be an irreducible element. If $\ell \nmid c_n$ and $\ell \mid c_i$ for all $0 \leq i \leq n-1$ and $\ell^2 \nmid c_0$, then $h(x)$ is irreducible in $F[x]$.

Proof. Suppose for a contradiction that $h(x)$ is irreducible in $F[x]$. By Gauss's Lemma for UFD, $\exists s(x)$ and $r(x) \in R[x]$ of degree ≥ 1 such that $h(x) = s(x)r(x)$. Write

$$s(x) = a_0 + a_1x + \cdots + a_mx^m \quad \text{and} \quad r(x) = b_0 + b_1x + \cdots + b_nx^n,$$

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

$$c_0 = a_0b_0, \quad c_1 = a_0b_1 + a_1b_0, \quad c_2 = a_0b_2 + a_1b_1 + a_2b_0, \quad \dots$$

Consider the constant term. Since $\ell \mid c_0$, we have $\ell \mid a_0b_0$. Since ℓ is irreducible and R is a UFD, we have ℓ is a prime. Hence, $\ell \mid a_0$ or $\ell \mid b_0$. WLOG, suppose that $\ell \mid a_0$. Since $\ell^2 \nmid c_0$, we have $\ell \nmid b_0$. Consider the coefficient of x. Since $\ell \mid c_1$, we ave $\ell \mid (a_0b_1 + a_1b_0)$. Since $\ell \mid a_0$, we have $\ell \mid a_1b_0$. Since $\ell \nmid b_0$, we have $\ell \mid a_1$. By repeating the above argument, the conditions on coefficients of $h(x)$ imply that $\ell \mid a_i$ for all $0 \leq i \leq m-1$. However, $\ell \nmid a_m$ since $\ell \nmid c_n$. Consider the reduction $\overline{h}(x) = \overline{s}(x)\overline{r}(x)$ in $R/_{\langle \ell \rangle}[x]$. By the assumption on the coefficients of h, we have $\overline{h}(x) = \overline{c_n}x^n$. However, since $\overline{s}(x) = \overline{a_m}x^m$ and $\ell \nmid b_0$, then $\overline{s}(x)\overline{r}(x)$ contains the term $\overline{a_mb_0}x^m$, which leads to a contradiction. So, $h(x)$ is irreducible in $F[x]$. □

Example. Consider $2x^7 + 3x^4 + 6x^2 + 12$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion with $\ell = 3$.

Example. Let p be a prime. Let $\zeta_p = e^{\frac{2\pi i}{p}} = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right)$ be a p-th root of 1. It is a root of the <u>p-th cyclotomic polynomial</u>:

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

Eisenstein's Criterion does not imply directly that $\Phi_p(x)$ is irreducible. However, we can consider

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

Since p is a prime, we know that $p \nmid 1$, $p \mid \binom{p}{i}$ for all $1 \leq i \leq p-1$ and $p^2 \nmid \binom{p}{p-1}$. Thus by Eisenstein's Criterion, $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$.

Note. Since $\Phi_p(x)$ is primitive, it is irreducible in $\mathbb{Z}[x]$.

3 Field Extensions

Lecture 9, 2025/01/24

3.1 Degree of Extensions

Definition 3.1 (**Field Extension**). If E is a field containing another field F, we say that E is a **field extension** of F, denoted by ${}^{E}\!/_{F}$.

Remark. Note that the notation ${}^{E}\!/_{F}$ is NOT used to denote a quotient ring as the field E has no ideals other than $\{0\}$ and E itself.

Remark. If ${}^{E}\!/_{F}$ is a field extention, we can view E as a vector space over F:

(1) **Addition**: For $e_1, e_2 \in E$, $e_1 \oplus e_2 := e_1 + e_2$ (addition of E).

(2) **Scalar Multiplication**: For $c \in F$ and $e \in E$, $c \odot e := ce$ (multiplication of E).

Definition 3.2 (**Degree, Finite/Infinite Extension**).
The dimension of E over F (viewed as a vector space) is called the **degree** of E over F, denoted by $[E : F]$. If $[E : F] < \infty$, we say that ${}^{E}\!/_{F}$ is a **finite extension**. Otherwise, ${}^{E}\!/_{F}$ is an **infinite extension**.

Example. $[\mathbb{C} : \mathbb{R}] = 2$ is a finite extension, since $\mathbb{C} \cong \mathbb{R} + \mathbb{R}i$ ($\mathbb{C} = \mathrm{Span}\{1, i\}$ over $\mathbb{R}$).

Example. Let F be a field. Define $F[x]$ as usual. Then define

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

to be the field of fractions of $F[x]$. Then $[F(x) : F] = \infty$ since $\{1, x, x^2, \ldots\}$ is linearly independent over F.

Theorem 3.1. If E/K and K/F are finite field extensions, then ${}^{E}\!/_{F}$ is a finite extension. Moreover, we have

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

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

Proof. Suppose $[E : K] = m$ and $[K : F] = n$. Let $\{a_1, \dots, a_m\}$ be a basis of E/K and $\{b_1, \dots, b_n\}$ be a basis of K/F. It suffices to prove that $\mathcal{C} = \{a_i b_j : 1 \le i \le m, 1 \le j \le n\}$ is a basis of E/F.

Claim (1). $\operatorname{Span}_F \mathcal{C} = E$. That is, every element of E is a linear combination of $\{a_i b_j\}$ over F.

Proof of Claim (1). For $e \in E$, we have $e = \sum_{i=1}^{m} k_i a_i$ with $k_i \in K$. For each $k_i \in K$, we have $k_i = \sum_{j=1}^{n} c_{ij} b_j$ with $c_{ij} \in F$. Thus, it follows that $e = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} b_j a_i$. It follows that Span $\mathcal{C} = E$. □

Claim (2). $\mathcal{C}$ is linearly independent over F.

Proof of Claim (2). Suppose that $\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} a_i b_j = 0$ for some $c_{ij} \in F$. Since $\sum_{j=1}^{n} c_{ij} b_j \in K$ and $\{a_1, \dots, a_m\}$ is linearly independent over K, so we have $\sum_{j=1}^{n} c_{ij} b_j = 0$ for all i. Since $\{b_1, \dots, b_n\}$ is linearly independent over F, we have $c_{ij} = 0$ for all i, j. Therefore, $\mathcal{C}$ is linearly independent over F. □

Combining the two claims, we have that $\mathcal{C}$ is a basis of E/F and $[E : F] = mn = [E : K][K : F]$. □

3.2 Algebraic and Transcendental Extensions

Definition 3.3 (Algebraic, Transendental).
Let E/F be a field extension and $\alpha \in E$. We say that α is **algebraic** over F if $\exists f(x) \in F[x] \setminus \{0\}$ with $f(\alpha) = 0$. Otherwise, we say that α is **transcendental** over F.

Example. $\frac{c}{d} \in \mathbb{Q}$ (root of $f(x) = dx - c$) and $\sqrt{2}$ (root of $f(x) = x^2 - 2$) are algebraic over $\mathbb{Q}$. However, π and e are transcendental over $\mathbb{Q}$.

Example.

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

Proof. To prove this claim, write $\alpha - \sqrt{2} = \sqrt{3}$. By squaring both sides, we have

$$\alpha^2 - 2\sqrt{2}\alpha + 2 = 3 \implies \alpha^2 - 1 = 2\sqrt{2}\alpha \implies \alpha^4 - 2\alpha^2 + 1 = 8\alpha^2 \implies \alpha^4 - 10\alpha^2 + 1 = 0.$$

It follows that α is a root of $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$, hence, α is algebraic over $\mathbb{Q}$. $\square$

Let E/F be a field extension and $\alpha \in E$. Let $F[\alpha]$ denote the smallest subring of E containing F and α, and we use $F(\alpha)$ to denote the smallest subfield of E containing F and α. For $\alpha, \beta \in E$, we define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ similarly.

Definition 3.4 (Simple Extension).
If $E = F(\alpha)$ for some $\alpha \in E$, we say that E/F is a **simple extension**.

Definition 3.5 (F-Homomorphism).
Let R and R_1 be two rings which contain a field F. A ring homomorphism $\varphi : R \to R_1$ is said to be an F-**homomorphism** if $\varphi|_F = 1_F$. That is, $\varphi(x) = x$ for all $x \in F$.

Theorem 3.2. Let E/F be a field extension and $\alpha \in R$. If α is transcendental over F, then we have

$$F[\alpha] \cong F[x] \quad \text{and} \quad F(\alpha) \cong F(x).$$

In particular, $F[\alpha] \neq F(\alpha)$.

Proof. Let $\varphi : F(x) \to F(\alpha)$ be the unique F-homomorphism defined by $\varphi(x) = \alpha$. Thus, for $f(x), g(x) \in F[x]$ and $g(x) \neq 0$, we have

$$\varphi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)} \in F(\alpha).$$

Since α is transcendental, we have $g(\alpha) \neq 0$ for all $g(x) \in F[x]$. Thus, this map is well-defined. Since $F(x)$ is a field and $\operatorname{Ker}\varphi$ is an ideal of $F(x)$, we have that $\operatorname{Ker}\varphi = \{0\}$ or $\operatorname{Ker}\varphi = F(x)$. Since φ is not the zero map because $\varphi(x) = \alpha \neq 0$, we have $\operatorname{Ker}\varphi = \{0\}$ and therefore φ is injective. Also, since $F(x)$ is a field, $\operatorname{im}\varphi$ contains a field generated by F and α. Since $F(\alpha)$ is the smallest field containing F and α, we must have $F(\alpha) \subseteq \operatorname{im}\varphi$. Thus, φ is surjective and therefore an isomorphism. It follows that $F(x) \cong F(\alpha)$ and $F[x] \cong F[\alpha]$. $\square$

Lecture 10, 2025/01/27

Theorem 3.3. Let ${}^{E}\!/_{F}$ be a field extension and $\alpha \in E$. If α is algebraic over F, then there exists a unique monic irreducible polynomial $p(x) \in F[x]$ such that there exists an F-isomorphism

$$\varphi : {}^{F[x]}\!/_{\langle p(x)\rangle} \to F[\alpha] \quad \text{with } \varphi(x) = \alpha.$$

From there we conclude that $F[\alpha] = F(\alpha)$.

Remark. Since α is algebraic, the map defined in the proof of previous theorem, $\frac{f(x)}{g(x)} \mapsto \frac{f(\alpha)}{g(\alpha)}$ is NOT well-defined.

Proof. Consider the unique F-homomorphism $\varphi : F[x] \to F(\alpha)$ by $\varphi(x) = \alpha$. Thus, for $f(x) \in F[x]$, we have $\varphi(f(x)) = f(\alpha) \in F[\alpha]$. Since $F[x]$ is a ring, $\operatorname{im}\varphi$ contains a ring generated by F and α. That is, $F[\alpha] \subseteq \operatorname{im}\varphi$ and thus $\operatorname{im}\varphi = F[\alpha]$. Consider

$$I = \operatorname{Ker}\varphi = \{f(x) \in F[x] : f(\alpha) = 0\}.$$

Since α is algebraic, $I \neq \{0\}$. Theorefore, by the First Ring Isomorphism Theorem, ${}^{F[x]}\!/_{I} \cong F[\alpha]$. Note that $\operatorname{im}\varphi$ is a subring of the field $F(\alpha)$. Thus, $\operatorname{im}\varphi$ is an integral domain and it follows that ${}^{F[x]}\!/_{I}$ is an integral domain. This implies that I is a prime ideal and say $I = \langle p(x)\rangle$ where $p(x)$ is irreducible. If we assume $p(x)$ is monic, then it is unique. It follows that

$${}^{F[x]}\!/_{\langle p(x)\rangle} \cong F[\alpha].$$

Since $F[x]$ is a PID, the prime ideal $\langle p(x)\rangle$ is maximal. Thus, ${}^{F[x]}\!/_{\langle p(x)\rangle}$ is a field and hence $F[\alpha]$ is a field. Since $F[\alpha]$ is the smallest field containing F and α, we have $F[\alpha] = F(\alpha)$. $\square$

Definition 3.6 (Minimal Polynomial).

If α is algebraic over a field F, the unique monic irreducible polynomial $p(x)$ in Theorem 3.3 is called the **minimal polynomial** of α over F.

As a direct consequence of the above two theorems, we have the following.

Theorem 3.4. Let ${}^{E}\!/_{F}$ be a field extension and $\alpha \in E$.

(1) α is transcendental over $F \iff [F(\alpha) : F] = \infty$.

(2) α is algebraic over $F \iff [F(\alpha) : F] < \infty$.

Moreover, if $p(x)$ is the minimal polynomial of α over F, we have

$$[F(\alpha) : F] = \deg(p(x))$$

and $\{1, a, a^2, \dots, a^{\deg(p(x))-1}\}$ is a basis of ${}^{F(\alpha)}\!/_{F}$.

Proof. It suffices to prove the $(\Rightarrow)$ in (1) and (2) since the $(\Leftarrow)$ comes from taking the contrapositive.

(1) $(\Rightarrow)$: By Theorem 3.2, if α is transcendental over F, then $F(\alpha) \cong F(x)$. In $F(x)$, the elements $\{1, x, x^2, \dots\}$ are linearly independent over F. Thus, $[F(\alpha) : F] = \infty$.

(2) $(\Rightarrow)$: By Theorem 3.3, if α is algebraic over F, then $F(\alpha) \cong {}^{F[x]}\!/_{\langle p(x)\rangle}$ with $x \mapsto \alpha$. Note that ${}^{F[x]}\!/_{\langle p(x)\rangle} \cong \{r(x) \in F[x] : \deg(r) < \deg(p)\}$. Thus, $\{1, x, \dots, x^{\deg(p)-1}\}$ is a basis of ${}^{F[x]}\!/_{\langle p(x)\rangle}$. It follows that $[F(\alpha) : F] = \deg(p)$ and $\{1, \alpha, \dots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)$ over F.

$\square$

Example. Let p be a prime and $\zeta_p = e^{2\pi i/p}$, a p-th root of unity. We have seen in Chapter 2 that ζ_p is a root of the p-th cyclotomic polynomial $\Phi_p(x)$, which is irreducible. Thus, by Theorem 3.4, $\Phi_p(x)$ is the minimal polynomial of ζ_p over $\mathbb{Q}$ and $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg(\Phi_p) = p-1$. The field $\mathbb{Q}(\zeta_p)$ is called the p-th cyclotomic field of $\mathbb{Q}$.

Example. Let $\alpha = \sqrt{2}+\sqrt{3}$. We recall that α is a root of x^4-10x^2+1. Note that $(\alpha-\sqrt{2})^2 = 3$. We have $\alpha^2 - 2\sqrt{2}\alpha + 2 = 3$. Hence, $\sqrt{2} = \frac{\alpha^2-1}{2\alpha}$ is an element in $\mathbb{Q}(\alpha)$. Since $\sqrt{2}$ is a root of x^2-2, which is irreducible, we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Also, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (see Piazza). Hence, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \geq 2$, since $\alpha = \sqrt{2}+\sqrt{3}$. Since α is a root of a polynomial of degree 4, it follows that $4 \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \geq 2 \cdot 2 = 4$. Hence, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $x^4 - 10x^2 + 1$ is the minimal polynomial of α over $\mathbb{Q}$.

Exercise: Can we show that $x^4 - 10x^2 + 1$ is irreducible using Eisenstein's criterion?

Theorem 3.5. Let ${}^{E}\!/\!_{F}$ be a field extension. If $[E : F] < \infty$, $\exists \alpha_1, \dots, \alpha_n \in E$ s.t.

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

Thus, to understand a finite extension, it suffices to understand a finite simple extension.

Proof. We will prove this theorem 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 $\alpha_1 \in E \setminus F$. By Theorem 3.1, $[E : F] = [E : F(\alpha_1)] \cdot [F(\alpha_1) : F]$. Since $[F(\alpha_1) : F] > 1$, we have $[E : F(\alpha_1)] < [E : F]$. By induction hypothesis, $\exists \alpha_2, \alpha_3, \dots, \alpha_n \in E$ s.t.

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

Thus, we have $F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq F(\alpha_1, \dots, \alpha_n) = E$. $\square$

Definition 3.7 (Algebraic, Transcendental).
A field extension ${}^{E}\!/\!_{F}$ is **algebraic** if every $\alpha \in E$ is algebraic over F. Otherwise, it is called **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. Then, $\exists c_i \in F$ $(0 \le i \le n)$, not all 0, such that

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

Thus, α is a root of the polynomial $\sum_{i=0}^{n} c_i x^i \in F[x]$, hence it is algebraic over F. □

Theorem 3.7. Let ${}^{E}\!/_{F}$ be a field extension. Define

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

Then, L is an intermediate field of ${}^{E}\!/_{F}$.

Proof. If $\alpha, \beta \in L$, we need to show that $\alpha \pm \beta$, $\alpha\beta$ and ${}^{\alpha}\!/_{\beta}(\beta \neq 0) \in L$. By the definition of L, we have $[F(\alpha) : F] < \infty$ and $[F(\beta) : F] < \infty$. Consider the field $F(\alpha, \beta)$. Since the minimal polynomial of α over $F(\beta)$ divides the minimal polynomial of α over F (the minimal polynomial of α over F, say $p(x) \in F[x]$, is also a polynomial over $F(\beta)$, i.e.$p(x) \in F(\beta)[x]$ s.t. $p(\alpha) = 0$), we have $[F(\alpha, \beta) : F(\beta)] \le [F(\alpha) : F]$. Combining this with Theorem 3.1, we have

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

Since $\alpha + \beta \in F(\alpha, \beta)$, it follows that $[F(\alpha + \beta) : F] \le [F(\alpha, \beta) : F] < \infty$, i.e. $\alpha + \beta \in L$. Similarly, we can show that $\alpha - \beta$, $\alpha\beta$ and ${}^{\alpha}\!/_{\beta}(\beta \neq 0) \in L$. □

Definition 3.8 (Algebraic Closure).
Let ${}^{E}\!/_{F}$ be a field extension. Then we say

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

is the **algebraic closure** of F in E.

Definition 3.9 (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.

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

Since $\zeta_p \in \overline{\mathbb{Q}}$, we have

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

Since $p \to \infty$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Hence, the converse of Theorem 3.6 is false.

4 Splitting Fields

Lecture 12, 2025/01/31

4.1 Existence of Splitting Fields

Definition 4.1 (**Split Over**). Let ${}^{E}\!/_{F}$ be a field extension. We say that $f(x) \in F[x]$ **splits over** E if E contains all roots of $f(x)$, i.e. $f(x)$ is a product of linear factors in $E[x]$.

Definition 4.2 (**Splitting Field**).
Let ${}^{\tilde{E}}\!/_{F}$ be a field extension, $f(x) \in F[x]$ and $F \subseteq E \subseteq \tilde{E}$. If

(1) $f(x)$ splits over E.

(2) There is no proper subfield of E such that $f(x)$ splits over it.

Then, we say 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, the ideal $I = \langle p(x)\rangle$ is maximal (since $F[x]$ is a PID). Thus, $E = {}^{F[x]}\!/_{I}$ is a field. Consider the map $\phi : F \to E$ given by $a \mapsto a + I$. Since F is a field and $\phi \neq 0$, we get that ϕ is injective. Thus, $F \cong \phi(F) \subseteq E$. By identifying F with $\phi(F)$, F can be viewed as a subfield of E. Let $\alpha = x + I \in E$. We claim that α is a root of $p(x)$. Write

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

Then, we have

$$\begin{aligned}
p(\alpha) &= (a_0 + I) + (a_1 + I)\alpha + \cdots + (a_n + I)\alpha^n \\
&= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\
&= (a_0 + I) + (a_1 x + I) + \cdots + (a_n x^n + I) \quad \text{since } (x + I)^k = x^k + I \\
&= (a_0 + a_1 x + \cdots + a_n x^n) + I \\
&= p(x) + I = 0 + I.
\end{aligned}$$

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

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. We prove this theorem by induction on $\deg(f)$. If $\deg(f) = 1$, then we let $E = F$ and we are done. If $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$ ($g(x)$ is not necessarily in $F[x]$). Write $f(x) = p(x)h(x)$ with $p(x), h(x) \in F[x]$ and $p(x)$ is irreducible. By Theorem 4.1, there exists a field K such that $F \subseteq K$ and K contains a root of $p(x)$, say α. Thus, $p(x) = (x - \alpha)q(x)$ and $f(x) = (x - \alpha)h(x)q(x)$ with $h(x) \in K[x]$. Since $\deg(hq) < \deg(f)$, by induction, there exists a field E containing K over which $h(x)q(x)$ splits. It follows that $f(x)$ splits over E. $\square$

Theorem 4.3. Every $f(x) \in F[x]$ has a splitting field which is a finite extension of F.

Proof. Let $f(x) \in F[x]$, by Theorem 4.2, there is a field extension ${}^{E}\!/_{F}$ over which $f(x)$ splits, say $\alpha_1, \dots, \alpha_n$ are roots of $f(x)$ in E. Consider $F(\alpha_1, \dots, \alpha_n)$. This is the smallest subfield of E containing all roots of $f(x)$. So $f(x)$ does not split over any proper subfield of it. Thus, $F(\alpha_1, \dots, \alpha_n)$ is the splitting field of $f(x)$ in E. Moreover, since α_i are all algebraic, ${}^{F(\alpha_1, \dots, \alpha_n)}\!/_{F}$ is a finite extension. $\square$

Example. Consider $x^3 - 2$ in $\mathbb{Q}[x]$. We have

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta_3)(x - \sqrt[3]{2}\zeta_3^2).$$

So, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

Remark. If $f(x)$ splits in E, i.e. $\alpha_1, \dots, \alpha_n$ are roots of $f(x)$ in E, then $F(\alpha_1, \dots, \alpha_n)$ is the splitting field of $f(x)$ in E.

4.2 Uniqueness of Splitting Fields

We have seen that for the field extension ${}^{E}\!/_{F}$, $F(\alpha_1, \dots, \alpha_n)$ is the splitting field of $f(x) \in F[x]$ in E and it is unique with E.

Question: If we change ${}^{E}\!/_{F}$ to a different field extension, say ${}^{E_1}\!/_{F}$, what is the relation between the splitting field of $f(x)$ in E and the one in E_1?

Definition 4.3 (**Extend**). Let $\phi : R \to R_1$ be a ring homomorphism and $\Phi : R[x] \to R_1[x]$ be the unique homomorphism satisfying $\Phi|_R = \phi$ and $\Phi(x) = x$. In this case, we say Φ **extends** ϕ. More generally, if $R \subseteq S$ and $R_1 \subseteq S_1$ and $\Phi : S \to S_1$ is a ring homomorhpism with $\Phi|_R = \phi$, we say Φ **extends** ϕ.

Theorem 4.4. Let $\phi : F \to F_1$ be an isomorphism of fields and $f(x) \in F[x]$. Let $\Phi : F[x] \to F_1[x]$ be the unique ring isomorphism which extends ϕ. Let $f_1(x) = \Phi(f(x))$ and ${}^{E}\!/_{F}$ and ${}^{E_1}\!/_{F_1}$ be the splitting fields of $f(x)$ and $f_1(x)$ in F and F_1, respectively. Then, there exists an isomorphism $\psi : E \to E_1$ which extends ϕ.

Corollary 4.5. Any two splitting fields of $f(x) \in F[x]$ over F are F-isomorphisic.

Lecture 13, 2025/02/03

Proof of Theorem 4.4. We prove this theorem by induction on $[E : F]$. If $[E : F] = 1$, then $f(x)$ is a product of linear function in $F[x]$ and so is $f_1(x)$ in $F_1[x]$. Thus, $E = F$ and $E_1 = F_1$. Take $\psi = \phi$, and we are done.

Suppose that $[E : F] > 1$ and the statement is true for all field extension ${}^{\tilde{E}}\!/_{\tilde{F}}$ with $[\tilde{E} : \tilde{F}] < [E : F]$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with $\deg(p) \geq 2$ and let $p_1(x) = \Phi(p(x))$ (such $p(x)$ exists as if all irreducible factors of $f(x)$ are of degree 1, then $[E : F] = 1$). 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 an F-isomorphism

$$F(\alpha) \cong {}^{F[x]}\!/_{\langle p(x) \rangle} \quad \alpha \mapsto x + \langle p(x) \rangle \,.$$

Similarly there is an F-isomorphism

$$F_1(\alpha_1) \cong {}^{F_1[x]}\!/\!_{\langle p_1(x)\rangle} \quad \alpha_1 \mapsto x + \langle p_1(x)\rangle\,.$$

Consider the isomorphism $\Phi : F[x] \to F_1[x]$ which extends ϕ. Since $p_1(x) = \Phi(p(x))$, there exists a field isomorphism

$$\tilde{\Phi} : {}^{F[x]}\!/\!_{\langle p(x)\rangle} \to {}^{F_1[x]}\!/\!_{\langle p_1(x)\rangle} \quad x + \langle p(x)\rangle \mapsto x + \langle p_1(x)\rangle$$

which extends ϕ. It follows that there exists an isomorphism

$$\tilde{\phi} : F(\alpha) \to F_1(\alpha_1) \quad \alpha \mapsto \alpha_1$$

which extends ϕ. Note that since $\deg(p) \geq 2$, $[E : F(\alpha)] < [E : F]$. Since E (respectively E_1) is the splitting field of $f(x) \in F(\alpha)[x]$ (respectively $f_1(x) \in F_1(\alpha_1)[x]$), by induction, there exists $\psi : E \to E_1$ which extends $\tilde{\phi}$. Thus, ψ extends ϕ. □

Remark. By taking $\phi : F \to F$ to be the identity map in Theorem 4.4, we obtain Corollary 4.5.

4.3 Degrees of Splitting Fields

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

Proof. We prove this by induction on $\deg(f)$. If $\deg(f) = 1$, choose $E = F$ and we have $[E : F] \mid 1!$. Suppose that $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$ ($g(x)$ is not necessarily in $F[x]$). Two cases:

(1) If $f(x) \in F[x]$ is irreducible and $\alpha \in E$ is a root of $f(x)$ by Theorem 3.3,

$$F(\alpha) \cong {}^{F[x]}\!/\!_{\langle f(x)\rangle} \text{ and } [F(\alpha) : F] = \deg(f) = n.$$

Write $f(x) = (x - \alpha)g(x) \in F(\alpha)[x]$ with $g(x) \in F(\alpha)[x]$. Since E is the splitting field of $g(x)$ over $F(\alpha)$ and $\deg(g) = n - 1$, by induction, $[E : F(\alpha)] \mid (n-1)!$. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, it follows that $[E : F] \mid n!$.

(2) If $f(x)$ is not irreducible, write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, $\deg(g) = m$, $\deg(h) = k$, $m + k = n$ and $1 \le m, k < n$. 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 and $\deg(h) = k$, by induction, $[E : K] \mid k!$. Thus, $[E : F] = [E : K][K : F] \mid m!k!$, which is a factor of $n!$ (since $\frac{n!}{m!k!} = \binom{n}{m} \in \mathbb{Z}$).

$\square$

5 More Field Theory

5.1 Prime Fields

Definition 5.1 (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, then its prime field is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p.

Definition 5.2 (Characteristic). Given a field F, if its prime field is isomorphic to $\mathbb{Q}$ (respectively $\mathbb{Z}_p$), we say F has **characteristic** 0 (respectively characteristic p), denoted by $\mathrm{ch}(F) = 0$ (respectively $\mathrm{ch}(F) = p$).

Note. If $\mathrm{ch}(F) = p$, for $a, b \in F$,

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

The last equality follows since $\binom{p}{i}$ $(1 \leq i \leq p-1)$ are divisible by p and hence 0.

Lecture 14, 2025/02/5

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

$$\chi : \mathbb{Z} \to F_1 \quad n \mapsto n \cdot 1 \quad \text{where } 1 \in F_1 \subseteq F.$$

Let $I = \operatorname{Ker}\chi$ be the kernel of χ. Since $\mathbb{Z}/I \cong \operatorname{im}\chi$ (by the First Ring Isomorphism Theorem), a subring of F_1, it is an integral domain. Thus, I is a prime ideal. Two cases.

(1) If $I = \langle 0 \rangle$, then $\mathbb{Z} \subseteq F_1$. Since F_1 is a field, $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z}) \subseteq F_1$.

(2) If $I = \langle p \rangle$, by the First Ring Isomorphism Theorem, then $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle \cong \operatorname{im}\chi \subseteq F_1$.

□

Note that if $\mathrm{ch}(F) = p$, we have $(a+b)^p = a^p + b^p$. Using this, we can prove the following.

Proposition 5.2. Let F be a field with $\mathrm{ch}(F) = p$ and let $n \in \mathbb{N}$. Then, the map $\varphi : F \to F$ given by $u \mapsto u^p$ is an injective $\mathbb{Z}_p$-homomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-isomorphism of F.

5.2 Formal Derivatives and Repeated Roots

Definition 5.3 (**Formal Derivative**).

If F is a field, the monomials $\{1, x, x^2, \ldots\}$ form an F-basis of $F[x]$. Define the linear operator $D : F[x] \to F[x]$ by $D(1) = 0$ and $D(x^i) = ix^{i-1}$ for $i \in \mathbb{N}$. Thus, for $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where $a_i \in F$,

$$D(f(x)) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

One can check that we have the following properties.

(1) $D(f + g) = D(f) + D(g)$.

(2) (Leibniz Rule) $D(fg) = D(f)g + fD(g)$.

We call $D(f) = f'$ the **formal derivative** of $f(x)$.

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

(1) If $\mathrm{ch}(F) = 0$, then $f'(x) = 0 \iff f(x) = c$ for some $c \in F$.

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

Proof.

(1) ($\Leftarrow$): is clear.

($\Rightarrow$): For $f(x) = a_0 + a_1x + \cdots a_nx^n$, we have $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} = 0$ implying that $ia_i = 0$ for $1 \leq i \leq n$. Since $\mathrm{ch}(F) = 0$, we have $i \neq 0$. Thus, $a_i = 0$ for $1 \leq i \leq n$ and $f(x) = a_0 \in F$.

(2) ($\Leftarrow$): Write $g(x) = b_0 + b_1x + \cdots + b_mx^m \in F[x]$. Then, $f(x) = g(x^p) = b_0 + b_1x^p + \cdots + b_mx^{pm}$. Thus, $f'(x) = pb_1x^{p-1} + 2pb_2x^{2p-1} + \cdots + pmb_mx^{pm-1}$. Since $\mathrm{ch}(F) = p$, we have $f'(x) = 0$.

($\Rightarrow$): For $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} = 0$ implies that $ia_i = 0$ for $1 \leq i \leq n$. Since $\mathrm{ch}(F) = p$, $ia_i = 0$ implies that $a_i = 0$ unless $p \mid i$. Thus,

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

where $g(x) = a_0 + a_px + \cdots + a_{mp}x^m \in F[x]$. $\square$

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

Proof.
($\Rightarrow$): Suppose $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in E[x]$. Then,

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

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

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

$$f'(x) = h(x) + (x-\alpha)h'(x).$$

Since $f'(\alpha) = 0$, we have $h(\alpha) = 0$. Thus, $(x-\alpha)$ is a factor of $h(x)$ and $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in E[x]$. $\square$

Definition 5.5 (**Separable**). Let F be a field and $f(x) \in F[x] \setminus \{0\}$. 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 $f(x) \in F[x] \setminus \{0\}$. $f(x)$ is separable $\iff \gcd(f, f') = 1$.

Remark. We note that the condition of repeated roots depends on the extension of F, while the gcd condition involves only F.

Proof. Note that $\gcd(f, f') \neq 1 \iff (x-\alpha) \mid \gcd(f, f')$ for some α in some extension of F. By Theorem 5.4, the result follows. $\square$

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

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

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

Suppose that $r(x)$ is not separable. Then, by Corollary 5.5, $\gcd(r, r') \neq 1$. Thus, $r'(x) = 0$. Since $\mathrm{ch}(F) = 0$, from Theorem 5.3, $r'(x) = 0$ implies that $r(x) = c \in F$, a contradiction since $\deg(r) \geq 1$. Thus, $r(x)$ is separable. $\square$

Example. The p-th cyclotonic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$ and hence separable. We recall that the roots of $\Phi_p(x)$ are $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$, which are all distinct.

Lecture 15, 2025/02/7

5.3 Finite Fields

Given a field F, let $F^* = F \setminus \{0\}$ be the multiplicative group of non-zero elements of F.

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

Proof. Since F is a finite field, by Theorem 5.1, its prime field is $\mathbb{Z}_p$. Since F is a finite dimentional vector space over $\mathbb{Z}_p$, say $\dim_{\mathbb{Z}_p} F = n$, then we know that

$$F \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ times}} \cong \mathbb{Z}_p^n$$

as vector spaces. This means that $|F| = p^n$. $\square$

Theorem 5.8. Let F be a field and G a finite subgroup of F^*. Then, G is a cyclic group. In particular, if F is a finite field, then F^* is a cyclic group.

Proof. WLOG, we can assume $G \neq \{1\}$. Since G is a finite abelian group, by the Fundamental Theorem of Finite Abelian Groups, we have

$$G \cong \mathbb{Z}/_{n_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{n_r\mathbb{Z}}$$

with $n_1 > 1$ and $n_1 \mid n_2 \mid \cdots \mid n_r$. Since $n_r(\mathbb{Z}/_{n_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{n_r\mathbb{Z}}) = 0$, it follows that every $u \in G$ is a root of $x^{n_r} - 1 \in F[x]$. Since the polynomial has at most n_r distinct roots in F, we have $r = 1$ and $G \cong \mathbb{Z}/_{n_r\mathbb{Z}}$. □

By taking u to be a generator of the multiplicative group F^*, we have the following.

Corollary 5.9. If F is a finite field, then F is a simple extension of $\mathbb{Z}_p$, i.e. $F = \mathbb{Z}_p(u)$ for some $u \in F^*$.

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

(1) F is a field with $|F| = p^n \iff F$ is a 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 $m \mid n$. Then, F contains a unique subfield K with $|K| = p^m$.

Proof.

(1) ($\Rightarrow$): If $|F| = p^n$, then $|F^*| = p^n - 1$. Then, every $u \in F^*$ satisfies $u^{p^n-1} = 1$. Thus, u is a root of $x(x^{p^n-1} - 1) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Since $0 \in F$ is also a root of $x^{p^n} - x$, the polynomial $x^{p^n} - x$ has p^n distinct roots in F, that is, it splits over F. Thus, F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

($\Leftarrow$): Suppose F is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Since $\mathrm{ch}(F) = p$, we have $f'(x) = -1$. Then, $\gcd(f, f') = 1$ which means $f(x)$ is separable and has p^n distinct roots in F by Corollary 5.5. Let E be the set of all roots of $f(x)$ in F and define

$$\varphi : F \to F \quad u \mapsto u^{p^n}.$$

For $u \in F$, u is a root of $f(x) \iff \varphi(u) = u$. Since the condition is closed under addition, subtraction, multiplication and division, the set E is a subfield of F of order p^n which contains $\mathbb{Z}_p$ (since all $u \in \mathbb{Z}_p$ satisfies $u^{p^n} = u$). Since F is the splitting field, it is generated over $\mathbb{Z}_p$ by the roots of $f(x)$, that is, the elements of E. Thus, $F = \mathbb{Z}_p(E) = E$.

(2) We recall that

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

Then if $n = mk$, we have

$$x^{p^n} - x = x(x^{p^n - 1} - 1) = x(x^{p^m - 1} - 1)g(x) = x(x^{p^m} - x)g(x)$$

for some $g(x) \in \mathbb{Z}_p[x]$. Since $x^{p^n} - x$ splits over F, so does $x^{p^m} - x$. Let

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

Thus, $|K| = p^m$, since $u^{p^m} - u$ is separable (we can see this by taking the derivative), so the roots are distinct. Also, by (1), K is a field. Note that if $K \subseteq F$ is any subfield with $|K| = p^m$, then $\tilde{K} \subseteq K$ since all elements $v \in \tilde{K}$ satisfies $v^{p^m} = v$. It follows that $\tilde{K} = K$ since they have the same size. Thus, we see that a subfield K of F with $|K| = p^m$ is unique.

□

As a direct consequence of Theorem 5.10, we have the following.

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 will denote such a field by $\mathbb{F}_{p^n}$.

Corollary 5.12. Let F be a finite field with $\mathrm{ch}(F) = p$. Then,

(1) $F = F^p = \{x^p : x \in F\}$.

(2) Every irreducible $r(x) \in F[x]$ is separable.

Proof.

(1) 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 $n \in \mathbb{N}$. Then for every $a \in F$, $a = a^{p^n} = (a^{p^{n-1}})^p$. Since $a^{p^{n-1}} \in F$, we have $F = F^p$.

(2) Let $r(x) \in F[x]$ be irreducible. Then,

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

Suppose that $r(x)$ is not separable. Then, by Corollary 5.5, $\gcd(r, r') \neq 1$. Thus, $r'(x) = 0$. Since $\mathrm{ch}(F) = p$, from Theorem 5.3, $r'(x) = 0$ implies that

$$r(x) = a_0 + a_p x^p + \cdots + a_{mp} x^{mp}$$

for some $a_i \in F$. Since $F = F^p$, we can write $a_i = b_i^p$. Thus,

$$r(x) = b_0^p + b_1^{p^2} x^p + \cdots + b_m^{p^{m+1}} x^{mp} = (b_0 + b_1 x + \cdots + b_m x^m)^p$$

which is a contradiction since $r(x)$ is irreducible. Thus, $r(x)$ is separable.

□

Example. Let $\mathrm{ch}(F) = p$ and consider $f(x) = x^p - a$. Since $f'(x) = px^{p-1} = 0$, we have $\gcd(f, f') \neq 1$. By Corollary 5.5, $f(x)$ is not separable. Define $F^p = \{b^p : b \in F\}$, which is a subfield of F.

(1) If $a \in F^p$, say $a = b^p$ for some $b \in F$, then $f(x) = x^p - b^p = (x - b)^p \in F[x]$. This has repeated roots so it is not separable, but this is reducible in $F[x]$.

(2) Suppose $a \notin F^p$. Let E/F be an extension where $x^p - a$ has a root, say $\beta \in E$. Hence,

we have $\beta^p - a = 0$. Note that since $a = \beta^p \notin F^p$, we know that $\beta \notin F$. We have $x^p - a = x^p - \beta^p = (x - \beta)^p$, which is not separable.

Claim. $f(x) = x^p - a$ is irreducible in $F[x]$ when $a \notin F^p$.

Proof. Write $x^p - a = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ are monic polynomials. We have seen that $x^p - a = (x - \beta)^p$. Thus, $g(x) = (x - \beta)^r$ and $h(x) = (x - \beta)^s$ for some $r, s \in \mathbb{N} \cup \{0\}$ with $r + s = p$. Write

$$g(x) = (x - \beta)^r = x^r - r\beta x^{r-1} + \cdots + (-\beta)^r.$$

Then, $r\beta \in F$. Since $\beta \notin F$, as an element of F, we have $r = 0_F$ in F. Thus, as an integer, $r = 0$ or $r = p$. It follows that either $g(x) = r$ or $h(x) = 1$ in $F[x]$. Thus, $f(x)$ is irreducible in $F[x]$. $\square$

6 Solvable Groups and Automorphism Groups

6.1 Solvable Groups

Definition 6.1 (**Solvable**)**.** A group G is **solvable** if there exists a tower:

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

with $G_{i+1} \lhd G_i$ and ${}^{G_i}\!/_{G_{i+1}}$ abelian for all $0 \leq i \leq m-1$.

Remark. G_{i+1} is not necessarily a normal subgroup of G. However, if G_{i+1} is a normal subgroup of G, we get $G_{i+1} \lhd G_i$ for free.

Example. Consider the symetric group S_4. Let A_4 be the alternating group of S_4 and $V \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$, the Klein 4-group. Note that A_4 and V are normal subgroups of S_4. We have

$$S_4 \supseteq A_4 \supseteq V \supseteq \{1\}.$$

Since ${}^{S_4}\!/_{A_4} \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ and ${}^{A_4}\!/_{V} \cong {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$. Both of them are abelian, so S_4 is solvable.

Theorem 6.1 (**Second Isomorphism Theorem**)**.**
Let H and K be subgroups of a group G with $K \lhd G$. Then, HK is a subgroup of G, $K \lhd HK$, $H \cap K \lhd H$ and

$${}^{HK}\!/_{K} \cong {}^{H}\!/_{H \cap K}.$$

Theorem 6.2 (**Third Isomorphism Theorem**)**.**
Let $K \subseteq H \subseteq G$ be groups with $K \lhd G$ and $H \lhd G$. Then, ${}^{H}\!/_{K} \lhd {}^{G}\!/_{K}$ and

$${}^{({}^{G}\!/_{K})}\!/_{({}^{H}\!/_{K})} \cong {}^{G}\!/_{H}.$$

Theorem 6.3. Let G be a solvable group. Then,

(1) If H is a subgroup of G, then H is solvable.

(2) Let N be a normal subgroup of G, then the quotient group ${}^{G}\!/_{N}$ is solvable.

Example. S_4 contains subgroups isomorphic to S_3 and S_2, Since S_4 is solvable, by Theorem 6.3, S_3 and S_2 are solvable.

Lecture 17, 2025/02/12

Proof of Theorem 6.3. Since G is a solvable group, there exists a tower

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

with $G_{i+1} \triangleleft G_i$ and G_i/G_{i+1} abelian for all $0 \leq i \leq m-1$.

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

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$$

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

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

Applying the Second Isomorphism Theorem, we have

$$H_i/H_{i+1} \cong H_i/H_i \cap G_{i+1} \cong H_iG_{i+1}/G_{i+1} \subseteq G_i/G_{i+1}$$

since $H_i \subseteq G_i$ and $G_{i+1} \subseteq G_i$. Now, since G_i/G_{i+1} is abelian, so is H_i/H_{i+1}. It follows that H is solvable.

(2) Consider the following tower

$$G = G_0N \supseteq G_1N \supseteq \cdots \supseteq G_mN = N$$

and take the quotient by N, we have

$$G/N = G_0N/N \supseteq G_1N/N \supseteq \cdots \supseteq G_mN/N = \{1\}.$$

Since $G_{i+1} \triangleleft G_i$ and $N \triangleleft G$, we have $G_{i+1}N \triangleleft G_iN$, which implies that $G_{i+1}N/N \triangleleft G_iN/N$.

By the Third Isomorphism Theorem, we have

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

Now, by the Second Isomorphism Theorem,

$$G_iN/G_{i+1}N \cong G_i/G_i \cap G_{i+1}N.$$

Consider the natural quotien map $\pi : G_i \to G_i/G_i \cap G_{i+1}N$ which is surjective. Since G_{i+1} is a subgroup of $(G_i \cap G_{i+1}N)$, this means that G_{i+1} is contained in $\operatorname{Ker} \pi$, so it induces a surjective map $G_i/G_{i+1} \to G_i/G_i \cap G_{i+1}N$ by the universal property of groups. Since G_i/G_{i+1} is abelian, so is $G_i/G_i \cap G_{i+1}N$. Thus, $\left(G_iN/N\right)/\left(G_{i+1}N/N\right)$ is abelian. It follows that G/N is solvable.

$\square$

Theorem 6.4. Let N be a normal subgroup of G. If N and G/N are 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

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

with $N_{i+1} \lhd N_i$ and N_i/N_{i+1} abelian for all $0 \leq i \leq m-1$. For a subgroup $H \subseteq G$ with $N \subseteq H$, we denote $\overline{H} = H/N$. Since G/N is solvable, we have a tower

$$G/N = \overline{G}_0 \supseteq \overline{G}_1 \supseteq \cdots \supseteq \overline{G}_m = \{1\}$$

with $\overline{G}_{i+1} \lhd \overline{G}_i$ and $\overline{G}_i/\overline{G}_{i+1}$ abelian. Let $\mathrm{Sub}_N(G)$ denote the subgroups of G which contain N. Consider the map

$$\sigma : \mathrm{Sub}_N(G) \to \underbrace{\mathrm{Sub}(G/N)}_{\text{all subgroups of } G/N} \qquad H \to H/N.$$

For all $i = 0, 1, \dots, r$, define $G_i = \sigma^{-1}(\overline{G}_i)$. Since $N \lhd G$ and $\overline{G}_{i+1} \lhd \overline{G}_i$, we have (see Piazza)

$G_{i+1} \lhd G_i$. Moreover, by the Third Isomorphism Theorem, we have

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

It follows that

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

with $G_{i+1} \lhd G_i, N_{i+1} \lhd N_i$ and $G_i/G_{i+1}, N_i/N_{i+1}$ are all abelian. Thus, G is solvable. □

Definition 6.2 (**Simple Group**).

A group G is **simple** if it is not trivial and has no normal subgroups other than $\{1\}$ and G.

Example. One can show that the alternating group A_5 is simple (see Bonus). Since $A_5 \supseteq \{1\}$ is the only tower and $A_5/\{1\}$ is not abelian, A_5 is not solvable. By Theorem 6.3, S_5 is not solvable. Moreover, since all S_n with $n \geq 5$ contains a subgroup isomorphic to S_5, which is not solvable. By Theorem 6.3 again, S_n is not solvable for all $n \geq 5$.

Note. This example is the reason why we separate polynomials of degree 5 or higher from those of degree $1, 2, 3, 4$.

Corollary 6.5. Let G be a finite solvable group. Then, there exists a tower

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

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

Proof. If G is solvable, there exists a tower

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian for all $0 \leq i \leq n-1$. Consider $A = G_i/G_{i+1}$, a finite abelian group. We have

$$A \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_r}$$

where C_k is a cyclic group of order k. Since each G_i/G_{i+1} can be rewritten as a product of cyclic groups, the result follows. □

Remark. In the above group, given a finite cyclic group C, by the Chinese Remainder Theorem, we have

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

where 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

$${}^{\mathbb{Z}}\!/\!_{\langle p^{\alpha}\rangle} \supseteq {}^{\mathbb{Z}}\!/\!_{\langle p^{\alpha-1}\rangle} \supseteq \cdots \supseteq {}^{\mathbb{Z}}\!/\!_{\langle p\rangle} \supseteq \{1\}.$$

So we can further require the quotient ${}^{G_i}\!/\!_{G_{i+1}}$ in the Corollary to be a cyclic group of prime order.

Lecture 18, 2025/02/24

6.2 Automorphism Groups

Definition 6.3 (F-**Automorphism, Automorphism Group**).
Let ${}^{E}\!/\!_{F}$ be a field extension. If ψ is an **automorphism** of E, i.e. $\psi : E \to E$ is an isomorphism. If $\psi|_F = 1_F$, then we say ψ is an F-**automorphism** of E. By map composition, one can verify that the set

$$\mathrm{Aut}_F(E) = \{\psi : E \to E \mid \psi \text{ is an } F\text{-automorphism}\}$$

is a group. We call it the **automorphism group** of ${}^{E}\!/\!_{F}$.

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

Proof. Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$, then

$$\begin{aligned} f(\psi(\alpha)) &= a_0 + a_1\psi(\alpha) + \cdots + a_n\psi(\alpha)^n \\ &= \psi(a_0) + \psi(a_1)\psi(\alpha) + \cdots + \psi(a_n)\psi(\alpha)^n \quad \text{since } \psi \text{ is an } F\text{-automorphism} \\ &= \psi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \psi(f(\alpha)) = \psi(0) = 0. \end{aligned}$$

Thus, $\psi(\alpha)$ is a root of $f(x)$. □

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

Proof. Note that for $\alpha \in E$, we have
$$\alpha = \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}$$
where $f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ with $g \neq 0$. Thus, the lemma follows. $\square$

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

Proof. Since E/F is a finite extension, by Theorem 3.5, we have
$$E = F(\alpha_1, \dots, \alpha_n)$$
where α_i is algebraic over F for $1 \le i \le n$. For $\psi \in \mathrm{Aut}_F(E)$, by Lemma 6.6, $\psi(\alpha_i)$ is a root of the minimal polynomial of α_i for all $1 \le i \le n$. Thus, it has only finitely many choices. Now, by Lemma 6.7, since $\psi \in \mathrm{Aut}_F(E)$ is completely determined by $\psi(\alpha_i)$, there are only finitely many choices for ψ. Thus, $\mathrm{Aut}_F(E)$ is finite. $\square$

Remark. The converse of above Corollary is false. For example, $\mathbb{R}/\mathbb{Q}$ is an infinite extension. But one can show that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{1\}$ (see A6).

6.3 Automorphism Groups of Splitting Fields

Definition 6.4 (Automorphism Group of Splitting Field).
Let F be a field and $f(x) \in F[x]$. The **automorphism group** of $f(x)$ over F is $\mathrm{Aut}_F(E)$, where E is the splitting field of $f(x)$ over F.

Remark. Recall Theorem 4.4 (a result in splitting field) and A4, we showed that the number of such $\psi \le [E : F]$. Also, one can show that the equality holds $\iff$ every irreducible factor of $f(x)$ is separable over F. As a direct consequence, we have the following.

Theorem 6.9. Let ${}^{E}\!/_{F}$ be the splitting field of a non-zero polynomial $f(x) \in F[x]$. We have

$$|\mathrm{Aut}_F(E)| \leq [E : F]$$

and the equality holds $\iff$ every irreducible factor of $f(x)$ is separable.

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

Proof. Let $X = \alpha_1, \dots, \alpha_n$ be distinct roots of $f(x)$ in E. By Lemma 6.6, if $\psi \in \mathrm{Aut}_F(E)$, then $\psi(X) = X$. Let $\psi|_X$ be the restriction of ψ in X and S_X be the permutation group of X. The map

$$\mathrm{Aut}_F(E) \to S_X \cong S_n \quad \text{by} \quad \psi \mapsto \psi|_X$$

is a group homomorphism. Moreover, by Lemma 6.7, this map is injective. Thus, $\mathrm{Aut}_F(E)$ is isomorphic to a subgroup of S_n. $\square$

Example. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and ${}^{E}\!/_{\mathbb{Q}}$ be the splitting field of $f(x)$. We have seen that $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and $[E : \mathbb{Q}] = 6$. Since $\mathrm{ch}(\mathbb{Q}) = 0$ and $f(x)$ is irreducible, so $f(x)$ is separable. By Theorem 6.9, $|\mathrm{Aut}_{\mathbb{Q}}(E)| = [E : \mathbb{Q}] = 6$. Also, since $f(x)$ has 3 distinct roots, by Theorem 6.10, $\mathrm{Aut}_{\mathbb{Q}}(E)$ is a subgroup of S_3 by isomorphism. Since $|S_3| = 6 = |\mathrm{Aut}_{\mathbb{Q}}(E)|$, we have $\mathrm{Aut}_{\mathbb{Q}}(E) \cong S_3$.

Example. Let F be a field with $\mathrm{ch}(F) = p$ and $F^p \neq F$. Let $f(x) = x^p - a$ with $a \in F \setminus F^p$. Let ${}^{E}\!/_{F}$ be the splitting field of $f(x)$. We have seen in Chapter 5 that $f(x)$ is irreducible in $F[x]$ and $f(x) = (x - \beta)^p$ for some $\beta \in E \setminus F$. This, $E = F(\beta)$. Since β can only map to β under any $\psi \in \mathrm{Aut}_F(E)$, we have $\mathrm{Aut}_F(E) = \{1\}$. However note that

$$|\mathrm{Aut}_F(E)| = 1 \quad \text{and} \quad [E : F] = \deg(f(x)) = p.$$

We have $|\mathrm{Aut}_F(E)| \neq [E : F]$. This is because $f(x)$ is not separable.

Definition 6.5 (**Fixed Field**).
Let E/F be a field extension and $\psi \in \mathrm{Aut}_F(E)$. Define

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

which is a subfield of E containing F. We call E^ψ the **fixed field** of ψ. If $G \subseteq \mathrm{Aut}_F(E)$, the **fixed field** of G is defined by

$$E^G = \bigcap_{\psi \in G} E^\psi = \{\alpha \in E : \psi(\alpha) = \alpha \text{ for all } \psi \in G\}.$$

Theorem 6.11. Let $f(x) \in F[x]$ be a polynomial in which every irreducible factor is separable. Let E/F be the splitting field of $f(x)$. If $G = \mathrm{Aut}_F(E)$, then $E^G = F$.

Proof. Let $L = E^G$. Since $F \subseteq L$, we have $\mathrm{Aut}_L(E) \subseteq \mathrm{Aut}_F(E)$. On the other hand, if $\psi \in \mathrm{Aut}_F(E)$, by definition of L, for all $a \in L$, we have $\psi(a) = a$. This implies that $\psi \in \mathrm{Aut}_L(E)$. Thus, $\mathrm{Aut}_F(E) \subseteq \mathrm{Aut}_L(E)$. It follows that $G = \mathrm{Aut}_F(E) = \mathrm{Aut}_L(E)$. Note chat since $f(x)$ is separable over F and splits over E, $f(x)$ is also separable over L and has E as its splitting field over L. Thus, by Theorem 6.9,

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

It follows that $[E : F] = [E : L]$ and since $[E : F] = [E : L][L : F]$, we have $[L : F] = 1$. Thus, $L = F$, i.e. $E^G = F$. □

7 Separable Extensions and Normal Extensions

7.1 Separable Extensions

Definition 7.1 (Separable, Separable Extension).
Let E/F ba an algebraic field extension. For $\alpha \in E$, let $p(x) \in F[x]$ be the minimal polynomial of α over F. We say that α is **separable** over F if $p(x)$ is separable. We say that E/F is a **separable extension** if α is separable for all $\alpha \in E$.

Example. If $\mathrm{ch}(F) = 0$, by Corollary 5.6, every irreducible polynomial $p(x) \in F[x]$ is separable. Thus, if $\mathrm{ch}(F) = 0$, 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 the minimal polynomial of α. Let $\{\alpha = \alpha_1, \dots, \alpha_n\}$ be all of the distinct roots of $p(x)$ in E. Define $\tilde{p}(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.

Claim. $\tilde{p}(x) \in F[x]$.

Proof of Claim. Let $G = \mathrm{Aut}_F(E)$ and $\psi \in G$. Since ψ is an automorphism, $\psi(\alpha_i) \neq \psi(\alpha_j)$ if $i \neq j$ and by Lemma 6.6, ψ permutes $\alpha_1, \dots, \alpha_n$. Thus by extending $\psi : E \to E$ uniquely to $\psi : E[x] \to E[x]$ by $x \mapsto x$, we have

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

It follows that $\tilde{p}(x) \in E^{\psi}[x]$ and since ψ is arbitrary, we get $\tilde{p}(x) \in E^G[x]$. Since E/F is the splitting field of $f(x)$ whose irreducible factors are separable, by Theorem 6.11, $E^G = F$. Thus, $\tilde{p}(x) \in F[x]$. □

Thus, we have $\tilde{p}(x) \in F[x]$ with $\tilde{p}(\alpha) = 0$. Since $p(x)$ is the minimal polynomial of α, we have $p(x) \mid \tilde{p}(x)$. Also, since $\alpha_1, \dots, \alpha_n$ are all distinct roots of $p(x)$, we have $\tilde{p}(x) \mid p(x)$. Also, since $p(x)$ and $\tilde{p}(x)$ are both monic, we have $p(x) = \tilde{p}(x)$. It follows that $p(x)$ is separable. □

Corollary 7.2. Let ${}^{E}\!/_{F}$ be a finite extension and $E = F(\alpha_1, \dots, \alpha_n)$. If each α_i is separable over F for all $1 \le i \le n$, then ${}^{E}\!/_{F}$ is separable.

Proof. Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i for all $1 \le i \le n$. Let $f(x) = p_1(x) \cdots p_n(x)$ with each $p_i(x)$ being separable. Let L be the splitting field of $f(x)$ over F. By Theorem 7.1, ${}^{L}\!/_{F}$ is separable. Since $E = F(\alpha_1, \dots, \alpha_n)$ is a subfield of L, we have E is also separable. □

Lecture 20, 2025/02/28

Corollary 7.3. Let ${}^{E}\!/_{F}$ be an algebraic extension and L be the set of all $\alpha \in E$ which is separable over F, then L is a field.

Proof. Let $\alpha, \beta \in L$. Then, $\alpha \pm \beta$, $\alpha\beta$, α/β $(\beta \neq 0) \in F(\alpha, \beta)$. By Corollary 7.2, $F(\alpha, \beta)$ is separable and hence $F(\alpha, \beta) \subseteq L$. Thus, L is a field. □

We have seen in Theorem 3.5 that a finite extension is a composition of simple extensions.

Definition 7.2 (**Primitive Element**).
If $E = F(\gamma)$ is a simple extension, we say that γ 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 $\mathrm{ch}(F) = 0$, then any finite extension ${}^{E}\!/_{F}$ is a simple extension.

Proof. We have seen in Corollary 5.9 that a finite extension of a finite field is always simple. Thus, WLOG, suppose that F is an infinite field. Since $E = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in E$, it suffices to consider when $E = F(\alpha, \beta)$ and the general case can be done by induction.

Let $E = F(\alpha, \beta)$ with $\alpha, \beta \notin F$.

Claim. There exists $\lambda \in F$ s.t. $\gamma = \alpha + \lambda\beta$ and $\beta \in F(\gamma)$.

Note. If the claim holds, then $\alpha = \gamma - \lambda\beta \in F(\gamma)$ and we have $F(\alpha, \beta) \subseteq F(\gamma)$. Also, since $\gamma = \alpha + \lambda\beta$, $F(\gamma) \subseteq F(\alpha, \beta)$. Thus, $E = F(\alpha, \beta) = F(\gamma)$.

Proof of Claim. Let $a(x)$ and $b(x)$ be the minimal polynomials of α and β over F, respectively. Since $\beta \notin F$, $\deg(b) > 1$. Thus, there exists a root $\tilde{\beta}$ of $b(x)$ such that $\tilde{\beta} \neq \beta$. Choose $\lambda \in F$ s.t.

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

for all roots $\tilde{\alpha}$ of $a(x)$ and all roots $\tilde{\beta}$ of $b(x)$ with $\tilde{\beta} \neq \beta$ in some splitting field of $a(x)b(x)$ over F. The choice of λ is possible since there are infinitely many elements in F but only finitely many choices of $\tilde{\alpha}$ and $\tilde{\beta}$. Let $\gamma = \alpha + \lambda\beta$. Consider

$$h(x) = a(\gamma - \lambda x) \in F(\gamma)[x].$$

Then, we have $h(\beta) = a(\gamma - \lambda\beta) = a(\alpha) = 0$. However, for any $\tilde{\beta} \neq \beta$, since

$$\gamma - \lambda\tilde{\beta} = \alpha + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha} \quad \text{by the choice of } \lambda,$$

we have $h(\tilde{\beta}) = a(\gamma - \lambda\tilde{\beta}) \neq 0$. Thus, $h(x)$ and $b(x)$ have β as a common root, but no other common roots in any extension of $F(\gamma)$. Let $b_1(x)$ be the minimal polynomial of β over $F(\gamma)$. Thus, $b_1(x)$ divides both $h(x)$ and $b(x)$. Since ${}^{E}\!/_{F}$ is separable and $b(x) \in F[x]$ is irreducible, $b(x)$ has distinct roots, so does $b_1(x)$. The roots of $b_1(x)$ are also common to $h(x)$ and $b(x)$. Since $h(x)$ and $b(x)$ have only β as a common root, $b_1(x) = x - \beta$. Since $b_1(x) \in F(\gamma)[x]$, we obtain $\beta \in F(\gamma)$. $\square$

$\square$

7.2 Normal Extensions

Definition 7.3 (Normal Extension).
Let ${}^{E}\!/_{F}$ be an algebraic extension. We say ${}^{E}\!/_{F}$ is a **normal extension** if for any irreducible polynomial $p(x) \in F[x]$, either $p(x)$ has no roots in E or $p(x)$ has all roots in E.

Note. In other words, 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.

($\Rightarrow$): Suppose that ${}^{E}\!/_{F}$ is normal, write $E = F(\alpha_1, \dots, \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i $(1 \le i \le n)$. Define $f(x) = p_1(x) \cdots p_n(x)$. Since ${}^{E}\!/_{F}$ is normal, $f(x)$ splits over E. Let $\alpha_i = \alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,r_i}$ $(1 \le i \le n)$ be the roots of $p_i(x)$ in E. Then,

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

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

Lecture 21, 2025/03/03

($\Leftarrow$): Let ${}^{E}\!/_{F}$ be the splitting field of $f(x) \in F[x]$. Let $p(x) \in F[x]$ be irreducible aand have root $\alpha_1 \in E$. Let ${}^{K}\!/_{E}$ be the splitting field of $p(x)$ over E. Write

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

where $0 \ne c \in F$ and $\alpha = \alpha_1 \in E$ and $\alpha_2, \dots, \alpha_n \in K = E(\alpha_1, \dots, \alpha_n)$. Since we know that

$$F(\alpha) \cong {}^{F[x]}\!/_{(p(x))} \cong F(\alpha_2),$$

we have the F-isomorphism $\theta : F(\alpha) \to F(\alpha_2)$ with $\theta(\alpha) = \alpha_2$. Thus, we can view K as the splitting field of $p(x)f(x)$ over $F(\alpha)$ and $F(\alpha_2)$, respectively. Thus by Theorem 4.4, there exists an isomorphism $\psi : K \to K$ which extends θ. In particular, $\psi \in \mathrm{Aut}_F(K)$. Since $\psi \in \mathrm{Aut}_F(K)$, we know that ψ permutes the roots of $f(x)$. Since E is generated over F by the roots of $f(x)$, by Lemma 6.6, we have $\psi(E) = E$. It follows that for $\alpha \in E$, we have $\alpha_2 = \psi(\alpha) \in E$. Similarly, we can show that $\alpha_i \in E$ for all i and thus $K = E$ and $p(x)$ splits over E. It follows that ${}^{E}\!/_{F}$ is normal. $\square$

Example.

Claim. Every quadratic extension is normal.

Proof. 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 α over F. If β is another root of $p(x)$, then

$$p(x) = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta.$$

Since $\alpha \in E$, $\alpha\beta \in F$, we have $\beta = -\alpha - a \in E$. Hence, E/F is normal. $\square$

Example. Consider $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. We say this extension is not normal since the irreducible polynomial $p(x) = x^4 - 2$ has a root in $\mathbb{Q}(\sqrt[4]{2})$ but does not split over $\mathbb{Q}(\sqrt[4]{2})$ (since $\pm\sqrt[4]{2}i$ are also roots). In fact, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is made up of the quadratic extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, which are both normal. Thus, if E/K, K/F are normal, then E/F is not necessarily normal.

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 and has a root $\alpha \in E$. Let $f(x) \in F[x] \subseteq K[x]$ be the minimal polynomial of α over F. Then, $p(x) \mid f(x)$. Since E/F is normal, $f(x)$ splits over E, so does $p(x)$. Thus, E/K is a normal extension. $\square$

Remark. In Proposition 7.6, K/F is not always a normal extension. For example, let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, and $E = \mathbb{Q}(\sqrt[4]{2}, i)$. Then, E/F is the splitting field of $x^4 - 2$ and hence normal. Also, E/K is normal but K/F is not normal.

Proposition 7.7. Let E/F be a finite normal extension and $\alpha, \beta \in E$. Then, the following are equivalent:

(1) There exists $\psi \in \mathrm{Aut}_F(E)$ such that $\psi(\alpha) = \beta$.

(2) The minimal polynomial of α and β over F are the same.

In this case, we say α and β are **conjugate** over F.

Proof.

(1) $\implies$ (2): Let $p(x)$ be the minimal polynomial of α over F and $\psi \in \mathrm{Aut}_F(E)$ with $\psi(\alpha) = \beta$. Then,

β is also a root of $p(x)$. Since $p(x)$ is monic and irreducible, it follows that $p(x)$ must be the minimal polynomial of β over F. Hence, α and β have the same minimal polynomial over F.

(2) $\implies$ (1): Suppose that the minimal polynomial of α and β are the same, say $p(x)$. Then,

$$F(\alpha) \cong {}^{F[x]}\!\big/_{\langle p(x)\rangle} \cong F(\beta).$$

We have the F-isomorphism $\theta : F(\alpha) \to F(\beta)$ with $\theta(\alpha) = \beta$. Since ${}^{E}\!/_{F}$ is a finite normal extension, E must be the splitting field of some polynomial $f(x) \in F[x]$. Then, we can also view E as the splitting field of $f(x)$ over $F(\alpha)$ and $F(\beta)$, respectively. By Theorem 4.4, there exists an isomorphism $\psi : E \to E$ which extends θ. It follows that $\psi \in \mathrm{Aut}_F(E)$ and $\psi(\alpha) = \beta$. □

Lecture 22, 2025/03/05

Example. The complex numbers $\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2$ are all conjugates over $\mathbb{Q}$ since they are roots of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$.

Definition 7.4 (**Normal Closure**).
A **normal closure** of a finite extension ${}^{E}\!/_{F}$ is a finite normal extension ${}^{N}\!/_{F}$ satisfying:

(1) E is a subfield of N.

(2) For any intermediate field L of ${}^{N}\!/_{E}$, if L is normal over F, then $L = N$. In other words, N is the smallest field containing E such that N is normal.

Example. The normal closure of ${}^{\mathbb{Q}\left(\sqrt[3]{2}\right)}\!/_{\mathbb{Q}}$ is ${}^{\mathbb{Q}\left(\sqrt[3]{2},\, \zeta_3\right)}\!/_{\mathbb{Q}}$.

Theorem 7.8. Every finite extension ${}^{E}\!/_{F}$ has a normal closure ${}^{N}\!/_{F}$ that is unique up to E-isomorphism.

Proof. Since ${}^{E}\!/_{F}$ is finite, we can write $E = F(\alpha_1, \ldots, \alpha_n)$ and let $p_i(x)$ be the minimal polynomial of α_i over F for all $1 \le i \le n$. Let $f(x) = p_1(x)p_2(x)\cdots p_n(x)$ and ${}^{N}\!/_{F}$ be the splitting field of $f(x)$ over E. Since $\alpha_1, \ldots, \alpha_n$ are roots of $f(x)$, N is also a splitting field of $f(x)$ over F. By Theorem 7.5, ${}^{N}\!/_{F}$ is normal. Let $L \subseteq N$ be a subfield containing E. Then, E contains all the α_i. If L is normal over F, then each $p_i(x)$ splits over L and $N \subseteq L$. Therefore, $L = N$. To show 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 all α_i, $f(x)$ splits over N. Thus, N_1 must contain a splitting field $\tilde{N}$ of $f(x)$ over F. 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. Thus by definitioin of normal closure, $\tilde{N} = N_1$. It follows that N and N_1 are E-isomorphic. $\square$

8 Galois Correspondence

8.1 Galois Extensions

We recall for a finite extension ${}^{E}\!/_{F}$, we have:

- Theorem 7.5: ${}^{E}\!/_{F}$ is the splitting field of some $f(x) \in F[x] \iff {}^{E}\!/_{F}$ is normal.
- Theorem 7.1: ${}^{E}\!/_{F}$ is the splitting field of some $f(x) \in F[x]$ whose irreducible factors are separable $\implies {}^{E}\!/_{F}$ is separable.

Definition 8.1 (**Galois Extension, Galois Group**).
An algebraic extension ${}^{E}\!/_{F}$ is **Galois** if it is normal and separable. If ${}^{E}\!/_{F}$ is Galois, then the **Galois group** of ${}^{E}\!/_{F}$, denoted $\mathrm{Gal}_F(E)$, is defined to be the automorphism group, $\mathrm{Aut}_F(E)$.

Note. That is, $\mathrm{Gal}_F(E) = \mathrm{Aut}_F(E)$.

Remark. We note that

(1) By Theorem 7.1 and 7.5, a finite Galois extension is equivalent to 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, we have

$$|\mathrm{Gal}_F(E)| = [E : F].$$

(3) If ${}^{E}\!/_{F}$ is the splitting field of some separable $f(x) \in F[x]$ with $\deg(f) = n$, then by Theorem 6.10, $\mathrm{Gal}_F(E)$ is isomorphic to a subgroup of S_n.

Example. Let E be the splitting field of $f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$. Then, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and $[E : \mathbb{Q}] = 8$ (exercise). For $\psi \in \mathrm{Gal}_{\mathbb{Q}}(E)$, we have

$$\psi(\sqrt{2}) = \pm\sqrt{2}, \quad \psi(\sqrt{3}) = \pm\sqrt{3}, \quad \psi(\sqrt{5}) = \pm\sqrt{5}.$$

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

Theorem 8.1 (**E. Artin**).

Let E be a field and G a finite subgroup of $\mathrm{Aut}(E)$. Let $E^G = \{\alpha \in E : \psi(\alpha) = \alpha \text{ for all } \psi \in G\}$. Then, ${}^{E}\!/_{E^G}$ is a finite Galois extension and $\mathrm{Gal}_{E^G}(E) = G$. In particular, $[E : E^G] = |G|$.

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

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

where each α_i is distinct. Note that $m \leq n$. Consider $f(x) = (x - \alpha_1) \cdots (x - \alpha_m)$. For any $\psi \in G$, ψ permutes the roots $\alpha_1, \dots, \alpha_m$. Since the coefficients of $f(x)$ are symmetric with respect to each α_i, they are fixed by all $\psi \in G$. Thus, $f(x) \in E^G[x] = F[x]$. To show that $f(x)$ is the minimal polynomial of α over F, consider a factor $g(x) \in F[x]$ of $f(x)$. WLOG, we can write

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

with $\ell \leq m$. If $\ell < m$, since α_i are in the G-orbit of α, $\exists \psi \in G$ s.t.

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

Then, we have

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

Thus if $\ell < m$, then $g(x) \notin F[x]$. It follows that $f(x)$ is the minimal polynomial of α over F. Since $f(x)$ is separable and splits over E, we know that ${}^{E}\!/_{F}$ is a Galois extension.

Lecture 23, 2025/03/07

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

Proof. Suppose for a contradiction that $[E : F] > n = |G|$. Then, we can choose $\beta_1, \dots, \beta_n, \beta_{n+1} \in E$

which are linearly independent over F. For all $G = \{\psi_1, \dots, \psi_n\}$, consider the system

$$\begin{aligned}\psi_1(\beta_1)v_1 + \cdots + \psi_1(\beta_{n+1})v_{n+1} &= 0\\ &\vdots\\ \psi_n(\beta_1)v_1 + \cdots + \psi_n(\beta_{n+1})v_{n+1} &= 0\end{aligned}$$

of n linear equations in $(n+1)$ variables $v_1, \dots, v_{n+1}$. Thus, it has a non-zero solution in E (more columns than rows, so nullity is at least 1). Let $(\gamma_1, \dots, \gamma_{n+1})$ be a non-zero solution which has the minimal number of non-zero coordinates, say r. Clearly $r > 1$ (since we need at least two non-zero coordinates to get a non-zero solution, it there is only one non-zero term, the sum will not be 0). WLOG, we can assume $\gamma_1, \dots, \gamma_r \neq 0$ and $\gamma_{r+1}, \dots, \gamma_n, \gamma_{n+1} = 0$.Thus,

$$\psi_j(\beta_1)\gamma_1 + \cdots + \psi_j(\beta_r)\gamma_r = 0. \tag{1}$$

for all $j \in \{1, \dots, n\}$. By dividing the solution by γ_r, we can assume $\gamma_r = 1$. Also, since $(\beta_1, \dots, \beta_r)$ are independent over F and

$$\beta_1\gamma_1 + \cdots + \beta_r\gamma_r = 0,$$

by taking $\psi_i = 1$ for some i. There exists at least one $\gamma_r \notin F$. Since $r \geq 2$, WLOG, we assume $\gamma_1 \notin F$ (if all $\gamma_i \in F$, then $\beta_1\gamma_1 + \cdots + \beta_r\gamma_r = 0 \implies \gamma_i = 0\ \forall i$). Choose $\phi \in G$ s.t. $\phi(\gamma_1) \neq \gamma_1$. Applying ψ in (1) gives

$$(\phi \circ \psi_j)(\beta_1)\phi(\gamma_1) + \cdots + (\phi \circ \psi_j)(\beta_r)\phi(\gamma_r) = 0 \tag{2}$$

for all $j \in \{1, \dots, n\}$. Since $\phi \in G$, therefore by the property of group, we have $\{\phi \circ \psi_1, \dots, \phi \circ \psi_n\} = \{\psi_1, \dots, \psi_n\} = G$. Therefore, we can rewrite (2) as

$$\psi_j(\beta_1)\phi(\gamma_1) + \cdots + \psi_j(\beta_r)\phi(\gamma_r) = 0 \tag{3}$$

for all $j \in \{1, \dots, n\}$. Then, by subtracting (3) form (1), we have

$$\psi_j(\beta_1)(\gamma_1 - \phi(\gamma_1)) + \cdots + \psi_j(\beta_r)(\gamma_r - \phi(\gamma_r)) = 0.$$

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

$$(\gamma_1 - \phi(\gamma_1), \dots, \gamma_{r-1} - \phi(\gamma_{r-1}), \gamma_r - \phi(\gamma_r) = 0, 0, \dots, 0)$$

is a non-zero solution to the system with fewer number of non-zero coordinates, which contradicts the choices of $(\gamma_1, \dots, \gamma_{n+1})$ with minimal number of non-zero coordinates. Thus, $[E : F] \leq n$. $\square$

Using the claim, we can see that $n = |G| \leq |\mathrm{Gal}_F(E)| = [E : F] \leq n$. By "Squeeze Theorem", we have $[E : F] = n$ and $\mathrm{Gal}_F(E) = G$. $\square$

Remark. Let E be a field and G a finite subgroup of $\mathrm{Aut}(E)$. For $\alpha \in E$, let $\{\alpha = \alpha_1, \dots, \alpha_m\}$ be the G-orbit of α, i.e. the set of conjugates of α. Then, we can see from the proof of Theorem 8.1 that the minimal polynomial of α over E^G is $(x - \alpha_1) \cdots (x - \alpha_m) \in E^G[x]$.

Definition 8.2 (Elementary Symmetric Functions).
Let $t_1, \dots, t_n$ be variables. We define the **elementary symmetric functions** in $t_1, \dots, t_n$ as $s_1, \dots, s_n$ where

$$s_m = \sum_{1 \leq j_1 < \cdots < j_m \leq n} t_{j_1} \cdots t_{j_m}.$$

For example,

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

Then,

$$f(x) = (x - t_1) \cdots (x - t_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n.$$

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 S_n as a subgroup of $\mathrm{Aut}(E)$ which permutes the variables $t_1, \dots, t_n$ and fixes the field F. We are interested in finding $E^{S_n} = E^G$ where $G = S_n$. From the proof of Theorem 8.1, the coefficients of the minimal polynomial of t_1 lie in E^G. Thus, by considering the minimal polynomial of t_1, we can get some hints about E^G. The G-orbit of t_1 is $\{t_1, \dots, t_n\}$. By the remark above, we see that

$$f(x) = (x - t_1) \cdots (x - t_n)$$

is the minimal polynomial of t_1 over E^G. Let $s_1, \dots, s_n$ be the elementary symmetric functions of $t_1, \dots, t_n$. So we have

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n \in L[x]$$

where $L = F(s_1, \dots, s_n)$.

Lecture 24, 2025/03/10

Claim. $L = E^G$.

Proof. E is the splitting field of $f(x)$ over L. Since $\deg(f) = n$, by Theorem 4.6, we have

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

On the other hand, by Theorem 8.1, we have

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

Since $L \subseteq E^G$,

$$n! = [E : E^G] \leq [E : L] \leq n! \implies E^G = L.$$

□

8.2 The Fundamental Theorem

Theorem 8.2 (**The Fundamental Theorem of Galois Theory**).
Let E/F be a finite Galois extension and $G = \mathrm{Gal}_F(E)$. There is an order reversing bijection between the intermediate fields of E/F and the subgroups of G. More precisely, let $\mathrm{Int}\left(E/F\right)$ denote the set of intermediate fields of E/F and $\mathrm{Sub}(G)$ denote the set of subgroups of G. Then, the maps

$$\mathrm{Int}\left(E/F\right) \to \mathrm{Sub}(G) \quad L \mapsto L^* := \mathrm{Gal}_L(E)$$

and

$$\mathrm{Sub}(G) \to \mathrm{Int}\left(E/F\right) \quad H \mapsto H^* := E^H$$

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

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

Note. We can use the following diagram to illustrate above.

$$\begin{tikzcd}
E \arrow[r, leftrightarrow] \arrow[d, dash] & \{1\} = \operatorname{Gal}_E(E) \arrow[d, dash] \\
L_1 \arrow[d, dash] & L_1^* = \operatorname{Gal}_{L_1}(E) \arrow[d, dash] \\
L_2 \arrow[d, dash] & L_2^* = \operatorname{Gal}_{L_2}(E) \arrow[d, dash] \\
F & G = \operatorname{Gal}_F(E)
\end{tikzcd}$$

Proof. Let $L \in \operatorname{Int}\left(E/F\right)$ and $H \in \operatorname{Sub}(G)$. We recall Theorem 6.11, which states that if $G_1 = \operatorname{Gal}_{F_1}(E_1)$, then $E^{G_1} = F_1$. Thus, we have

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

Also, Theorem 8.1 states that if $G_1 \subseteq \operatorname{Aut}(E_1)$, then $\operatorname{Gal}_{E^{G_1}}(E) = G_1$. Thus, we have

$$(H^*)^* = \left(E^H\right)^* = \operatorname{Gal}_{E^H}(E) = H.$$

Thus, we have

$$H \mapsto H^* \mapsto H^{**} = H \quad \text{and} \quad L \mapsto L^* \mapsto L^{**} = L.$$

In particular, the maps $L \mapsto L^*$ and $H \mapsto H^*$ are reverses of each other. Let $L_1, L_2 \in \operatorname{Int}\left(E/F\right)$. 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 the splitting field of $f(x)$ over L_1 and L_2, respectively. We have

$$L_2 \subseteq L_1 \implies \operatorname{Gal}_{L_1}(E) \subseteq \operatorname{Gal}_{L_2}(E) \implies L_1^* \subseteq L_2^*.$$

Also,

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

For $H_1, H_2 \in \mathrm{Sub}(G)$,

$$H_2 \subseteq H_1 \implies E^{H_1} \subseteq E^{H_2} \implies H_1^* \subseteq H_2^*.$$

Also,

$$[H_1 : H_2] = \frac{|H_1|}{|H_2|} = \frac{\left|\mathrm{Gal}_{E^{H_1}}(E)\right|}{\left|\mathrm{Gal}_{E^{H_2}}(E)\right|} = \frac{[E : E^{H_1}]}{[E : E^{H_2}]} = [E^{H_2} : E^{H_1}] = [H_2^* : H_1^*].$$

$\square$

Remark. Consider $E/\mathbb{Q}$ with $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We recall that $\left|\mathrm{Gal}_{\mathbb{Q}}(E)\right| = 4$, note that $\mathrm{Gal}_{\mathbb{Q}}(E) \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$. Since there are only finitely many subgroups of $\mathrm{Gal}_{\mathbb{Q}}(E)$, there are only finitely many intermediate fields between $\mathbb{Q}$ and E.

We recall that if E/F is a finite Galois extension and $L \in \mathrm{Int}\left(E/F\right)$, then L/F is not always Galois. For example, if we take $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $L = \mathbb{Q}(\sqrt[3]{2})$, and $F = \mathbb{Q}$, then L/F is not Galois.

Remark. We have the following diagram.

$$\begin{array}{ccc}
E & \longleftrightarrow & \{1\} = \mathrm{Gal}_E(E) \\
| & & | \\
L & \longleftrightarrow & L^* = \mathrm{Gal}_L(E) \\
| & & | \\
F & \longleftrightarrow & G = \mathrm{Gal}_F(E)
\end{array}$$

From the above picture, if L/F is Galois, the corresponding group is G/L^*, which is well-defined only if $L^* \lhd G$.

Proposition 8.3. Let E/F be a finite Galois extension with $G = \mathrm{Gal}_F(E)$. Let L be an intermediate field. For $\psi \in G$, we have

$$\mathrm{Gal}_{\psi(L)}(E) = \psi\,\mathrm{Gal}_L(E)\psi^{-1}.$$

Proof of Proposition 8.3. For $\alpha \in \psi(L)$, then $\psi^{-1}(\alpha) \in L$. If $\phi \in \mathrm{Gal}_L(E)$, we have

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

Thus, $\psi\phi\psi^{-1} \in \mathrm{Gal}_{\psi(L)}(E)$. Thus,

$$\psi\,\mathrm{Gal}_L(E)\psi^{-1} \subseteq \mathrm{Gal}_{\psi(L)}(E).$$

Since we have

$$\left|\psi\,\mathrm{Gal}_L(E)\psi^{-1}\right| = |\mathrm{Gal}_L(E)| = [E : L] = [E : \psi(L)] = \left|\mathrm{Gal}_{\psi(L)}(E)\right|,$$

it follows that $\mathrm{Gal}_{\psi(L)}(E) = \psi\,\mathrm{Gal}_L(E)\psi^{-1}$. □

Theorem 8.4. Let ${}^{E}\!/_{F}$, L, L^* be defined as in the Fundamental Theorem. Then, ${}^{L}\!/_{F}$ is a Galois extension $\iff$ L^* is a normal subgroup of $G = \mathrm{Gal}_F(E)$. In this case, we have

$$\mathrm{Gal}_F(L) \cong {}^{G}\!/_{L^*} = {}^{\mathrm{Gal}_F(E)}\!/_{\mathrm{Gal}_L(E)}.$$

Proof. To get the "if and only if", we have

$$\begin{aligned} {}^{L}\!/_{F} \text{ is normal} &\iff \psi(L) = L \text{ for all } \psi \in \mathrm{Gal}_F(E) \\ &\iff \mathrm{Gal}_{\psi(L)}(E) = \mathrm{Gal}_L(E) \text{ for all } \psi \in \mathrm{Gal}_F(E) \\ &\iff \psi\,\mathrm{Gal}_L(E)\psi^{-1} = \mathrm{Gal}_L(E) \text{ for all } \psi \in \mathrm{Gal}_F(E) \\ &\iff L^* = \mathrm{Gal}_L(E) \text{ is a normal subgroup of } G. \end{aligned}$$

In this case, if ${}^{L}\!/_{F}$ is a Galois extension, the restriction map

$$G = \mathrm{Gal}_F(E) \to \mathrm{Gal}_F(L) \quad \psi \mapsto \psi|_L$$

is well-defined. Moreover, it is surjective and its kernel is $\mathrm{Gal}_L(E)$, as elements in the kernel fix everything in L. Thus, we get $\mathrm{Gal}_F(L) \cong {}^{\mathrm{Gal}_F(E)}\!/_{\mathrm{Gal}_L(E)}$. □

Example. For a prime p, let $q = p^n$. We have seen that the Frobenius automorphism of $\mathbb{F}_q$ is defined by $\sigma_p : \mathbb{F}_q \to \mathbb{F}_q$ by $\alpha \mapsto \alpha^p$. For $\alpha \in \mathbb{F}_q$, we have

$$\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha.$$

For $1 \leq m < n$, we have $\sigma_P^m(\alpha) = \alpha^{p^m}$. Since the polynomial $x^{p^m} - x$ has at most p^m roots in $\mathbb{F}_q$, $\exists \alpha \in E$ such that $\alpha^{p^m} - \alpha \neq 0$. Thus, $\sigma_p^m \neq 1$. Hence, σ_o has order n. Let $G = \mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$, it follows that

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

Thus, $G = \langle \sigma_p \rangle$, a cyclic group of order n. Consider the subgroup H of G of order d. Then, $d \mid n$ and $[G : H] = \frac{n}{d}$. By Theorem 8.2, we have

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

Thus, $H^* = \mathbb{F}_q^H = \mathbb{F}_{p^{n/d}}$. The picture is as follows:

$$\begin{tikzcd}
\mathbb{F}_q \arrow[r, leftrightarrow] \arrow[d, dash] & \{1\} \arrow[d, dash] \\
H^* = \mathbb{F}_{p^{n/d}} \arrow[r, leftrightarrow] \arrow[d, dash] & H \arrow[d, dash] \\
\mathbb{F}_p \arrow[r, leftrightarrow] & G
\end{tikzcd}$$

Example. Let E be the splitting field of $x^5 - 7$ over $\mathbb{Q}$ in $\mathbb{C}$. Then $E = \mathbb{Q}(\alpha, \zeta_5)$ with $\alpha = \sqrt[5]{7}$ and $\zeta_5 = e^{2\pi i/5}$. The minimal polynomials of α and ζ_5 over $\mathbb{Q}$ are $x^5 - 7$ and $x^4 + x^3 + x^2 + x + 1$, respectively. We can show that $[E : \mathbb{Q}] = 20$ and hence $G = \mathrm{Gal}_{\mathbb{Q}}(E)$ is a subgroup of S_5 of order 20 (Piazza exercise).

Lecture 26, 2025/03/14

For $\psi \in G$, its action is determined by $\psi(\alpha)$ and $\psi(\zeta_5)$. We write $\psi = \psi_{k,s}$ if

$$\psi(\alpha) = \alpha\zeta_5^k,\ k \in \mathbb{Z}_5 \quad \text{and} \quad \psi(\zeta_5) = \zeta_5^s,\ s \in \mathbb{Z}_5^*.$$

Define $\sigma = \psi_{1,1}$ where

$$\psi_{1,1} : \alpha \to \alpha\zeta_5 \quad \text{and} \quad \zeta_5 \to \zeta_5$$

and $\tau = \psi_{0,2}$ where

$$\psi_{0,2} : \alpha \to \alpha \quad \text{and} \quad \zeta_5 \to \zeta_5^2.$$

We can show that $\tau\sigma = \sigma^2\tau$ (exercise) and we have

$$G = \langle \sigma, \tau : \sigma^5 = 1 = \tau^4, \tau\sigma = \sigma^2\tau \rangle.$$

Since $|G| = 20$, by Lagrange's Theorem, the possible subgroups of G are of order $1, 2, 4, 5, 10, 20$. We have $|G| = 20 = 2^2 \cdot 5$. Let n_p be the number of Sylow-p subgroups of G. By the Third Sylow's Theorem, we have $n_5 \mid 4$ and $n_5 \equiv 1 \pmod 5$. Hence, $n_5 = 1$. It follows that G has a unique Sylow 5-subgroup, say P_5, which is of order 5. Since $\langle \sigma \rangle$ is a subgroup of order 5, we have $P_5 = \langle \sigma \rangle \cong \mathbb{Z}_5$. Note that by the Second Sylow Theorem, we have $P_5 \lhd G$. Also, $n_2 \mid 5$ and $n_2 \equiv 1 \pmod 2$. Hence, $n_2 = 1$ or 5. If $n_2 = 1$, then the only Sylow 2-subgroup is $P_4 = \langle \tau \rangle \cong \mathbb{Z}_4$ and $P_4 \lhd G$. Since $|P_4 \cap P_5| = 1$, $G \cong P_4 \times P_5 \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20}$, which is abelian, and this contradicts that G is not abelian. Thus, there are 5 Sylow-2 groups. We have seen that $\tau \in G$ is of order 4. Thus, the cyclic group $\langle \tau \rangle$ is a Sylow 2-subgroup and all other Sylow 2-subgroups are conjugates to it. Note that since all elements of G are of the form $\sigma^a\tau^b$, we have

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

where $a \in \{0, 1, 2, 3, 4\}$. Now, using the relation $\tau\sigma = \sigma^2\tau$, we have

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

Using the same argument, we see that 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 of G, then

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

are all subgroups of order 2. For a subgroup H of G of order 10, since P_5 is the only sungroup of G of order 5, H contains $P_5 = \langle\sigma\rangle$. Thus, $\sigma^a\tau^b \in H \iff \tau^b \in H$. The only elements of the form τ^b which is of order 2 is τ^2. Thus, $H = \langle \sigma, \tau^2 \rangle$. Combining all the arguments, we have the following diagram of subgroups of G.

$$
\begin{tikzcd}
 & \{1\} \arrow[dl, dash, "5"'] \arrow[d, dash, "2"] \arrow[dr, dash] \arrow[drr, dash] \arrow[drrr, dash] \arrow[drrrr, dash] & & & & \\
\langle \psi_{1,1} \rangle \arrow[d, dash, "2"'] & \langle \psi_{0,2}^2 \rangle \arrow[d, dash, "2"'] & \langle \psi_{1,2}^2 \rangle \arrow[d, dash] & \langle \psi_{2,2}^2 \rangle \arrow[d, dash] & \langle \psi_{3,2}^2 \rangle \arrow[d, dash] & \langle \psi_{4,2}^2 \rangle \arrow[d, dash] \\
\langle \psi_{1,1}, \psi_{0,2}^2 \rangle \arrow[dr, dash, "2"'] & \langle \psi_{0,2} \rangle \arrow[d, dash, "5"'] & \langle \psi_{1,2} \rangle \arrow[dl, dash] & \langle \psi_{2,2} \rangle \arrow[dll, dash] & \langle \psi_{3,2} \rangle \arrow[dlll, dash] & \langle \psi_{4,2} \rangle \arrow[dllll, dash] \\
 & G = \mathrm{Gal}_{\mathbb{Q}}(E) & & & &
\end{tikzcd}
$$

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

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

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

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

we have $\mathbb{Q}(\alpha\zeta_5^2)^* = \langle \psi_{1,2} \rangle$. Using the same argument, we can get $\langle \psi_{r,2} \rangle^*$ for $r \in \{0,1,2,3,4\}$. Consider $\beta = \zeta_5 + \zeta_5^{-1}$, we have

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

The last equality is because the minimal polynomial of ζ_5 is $x^4 + x^3 + x^2 + x + 1$. Since $x^2 + x - 1 = 0$ has no rational roots, we have $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$. Therefore, we have the following corresponding diagram of the intermediate fields of ${}^{E}\!/\!_{\mathbb{Q}}$.

$$
\begin{tikzcd}
 & E = \mathbb{Q}(\alpha, \zeta_5) \arrow[dl, dash, "5"'] \arrow[dr, dash, "2"] \arrow[drr, dash] \arrow[drrr, dash] \arrow[drrrr, dash] \arrow[drrrrr, dash] & & & & & \\
\mathbb{Q}(\zeta_5) \arrow[d, dash, "2"'] & & \mathbb{Q}(\alpha, \beta) \arrow[d, dash, "2"'] & \mathbb{Q}(\alpha\zeta_5, \beta) \arrow[d, dash] & \mathbb{Q}(\alpha\zeta_5^2, \beta) \arrow[d, dash] & \mathbb{Q}(\alpha\zeta_5^3, \beta) \arrow[d, dash] & \mathbb{Q}(\alpha\zeta_5^4, \beta) \arrow[d, dash] \\
\mathbb{Q}(\beta) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash, "5"] & \mathbb{Q}(\alpha\zeta_5) \arrow[dll, dash] & \mathbb{Q}(\alpha\zeta_5^2) \arrow[dlll, dash] & \mathbb{Q}(\alpha\zeta_5^3) \arrow[dllll, dash] & \mathbb{Q}(\alpha\zeta_5^4) \arrow[dlllll, dash] \\
 & \mathbb{Q} & & & & &
\end{tikzcd}
$$

9 Cyclic Extensions

Lecture 27, 2025/03/17

Definition 9.1 (Abelian, Cyclic, or Solvable Galois Extensions).
A Galois extension ${}^{E}\!/_{F}$ is called **abelian**, **cyclic**, or **solvable** if $\mathrm{Gal}_F(E)$ has the corresponding property.

Lemma 9.1 (Dedekind's Lemma).
Let K and L be fields and let $\psi_i : L \to K$ $(0 \le i \le n)$ be the distinct non-zero homomorphisms. If $c_i \in K$ and

$$c_i\psi_1(\alpha) + \cdots + c_n\psi_n(\alpha) = 0 \quad \forall\, \alpha \in L,$$

then, $c_1 = \cdots = c_n = 0$.

Proof. Suppose the statement is false, so there exists $c_1, \ldots, c_n \in K$, not all 0 such that

$$c_1\psi_1(\alpha) + \cdots + c_n\psi_n(\alpha) = 0 \quad \forall\, \alpha \in L. \tag{1}$$

Let $m \ge 2$ be the minimal positive integer such that

$$c_1\psi_1(\alpha) + \cdots + c_m\psi_m(\alpha) = 0 \quad \forall\, \alpha \in L.$$

Since m is minimal, we have $c_i \neq 0$ for all $1 \le i \le m$. Since $\psi_1 \neq \psi_2$, we can choose $\beta \in L$ s.t. $\psi_1(\beta) \neq \psi_2(\beta)$. Moreover, we can assume $\psi_1(\beta) \neq 0$. By (1), we have

$$c_1\psi_1(\alpha\beta) + \cdots + c_m\psi_m(\alpha\beta) = 0 \quad \forall\, \alpha \in L.$$

By dividing the above equation by $\psi_1(\beta)$, we have

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha)\cdot\frac{\psi_2(\beta)}{\psi_1(\beta)} + \cdots + c_m\psi_m(\alpha)\cdot\frac{\psi_m(\beta)}{\psi_1(\beta)} = 0 \quad \forall\, \alpha \in L. \tag{2}$$

Consider (1) − (2), we obtain

$$c_2\left(1 - \frac{\psi_2(\beta)}{\psi_1(\beta)}\right)\psi_2(\alpha) + \cdots + c_m\left(1 - \frac{\psi_m(\beta)}{\psi_1(\beta)}\right)\psi_m(\alpha) = 0 \quad \forall\, \alpha \in L.$$

As $c_2\left(1-\frac{\psi_2(\beta)}{\psi_1(\beta)}\right)\neq 0$, we have a contradiction with the minimal choice of m (we have $m-1$ now). Thus, such $c_1,\dots,c_m$ do not exist and the lemma holds. $\square$

Theorem 9.2. Let F be a field and $n\in\mathbb{N}$. Suppose that $\mathrm{ch}(F)=0$ or p with $p\nmid n$. Assume also that x^n-1 splits over F.

(1) If the Galois extension E/F is cyclic of degree n, then $E=F(\alpha)$ for some $\alpha\in E$ with $\alpha^n\in F$. In particular, $x^n-\alpha^n$ is the minimal polynomial of α over F.

(2) If $E=F(\alpha)$ with $\alpha^n\in F$, then E/F is a cyclic extension of degree d with $d\mid n$ and $\alpha^d\in F$. In particular, $x^d-\alpha^d$ is the minimal polynomial of α over F.

Proof. Let $\zeta_n\in F$ be the primitive n-th root of unity, that is, $\zeta_n^n=1$ and $\zeta_n^d\neq 1$ for all $1\leq d<n$. Note that since $\mathrm{ch}(F)=0$ or p with $p\nmid n$, the polynomial x^n-1 is separable. Thus, $\{1,\zeta_n,\zeta_n^2,\dots,\zeta_n^{n-1}\}$ are distinct.

(1) Let $G=\mathrm{Gal}_F(E)=\langle\psi\rangle\cong C_n$, the cyclic group of order n. Apply Lemma 9.1 to $K=L=E$ and ψ_i, all elements of G, and $c_1=1, c_2=\zeta_n^{-1},\dots,c_n=\zeta_n^{-(n-1)}$. Since $c_i\neq 0$ for all $1\leq i\leq n$, there exists $u\in E$ such that

$$\alpha=u+\zeta_n^{-1}\psi(u)+\cdots+\zeta_n^{-(n-1)}\psi^{n-1}(u)\neq 0.$$

We have $1(\alpha)=\alpha$ and

$$\begin{aligned}\psi(\alpha)&=\psi(u)+\zeta_n^{-1}\psi^2(u)+\cdots+\zeta_n^{-(n-1)}\psi^n(u)=\alpha\zeta_n\\ \psi^2(\alpha)&=\alpha\zeta_n^2\\ &\ \ \vdots\\ \psi^{n-1}(\alpha)&=\alpha\zeta_n^{n-1}.\end{aligned}$$

Thus, $\alpha,\alpha\zeta_n,\dots,\alpha\zeta_n^{n-1}$ are conjugates to each other, i.e. they have the same minimal polynomial over F, say $p(x)$. Since $\alpha,\dots,\alpha\zeta_n^{n-1}$ are all distinct, it follows that $\deg(p(x))=n$. Also, since $p(x)\in F[x]$,

$$p(0)=\pm\alpha(\alpha\zeta_n)\cdots(\alpha\zeta_n^{n-1})=\alpha^n\zeta^{\frac{n(n-1)}{2}}\in F.$$

Since $\zeta_n\in F$, we have $\alpha^n\in F$. Since α is a root of $x^n-\alpha^n\in F[x]$ and $\deg(p(x))=n$, we have $p(x)=x^n-\alpha^n$. Moreover, since $F(\alpha)\subseteq E$ and $[F(\alpha):F]=n=[E:F]$, we obtain $E=F(\alpha)$.

(2) Suppose $\alpha^n \in F$ and let $p(x) \in F[x]$ be the minimal polynomial of α over F. Since α is a root of $x^n - \alpha^n \in F[x]$, so $p(x) \mid (x^n - \alpha^n)$. Thus, the roots of $p(x)$ are of the form $\alpha\zeta_n^i$ for some i and we have

$$p(0) = \pm\alpha^d \cdot \zeta_n^k$$

for some $k \in \mathbb{Z}$ and $d =$ number of roots of $p(x) = \deg(p)$. Since $p(0) \in F$ and $\zeta_n \in F$, we have $\alpha^d \in F$. Since $x^d - \alpha^d \in F[x]$ has α as a root, we know that $p(x) \mid (x^d - \alpha^d)$. Since $\deg(p) = d$ and $p(x)$ is monic, we have $p(x) = x^d - \alpha^d$.

Claim. $d \mid n$.

Proof of Claim. Suppose not, say $n = qd + r$ with $q \in \mathbb{Z}$ and $0 < r < d$. Since $\alpha^n, \alpha^d \in F$, we have

$$\alpha^r = \alpha^{n-qd} = (\alpha^n)(\alpha^d)^{-q} \in F.$$

Since $\alpha^r \in F$, we know that α is not a root of $x^r - \alpha^r \in F[x]$. It follows that $p(x) \mid (x^r - \alpha^r)$, a contradiction since $\deg(p) = d > r$. Thus, $d \mid n$. □

Write $n = md$. Since $p(x) = x^d - \alpha^d$, then the roots of $p(x)$ are

$$\alpha, \alpha\zeta_n^m, \dots, \alpha\zeta_n^{(d-1)m}.$$

Since $\zeta_n \in F$, $E = F(\alpha)$ is the splitting field of the separable polynomial $p(x)$ over F, thus E is Galois. If $\psi \in G = \mathrm{Gal}_F(E)$ satisfies $\psi(\alpha) = \alpha\zeta_n^m$, then $G = \langle\psi\rangle \cong C_d$. Thus, E/F is a cyclic extension of degree d.

□

Theorem 9.3. Let F be a field with $\mathrm{ch}(F) = p$, where p is a prime.

(1) If $x^p - x - a \in F[x]$ is irreducible, then its splitting field E/F is a cyclic extension of degree p.

(2) If E/F is a cyclic extension of degree p, then E/F is the splitting field of some irreducible polynomial $x^p - x - a \in F[x]$.

Proof.

(1) Let $f(x) = x^p - x - a$ and α a root of $f(x)$. Then since $\mathrm{ch}(F) = p$, we have

$$f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a = \alpha^p + 1 - \alpha - 1 - a = \alpha^p - \alpha - a = 0.$$

Thus, $\alpha + 1$ is also a root of $f(x)$. Similarly, $\alpha, \alpha + 1, \dots, \alpha + (p - 1)$ are all roots of $f(x)$. It follows that $E = F(\alpha, \alpha + 1, \dots, \alpha + (p - 1)) = F(\alpha)$ and $[E : F] = \deg(f) = p$. Since $\mathbb{Z}_p$ is the only cyclic group of order p, it follows that $\mathrm{Gal}_F(E) \cong \mathbb{Z}_p$. Indeed, $\mathrm{Gal}_F(E) = \langle \psi \rangle$ whether

$$\psi : E \to E \quad \text{by } \psi|_F = 1|_F \quad \text{and} \quad \psi(\alpha) = \alpha + 1.$$

(2) Let $G = \mathrm{Gal}_F(E) = \langle \psi \rangle \cong \mathbb{Z}_p$. Apply Lemma 9.1 to $K = L = E$ and ψ_i, all elements of G, and $c_1 = \cdots = c_p = 1$. Since $c_i \neq 0\,(1 \leq i \leq p)$, $\exists v \in E$ s.t.

$$\beta := v + \psi(v) + \cdots + \psi^{p-1}(v) \neq 0.$$

Note that $\psi^i(\beta)\, \forall \psi^i \in G$ where $1 \leq i \leq p-1$, we have $\beta \in F$. Set $u = \frac{v}{\beta}$. Since $\beta \in F$, we haev

$$\begin{aligned} u + \psi(u) + \cdots + \psi^{p-1}(u) &= \frac{v}{\beta} + \psi\left(\frac{v}{\beta}\right) + \cdots + \psi^{p-1}\left(\frac{v}{\beta}\right) \\ &= \frac{v + \psi(v) + \cdots + \psi^{p-1}(v)}{\beta} = \frac{\beta}{\beta} = 1. \end{aligned}$$

Now, we define $\alpha = 0 \cdot u - 1 \cdot \psi(u) - 2\psi^2(u) - \cdots - (p - 1)\psi^{p-1}(u)$. Then, we have

$$\psi(\alpha) = -\psi^2(u) - 2\psi^3(u) - \cdots - (p - 1)\psi^p(u).$$

Thus,

$$\psi(\alpha) - \alpha = \psi(u) + \psi^2(u) + \cdots + \psi^p(u) = 1.$$

It follows that $\psi(\alpha) = \alpha + 1$. Since $\mathrm{ch}(F) = p$, we have

$$\psi(\alpha^p) = \psi(\alpha)^p = (\alpha + 1)^p = \alpha^p + 1.$$

It follows that

$$\psi(\alpha^p - \alpha) = \psi(\alpha^p) - \psi(\alpha) = (\alpha^p + 1) - (\alpha + 1) = \alpha^p - \alpha.$$

Thus, $\alpha^p - \alpha$ is fixed by ψ. Since $G = \langle\psi\rangle$, we have $a = \alpha^p - \alpha \in F$ and α is a root of $x^p - x - a \in F[x]$. Since $[E : F] = p$, we have $[F(\alpha) : F]$ is a factor of p. Note that $\alpha \notin F$, as $\psi(\alpha) = \alpha + 1$, so α is not fixed by ψ. And since p is a prime, it follows that $[F(\alpha) : F] = p$ and $E = F(\alpha)$. Since $[F(\alpha) : F] = p$, we know that $x^p - x - a$ is the minimal polynomial of α over F.

$\square$

10 Solvability by Radicals

Lecture 29, 2025/03/21

10.1 Radical Extensions

Definition 10.1 (Radical Extension).
A finite extension E/F is **radical** if there exists a tower of fields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$$

such that $F_i = F_{i-1}(\alpha_i)$ where $\alpha_i \in F_i$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$ for all $i = 1, \dots, m$.

Lemma 10.1. If E/F is a finite separable radical extension, then its normal closure N/F is also radical.

Proof. Since E/F is a finite separable extension, by Theorem 7.4, $E = F(\beta)$ for some $\beta \in E$. Since E/F is a radical extension, there is a tower $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$ such that $F_i = F_{i-1}(\alpha_i)$ where $\alpha_i \in F_i$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$. Let $p(x) \in F[x]$ be the minimal polynomial of β and let $\beta = \beta_1, \beta_2, \dots, \beta_n$ be roots of $p(x)$. By definition of normal closure and Theorem 7.5,

$$N = E(\beta_2, \dots, \beta_n) = F(\beta_1, \beta_2, \dots, \beta_n).$$

Also, there is an F-isomorphism

$$\sigma_j : F(\beta) \to F(\beta_j) \quad \text{by} \quad \beta \mapsto \beta_j \quad \forall\, 2 \le j \le n.$$

Since N can be viewed as the splitting field of $p(x)$ over $F(\beta)$ and $F(\beta_j)$, respectively, by Theorem 4.4, there exists $\psi_j : N \to N$ which extends σ_j for $2 \le j \le n$. Thus, $\psi_j \in \mathrm{Gal}_F(N)$ and $\psi_j(\beta) = \beta_j$. Then, we have the following tower of fields

$$\begin{aligned} F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E = F(\beta_1) \\ &= F(\beta_1)\psi_2(F_0) \subseteq F(\beta_1)\psi_2(F_1) \subseteq \cdots \subseteq F(\beta_1)\psi_2(F_m) \\ &= F(\beta_1, \beta_2) \subseteq F(\beta_1, \beta_2)\psi_3(F_0) \subseteq F(\beta_1, \beta_2)\psi_3(F_1) \subseteq \cdots \subseteq F(\beta_1, \beta_2, \dots, \beta_n) = N. \end{aligned}$$

Note that since $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$, we have

$$\begin{aligned} F(\beta_1, \dots, \beta_{j-1})\psi_j(F_i) &= F(\beta_1, \dots, \beta_{j-1})\psi_j(F_{i-1}(\alpha_i)) \\ &= (F(\beta_1, \dots, \beta_{j-1})\psi_j(F_{i-1}))(\psi_j(\alpha_i)) \end{aligned}$$

and $(\psi_j(\alpha_i))^{d_i} = \psi_j(\alpha_i^{d_i}) \in \psi_j(F_{i-1})$. Thus, N/F is a radical extension. □

Remark. By Lemma 10.1, to consider a finite separable radical extension, we could instead consider its normal closure, which is Galois.

Definition 10.2 (Solvable by Radicals).
Let F be a field and $f(x) \in F[x]$. We say $f(x)$ is **solvable by radicals** if there exists a radical extension E/F such that $f(x)$ splits over E.

Remark. It is possible that $f(x) \in F[x]$ is solvable by radicals, but its splitting field is not a radical extension over F (see A10).

Remark. We recall that an expression involving only $+, -, \times, \div, \sqrt[n]{\cdot}$ is a radical. Let F be a field and $f(x) \in F[x]$ with separable irreducible factors. If $f(x)$ is solvable by radicals, by the definition of radical extensions, $f(x)$ has a radical root. Conversely, if $f(x)$ has a radical root, it is in some radical extension. By Lemma 10.1, the normal closure N/F of E/F is radical. Since $f(x)$ splits over N, $f(x)$ is solvable by radicals.

10.2 Radical Solutions

We have seen in A8 that the following result holds.

Lemma 10.2. Let E/F be a field extension, and let K, L be intermediate fields of E/F. Suppose that K/F is a finite Galois extension. Then, KL is a finite Galois extension of L and $\mathrm{Gal}_L(KL)$ is isomorphic to a subgroup of $\mathrm{Gal}_F(K)$.

Proof. Since K/F is a finite Galois extension, K is the splitting field of some $f(x) \in F[x]$ over F whose irreducible factors are separable. Since $F \subseteq L$, we know that KL is the splitting field of $f(x)$ over L, thus it is also Galois. Consider the map

$$\Gamma : \mathrm{Gal}_L(KL) \to \mathrm{Gal}_F(K) \quad \text{by} \quad \sigma \mapsto \sigma|_K.$$

Note that $\psi \in \mathrm{Gal}_L(KL)$ fixed L, thus F. Also, since ${}^{K}\!/_{F}$ is a Galois extension, $\psi(K) = K$. Thus, Γ is well-defined. Moreover, if $\psi|_K = 1|_K$, thus, ψ is trivial on K and L. Thus, ψ is trivial on KL. This shows that Γ is an injection. Thus, by the First Isomorphism Theorem, $\mathrm{Gal}_L(KL) \cong \operatorname{im}\Gamma$, a subgroup of $\mathrm{Gal}_F(K)$. ☐

Definition 10.3 (**Galois Group of a Polynomial**).
Let ${}^{E}\!/_{F}$ be the splitting field of a polynomial $f(x) \in F[x]$ whose irreducible factors are separable. The **Galois group** of $f(x)$ is defined to be $\mathrm{Gal}_F(E)$, denoted by $\mathrm{Gal}(f)$.

Theorem 10.3. Let F be a field with $\mathrm{ch}(F) = 0$ and $f(x) \in F[x] \setminus \{0\}$. Then, $f(x)$ is solvable by radicals $\iff$ its Galois group $\mathrm{Gal}(f)$ is solvable.

Proof. To be finished... ☐

Lecture 30, 2025/03/24

Proposition 10.4. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p. If $f(x)$ contains precisely two non-real roots in $\mathbb{C}$, then $\mathrm{Gal}(f) \cong S_p$.

Proof. One can show that the symmetric group S_n can be generated by cycles $(1\,2)$ and $(1\,2\,\dots\,n)$. Thus, to show $\mathrm{Gal}(f) \cong S_p$, it suffices to find a p-cycle and a 2-cycle in $\mathrm{Gal}(f)$. Let α be a root of $f(x)$. Since $f(x)$ is irreducible of degree p, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = p$. Thus, $p \mid |\mathrm{Gal}(f)|$. By Cauchy's Theorem, there exists an element of $\mathrm{Gal}(f)$ which is of order p, i.e. a p-cycle. Also, the complex conjugage map $\sigma(a + bi) = a - bi$ will interchange two non-real roots of $f(x)$ and fix all real roots. Thus, it is of order 2, i.e. a 2-cycle. By changing notation, if necessary, we have $(1\,2)$, $(1\,2\,\dots\,p) \in \mathrm{Gal}(f)$. It follows that $\mathrm{Gal}(f) \cong S_p$. ☐

Example. Consider $f(x) = x^5 + 2x^3 - 24x - 2 \in \mathbb{Q}[x]$, which is irreducible by Eisenstein's Criterion with $p = 2$. Since

$$f(-1) = 19 \quad f(1) = -23$$
$$\lim_{x\to\infty} f(x) = \infty \qquad \lim_{x\to-\infty} f(x) = -\infty,$$

there are at least 3 real roots of $f(x)$. Let $\alpha_1, \alpha_2, \dots, \alpha_5$ be roots of $f(x)$, i.e. $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_5)$. By considering the coefficients of x^4 and x^3 terms of $f(x)$, we have

$$\sum_{i=1}^{5} \alpha_i = 0 \quad \text{and} \quad \sum_{i<j} \alpha_i\alpha_j = 2.$$

From the first sum, we have

$$\left(\sum_{i=1}^{5} \alpha_i\right)^2 = \sum_{i=1}^{5} \alpha_i^2 + 2\sum_{i<j} \alpha_i\alpha_j = 0.$$

It follows that $\sum_{i=1}^{5} \alpha_i^2 = -4$. Thus, not all roots of $f(x)$ are real. It follows that $f(x)$ has three real roots and two non-real roots. By Proposition 10.4, $\mathrm{Gal}(f) \cong S_5$. Since S_5 is not solvavle, by Theorem 10.3, $f(x)$ is not solvable by radicals.

Note. Review this example for Test 2.

From the above example, we see a polynomial of degree 5 is not always solvable by radicals. Since $S_5 \subseteq S_n$ for all $n \geq 5$, we also have the following result.

Theorem 10.5 (**The Abel-Ruffini Theorem**).
A general polynomial $f(x)$ with $\deg(f) \geq 5$ is not solvable by radicals.

Example. The polynomial $x^7 - 2x^4 - 7x^3 + 14$ is solvable since $x^7 - 2x^4 - 7x^3 + 14 = (x^3 - 2)(x^4 - 7)$.

Cutoff for Test 2!

Indeed, we can show that "almost all" polynomial $f(x)$ of degree n satisfy $\mathrm{Gal}(f) \cong S_n$. More precisely, let

$$E_n(N) = \#\{f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] : |a_i| \leq N, \mathrm{Gal}(f) \subsetneq S_n\}$$

and let

$$T_n(N) = \#\{f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] : |a_i| \leq N\}.$$

Then by the large sieve, Gallagher proved that

$$\lim_{N \to \infty} \frac{E_n(N)}{T_n(N)} = 0.$$

Thus, we conclude that for "almost all" (i.e. desity 100%) $f(x) \in \mathbb{Z}[x]$ with $\deg(f) = n$, we have $\mathrm{Gal}(f) \cong S_n$. This is the Probablistic Galois Theory.

Probablistic Galois Theory: the study of the "density" of $f(x)$ with $\mathrm{Gal}(f) \cong S_n, A_n$, or etc.

For each $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ with $|a_i| \leq N$, there are $(2N+1)$ choices for each one of them. Thus, $T_n(N) = (2N+1)^n$. Note that if $a_0 = 0$, $f(x) = x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$, then

$$\mathrm{Gal}(f) = \mathrm{Gal}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \subseteq S_{n-1} \subsetneq S_n.$$

Thus, $E_n(N) \geq (2N+1)^{n-1}$.

Conjecture (van der Waerden): $E_n(N)$ is of size N^{n-1}.

The best result is due to Gallagher that $E_n(N) \leq CN^{n-\frac{1}{2}}(\log N)$.

11 Cyclotomic Extensions

For a prime p, we have seen in Chapter 2 that the p-th cyclotomic polynomial

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

is irreducible in $\mathbb{Q}[x]$. However, for a general $n \in \mathbb{N}$ with $n \geq 2$, $x^{n-1} + x^{n-2} + \cdots + x + 1$ is not always irreducible. For example, since $x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x^2 + 1)(x - 1)(x + 1)$, we have

$$\frac{x^4 - 1}{x - 1} = (x^2 + 1)(x + 1)$$

which is not irreducible in $\mathbb{Q}[x]$.

Thus, to generalize the definition of cyclotomic polynomial to general positive integer n, we note that

$$\Phi_p(x) = (x - \zeta_;)(x - \zeta_p^2) \cdots (x - \zeta_p^{p-1})$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$. For each $k = 1, 2, \dots, p - 1$, we have $\gcd(k, p) = 1$. So we can rewrite

$$\Phi_p(x) = \prod_{\substack{1 \leq k \leq p-1 \\ \gcd(k,p)=1}} (x - \zeta_p^k).$$

Let $\zeta_n = e^{\frac{2\pi i}{n}}$, which is of order n in the multiplicative group $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. We recall that for a general $k \in \mathbb{Z}$, the order of ζ_n^k is $\frac{n}{\gcd(n,k)}$, which is a divisor of n. In particular, the order of ζ_n^k is the same as the order of $\zeta_n \iff \gcd(n, k) = 1$.

Definition 11.1 (*n*-**th Cyclotomic Polynomial**).

The n-**th cyclotomic polynomial** is defined by

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \zeta_n^k) \quad \text{where } \zeta_n = e^{\frac{2\pi i}{n}}.$$

Definition 11.2 (**Primitive** *n*-**th Root of Unity,** *n*-**th Cyclotomic Extension**).

For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $\gcd(k, n) = 1$, we call ζ_n^k a **primitive** n-**th root of unity** in $\mathbb{C}$.

Also, the field $\mathbb{Q}(\zeta_n^k) = \mathbb{Q}(\zeta_n)$ is called the **n-th cyclotomic extension** over $\mathbb{Q}$, which is the splitting field of $\Phi_n(x)$.

Since the order of ζ_n^k is $\frac{n}{\gcd(n,k)}$, which is a positive divisor of n, we have the following result.

Proposition 11.1.
$x^n - 1 = \prod_{d|n} \Phi_d(x)$, where d runs through all positive divisors of n.

Example. $x^6-1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2-x+1)$.

Lecture 32, 2025/03/28

Let $\psi \in G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$. Since ζ_n is of order n, $\psi(\zeta_n)$ is also of order n. It follows that $\psi(\zeta_n) = \zeta^k$ for some k with $\gcd(k,n) = 1$. Thus, ψ permutes the set

$$\{\zeta_n^k : 1 \le k \le n, \gcd(k,n) = 1\}.$$

Since the above set contains all roots of $\Phi_n(x)$, it follows that $\Phi_n(x) \in \mathbb{Q}(\zeta_n)^G[x] = \mathbb{Q}[x]$. Thus

Theorem 11.2 (Gauss). $\Phi_n(x) \in \mathbb{Z}[x]$ and is irreducible.

Theorem 11.3 (Gauss). We have $\mathrm{Gal}_{\mathbb{Q}}(\zeta_n) \cong \left(\mathbb{Z}/\langle n\rangle\right)^*$, the unit group of $\mathbb{Z}/\langle n\rangle$. In particular, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where φ is the Euler totient function.

Proof. We have seen that for $\psi \in \mathrm{Gal}_{\mathbb{Q}}(\zeta_n)$, $\psi(\zeta_n) = \zeta_n^k$ for some k with $\gcd(k,n) = 1$. Define the maps

$$\Gamma : \left(\mathbb{Z}/\langle n\rangle\right)^* \to \mathrm{Gal}_{\mathbb{Q}}(\zeta_n) \quad k + \langle n\rangle \mapsto (\psi_k : \zeta_n \mapsto \zeta_n^k)$$

which is a bijection. Also, for $k_1k_2 + \langle n\rangle \in \left(\mathbb{Z}/\langle n\rangle\right)^*$, we have

$$\psi_{k_1k_2}(\zeta_n) = \zeta_n^{k_1k_2} = (\zeta_n^{k_1})^{k_2} = (\psi_{k_1}(\zeta_n))^{k_2} = (\psi_{k_1} \circ \psi_{k_2})(\zeta_n).$$

Thus, Γ is a group isomorphism and we have $\mathrm{Gal}_{\mathbb{Q}}(\zeta_n) \cong \left(\mathbb{Z}/\langle n\rangle\right)^*$. □

Theorem 11.4. A quadratic extension of $\mathbb{Q}$ in $\mathbb{C}$ is contained in some $\mathbb{Q}(\zeta_n)$.

Proof. A quadratic extension $E/\mathbb{Q}$ is the splitting field of $ax^2 + bx + c \in \mathbb{Q}[x]$ with $a \neq 0$. Since ax^2+bx+c has roots $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$, we have $E = \mathbb{Q}(\sqrt{b^2-4ac})$, where $b^2-4ac \in \mathbb{Q}$. Write $b^2-4ac = \frac{d}{q}$ for some $d \in \mathbb{Z}$, $q > 0$, and $\gcd(d, q) = 1$. Since $q^2\left(\frac{d}{q}\right) = dq$, we have $\mathbb{Q}\left(\sqrt{\frac{d}{q}}\right) = \mathbb{Q}(\sqrt{dq})$. Thus, it suffices to consider a quadratic extension of the form $\mathbb{Q}(\sqrt{D})$ where D is a square-free integer. Note that $\mathbb{Q}(\sqrt{1}) = \mathbb{Q}$ and $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$. Also, for the distinct primes p_1, p_2, if $\mathbb{Q}(\sqrt{p_1}) = \mathbb{Q}(\zeta_{n_1})$ and $\mathbb{Q}(\sqrt{p_2}) = \mathbb{Q}(\zeta_{n_2})$, then $\sqrt{p_1p_2} \in \mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}) \subseteq \mathbb{Q}(\zeta_{n_1n_2})$ since $\zeta_{n_1} = \zeta_{n_1n_2}^{n_1}$ and $\zeta_{n_2} = \zeta_{n_1n_2}^{n_2}$. It follows that $\mathbb{Q}(\sqrt{p_1p_2}) \subseteq \mathbb{Q}(\zeta_{n_1n_2})$. Thus, to prove this theorem, it suffices to consider the case when $D = p$. If $p = 2$, since $(1+i)^2 = 2i$ and $(1+i) \in \mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, we haev $\sqrt{2i} = \sqrt{2}\cdot\sqrt{i} \in \mathbb{Q}(\zeta_4)$. Also, $i \in \mathbb{Q}(\zeta_4)$ implies that $\sqrt{i} \in \mathbb{Q}(\zeta_8)$. It follows that

$$-\sqrt{2} = \sqrt{2}\sqrt{i}(\sqrt{i})^3 \in \mathbb{Q}(\zeta_8) \quad \text{and} \quad \mathbb{Q}(\zeta_2) \subseteq \mathbb{Q}(\zeta_8).$$

Now, let p be an odd prime. The minimal polynomial of ζ_p is

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{\substack{1\le k\le p-1\\ \gcd(k,p)=1}} (x - \zeta_p^k).$$

The discriminant of $\Phi_p(x)$ is defined to be

$$D(\Phi_p) = \prod_{\substack{1\le k\le p-1\\ \gcd(k,p)=1}} (\zeta_p^i - \zeta_p^j)^2.$$

One can verify that $D(\Phi_p) = (-1)^{\frac{p-1}{2}} p^{p-2}$ (exercise). If $p \equiv 1 \pmod 4$, we get $\sqrt{p} \in \mathbb{Q}(\zeta_p)$. If $p \equiv 3 \pmod 4$, we have $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$. Since $\sqrt{p} = \pm i\sqrt{-p}$ and $i \in \mathbb{Q}(\zeta_4)$, we have $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$. In all cases, we have $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$ and $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_{4p})$. ☐

Remark. Note that $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{D})) \cong 1$ or $\mathbb{Z}/\langle 2\rangle$, which is an abelian group. The above term is a special case of a theorem of Kronecker-Weber, which states that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Lemma 11.5. Let p be a prime and $m \in \mathbb{N}$ with $p \nmid m$. Then for $a \in \mathbb{Z}$, $p \mid \Phi_m(a) \iff p \nmid a$ and $a \pmod p$ has order m in $\mathbb{F}_p^*$.

Lecture 33, 2025/03/31

We recall Euclid's Theorem that there are infinitely many primes. This is equivalent to saying that there are infinitely many primes $p \equiv 1 \pmod 2$.

Question: How about $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$?

The same proof as the one for Euclid's Theorem can be adapted to prove the $p \equiv 3 \pmod 4$ case, but not the $p \equiv 1 \pmod 4$ case.

Question: For any $m \in \mathbb{N}$, let $k \in \mathbb{Z}$ with $\gcd(k, m) = 1$. Are there infinitely many primes of the form $p \equiv k \pmod m$?

Another way to formulate Euclid's Theorem is that for $f(x) = x$ (or $f(x) = x + 1$, $x + k$), the set of prime divisors of the sequence $f(1), f(2), \dots$ is infinite.

Lemma 11.6. If $f(x) \in \mathbb{Z}[x]$ is monic and $\deg(f) \geq 1$, the set of prime divisors of the nonzero integers in the sequence $f_1, f_2, \dots$ is infinite.

Theorem 11.7 (**Dirichlet's Theorem**).
For $m \in \mathbb{N}$, $m \geq 2$, there are infinitely many primes p s.t. $p \equiv 1 \pmod m$.

Proof. Consider $\Phi_m(x)$. By Lemma 11.6, there are infinitely many prime divisors p of the nonzero integers in the sequence $\Phi_m(2), \Phi_m(3), \dots$. If $p \mid \Phi_m(a)$ for some integer $a \geq 2$, by Lemma 11.5, the reduction of a mod p has order m in $\mathbb{F}_p^*$. Since $\mathbb{F}_p^*$ has order $(p-1)$, we have $m \mid (p-1)$, i.e. $p \equiv 1 \pmod m$. □

Remark. Dirichlet's Theorem indeed gives a much stronger result. Let

$$\pi(x) = \#\{p \leq x,\ p \text{ prime}\} = \frac{x}{\log x} + \text{Error}.$$

Then, Dirichlet's Theorem states that

$$\begin{aligned}\pi(x,1,m) &= \#\{p \le x,\ p \text{ prime},\ p \equiv 1 \pmod{m}\} \\ &= \frac{1}{\psi(m)} \cdot \frac{x}{\log x} + \text{Error}.\end{aligned}$$

Check out PMATH 440, Analytic Number Theory!

Theorem 11.8. Let A be a finite abelian group. Then, there exists a Galois extension ${}^{E}\!/\!_{\mathbb{Q}}$ with $E = \mathbb{Q}(\zeta_n)$ and $\mathrm{Gal}_{\mathbb{Q}}(E) \cong A$.

Proof. Since A is a finite abelian group, we can write

$$A \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \quad \text{where } C_{k_i} \text{ is a cyclic group of order } k_i.$$

Choose primes $p_1 < p_2 < \cdots < p_s$ s.t.

$$\begin{aligned} p_1 &\equiv 1 \pmod{k_1} \\ p_2 &\equiv 1 \pmod{k_2} \\ &\vdots \\ p_s &\equiv 1 \pmod{k_s}. \end{aligned}$$

Such primes exist by Theorem 11.7. Let $n = p_1 p_2 \cdots p_s$ and consider $E = \mathbb{Q}(\zeta_n)$. Then,

$$\begin{aligned} G = \mathrm{Gal}_{\mathbb{Q}}(E) &\cong \left(\mathbb{Z}/\langle n\rangle\right)^* \\ &\cong \left(\mathbb{Z}/\langle p_1\rangle\right)^* \times \left(\mathbb{Z}/\langle p_2\rangle\right)^* \times \cdots \times \left(\mathbb{Z}/\langle p_s\rangle\right)^* \\ &\cong C_{p_1-1} \times C_{p_2-1} \times \cdots \times C_{p_s-1}. \end{aligned}$$

Write $p_1 - 1 = k_1 d_1, \ldots, p_s - 1 = k_s d_s$. Since C_{p_1-1} is cyclic, there exists a subgroup $D_{d_i} \cong C_{d_i}$ of C_{p_i-1}, which is of order d_i. Moreover, ${}^{C_{p_i-1}}\!/\!_{D_{d_i}} \cong C_{k_i}$. Define

$$H \cong D_{d_1} \times \cdots \times D_{d_s}$$

which is a normal subgroup of G. Also, ${}^{G}\!/\!{}_{H} \cong C_{k_1} \times \cdots \times C_{k_s} \cong A$. Let $L = H^* = E^H$.

$$
\begin{tikzcd}
E = \mathbb{Q}(\zeta_n) \arrow[r, leftrightarrow] \arrow[d, dash] & \{1\} \arrow[d, dash] \\
L = E^H \arrow[r, leftrightarrow] \arrow[d, dash] & H \arrow[d, dash] \\
\mathbb{Q} \arrow[r, leftrightarrow] & G
\end{tikzcd}
$$

Since H is a normal subgroup of G, by Theorem 8.4, ${}^{L}\!/\!{}_{\mathbb{Q}}$ is a Galois extension and

$$\mathrm{Gal}_{\mathbb{Q}}(L) \cong {}^{G}\!/\!{}_{H} \cong A.$$

$\square$

END OF PMATH 348!