PMATH 348 Notes

Winter 2024

Based on Professor Yu-Ru Liu's Lectures

Contents

Lecture 1, 2024/01/08

1 Review of Ring Theory

1.1 Introduction to Galois Theory

Let's look at Polynomial Equations:

- Linear Equations. Let $ax + b = 0$ and $a, b \in \mathbb{R}$ and $a \neq 0$. Its solution is $x = -b/a$.
- Qudratic Equations. Consider $ax^2 + bx + c = 0$ and $a, b, c \in \mathbb{R}$ and $a \neq 0$. Its solutions are:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Definition An expression involving only addition, subtraction, multiplication, division and taking n-th root is called a **radical**.

- Cubic Equations (Tartaglia, del Ferro, Fontana). All cubic equations can be reduced to $x^3+px = q$. A solution of the above equation is of the following form:

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

- Quartic Equations (Ferrari). See Bonus 1.
- Quintic Equations.
  - This question were attempted by Euler, Bezout and 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.

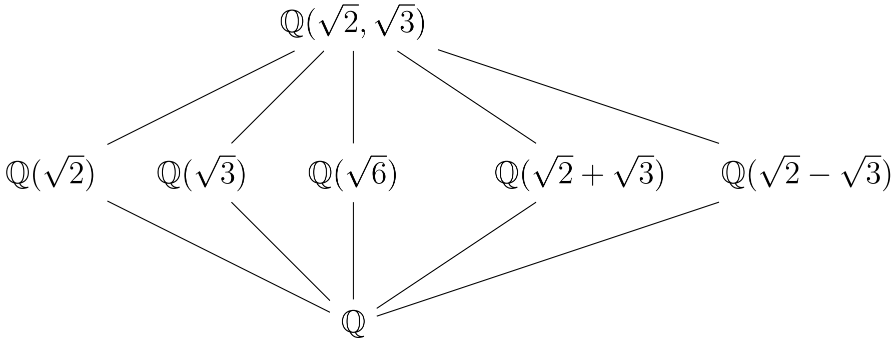
Question: Given a quintic equation, is it solvable by radicals?

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

Two main steps of Galois Theory:

Step 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 but our knowledge about fields is limited.

Example Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, the smallest field containing $\mathbb{Q}, \sqrt{2}, \sqrt{3}$.



Step 2: Link the field $\mathbb{Q}(\alpha)$ to a group. More precisely, we associate the field extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ to the group:

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\psi \in \mathrm{Aut}(\mathbb{Q}(\alpha)) : \psi(x) = x \text{ for all } x \in \mathbb{Q}\} \tag{1}$$

It is the set of all automorphisms in $\mathbb{Q}(\alpha)$ that fixes elements in $\mathbb{Q}$. Where we recall that the automorphism group is:

$$\mathrm{Aut}(R) = \{\phi : R \to R : \phi \text{ is an isomorphism}\}$$

One can show that if α is "good", say "algebraic", then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite! We will prove there is a one-to-one correspondence between the intermediate fields of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and the subgroups of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$.

1.2 Review of Ring Theory

Definition A set R is a **(unitary) ring** if it has two operations, addition $+$ and multiplication $\cdot$ such that for all $a, b, c \in R$:

1. $a + b \in R$.
2. $a + b = b + a$.
3. $a + (b + c) = (a + b) + c$.
4. There exists $0 \in R$ such that $a + 0 = a = 0 + a$.
5. There exists $-a \in R$ such that $a + (-a) = 0 = (-a) + a$.

6. $a \cdot b \in R$.
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
8. There exists $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a$.
9. **(Distributive Law)** $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

The ring R is **commutative** if we have $ab = ba$. In PMATH 348, we only consider commutative rings.

Lecture 2, 2024/01/10

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

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

Definition A commutative ring $R \neq \{0\}$ is an **integral domain** if for all $a, b \in R$ with $ab = 0$, then $a = 0$ or $b = 0$.

Example $\mathbb{Z}$ is an integral domain. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (p prime) are all fields.

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

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

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

Note Yu-Ru uses $\langle a \rangle$ to denote the principal ideal generated by a. But I will use (a) in this note.

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

Example The ring of integers $\mathbb{Z}$.

- $\mathbb{Z}$ is an integral domain.
- The units of $\mathbb{Z}$ are $\{1, -1\}$.
- **Division Algorithm in $\mathbb{Z}$:** For $a, b \in \mathbb{Z}$ and $a \neq 0$. We can write $b = qa + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < |a|$.

- Using the division algorithm we can show that all ideals of $\mathbb{Z}$ are $I = (n) = n\mathbb{Z}$. 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 $\mathbb{Q}$ (The field of fractions of $\mathbb{Z}$).
$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

Example The polynomial ring $F[x]$.

Let F be 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 $f(x)$ is **monic**.
- If $a_m \neq 0$, we define the **degree** of f to be $\deg(f) = m$. And we define $\deg(0) = -\infty$.
- For $f(x), g(x) \in F[x]$, we have $\deg(fg) = \deg(f) + \deg(g)$.
- $F[x]$ is an integral domain.
- The units of $F[x]$ are $F^* = F \setminus \{0\}$.
- **Divsion Algorithm in** $F[x]$: For $f(x), g(x) \in F[x]$ with $f(x) \neq 0$, we can write:
$$g(x) = q(x)f(x) + r(x)$$
where $q(x), r(x) \in F[x]$ with $\deg(r) < \deg(f)$.
- **Remark:** We define $\deg(0) = -\infty$ because we need $\deg(fg) = \deg(f) + \deg(g)$, so if $g = 0$, then for all $f \in F[x]$ we get $fg = 0$, so $\deg(0) = \deg(0) + \deg(f)$ for all $f(x)$, it forces us to define $\deg(0) = \infty$ or $-\infty$. And in the division algorithm, if the remainder is $r(x) = 0$, we want to have $\deg(r) < \deg(f)$, so define $\deg(r) = -\infty$ is a good choice.
- Using the division algorithm, we can prove all ideals I of $F[x]$ is of the form $I = (f(x))$. Note that if $f(x)$ is monic, then it is unique.
- Consider all fields containing $F[x]$. Their intersection is its field of fractions, 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 Let I be an ideal of a ring R. We recall that the additive quotient group R/I is a ring with the multiplication $(r + I)(s + I) = rs + I$. Then the unity of R/I is $1 + I$. This is the **quotient ring** R/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 and we have:

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

by the isomorphism $\tilde{\theta} : R/\operatorname{Ker}\theta \to \operatorname{im}\theta$ defined by $\tilde{\theta}(r + \operatorname{Ker}\theta) = \theta(r)$.

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

Definition 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 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 is prime.

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

1. I is a maximal ideal if and only if R/I is a field.
2. I is a prime ideal if and only if R/I is an integral domain.

2 Integral Domains

2.1 Irreducibles and Primes

Definition Let R be an integral domain and $a, b \in R$. We say a **divdies** b, denoted by $a \mid b$, if $b = ca$ for some $c \in R$.

We recall that in $\mathbb{Z}$, if $n \mid m$ and $m \mid n$, then $n = \pm m$ and $(n) = (m)$.

Also, in $F[x]$, if $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f = cg$ for some $c \in F^*$ and $(f(x)) = (g(x))$.

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. $(a) = (b)$.

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

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

(3) $\implies$ (1). If $(a) = (b)$, then $a \in (a) = (b)$. Then $a = ub$ for some $u \in R$, that is $b \mid a$. Similarly, since $b \in (a)$, we have $a \mid b$. $\square$

Lecture 3, 2024/01/12

Definition 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 $b \mid a$. By Prop 2.1, $\sim$ is an equivalence relation in R. More precisely we have:

1. $a \sim a$ for all $a \in R$.
2. If $a \sim b$ then $b \sim a$.
3. If $a \sim b$ and $b \sim c$, then $a \sim c$.

Also, we can show that (see Piazza Exercise):

1. If $a \sim a'$ and $b \sim b'$, then $ab \sim a'b'$.
2. If $a \sim a'$ and $b \sim b'$, then $a \mid b$ if and only if $a' \mid b'$.

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 $3 + 2\sqrt{3} \sim \sqrt{3}$ by definition. In $\mathbb{Z}$, if $a \mid b$ and $b \mid a$, then $a = \pm b$. In $F[x]$, if $f(x) \mid g(x)$ and $g(x) \mid f(x)$, we get $f(x) = cg(x)$ for $c \in F^*$. But we just saw it is not the case in $\mathbb{Z}[\sqrt{3}]$.

Note When we write the word "domain", it just means "integral domain".

Definition Let R be a domain. We say $p \in R$ is **irreducible** if $p \neq 0$ and not a unit, and if $p = ab$ with $a, b \in R$, then either a or b is a unit in R. Suppose a is not 0 and not a unit, then we say a is **reducible** if a is not irreducible.

Example Let $R = \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ and $p = 1 + \sqrt{-5}$. We claim p is irreducible in R. For $d = m + n\sqrt{-5}$, the **norm** of d is defined to be:

$$N(d) = (m + n\sqrt{-5})(m - n\sqrt{-5}) = m^2 + 5n^2 \in \mathbb{Z}_{\geq 0}$$

One can check that $N(ab) = N(a)N(b)$ for all $a, b \in R$ and $N(d) = 1$ if and only if d is a unit. (Piazza Exercise and A1). Now suppose that $p = ab$ in R. Then:

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

Note that $6 = 1 \cdot 6 = 2 \cdot 3$. For all $d \in R$, if $N(d) = m^2 + 5n^2 = 2$ with $m, n \in \mathbb{Z}$, then $n = 0$. So we get $m^2 = 2$, but this is also impossible. Hence $N(d) \neq 2$ (So nothing has norm 2 in R). Similarly nothing has norm 3. Thus we have either $N(a) = 1$ or $N(b) = 1$, that is, either a or b is a unit in R. Therefore p is irreducible.

Proposition 2.2 Let R be a domain and let $p \in R$ with $p \neq 0$ and 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 $p \sim b$.

Proof: (1) $\implies$ (2). If $p = ad$, then by (1), either d or a is a unit. If d is a unit then $d \sim 1$. If a is a unit, then $d \sim p$.

(2) $\implies$ (3). If $p \sim ab$, then $ab \mid p$, thus $b \mid p$. By (2), either $b \sim 1$ or $b \sim p$. In the first case we get $p \sim a$. In the second case we get $p \sim b$ trivially.

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

(4) $\implies$ (1). If $p = ab$, then by (4), $p \sim a$ 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 a domain and $p \neq 0$, we get $ub = 1$ so b is a unit. Similarly, if $p \sim b$ then a is a unit. Thus (1) follows. $\square$

Definition Let R be a domain and $p \in R$. We say p is **prime** if $p \neq 0$, 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 if and only if q is prime. (Exericse). 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 a domain and $p \in R$. If p is a prime, then p is irreducible.

Proof: Let $p \in R$ be a prime. If $p = ab$ in R, then $p \mid ab$. Since p is prime we get $p \mid a$ or $p \mid b$. If $p \mid a$, write $a = dp$ for some $d \in R$, then since R is commutative, we have that:

$$a = dp \implies p = (dp)b = p(db) \implies p(1 - db) = 0$$

Since R is domain and $p \neq 0$, we get $db = 1$ so b is a unit. Similarly if $p \mid b$, we can show that a is a unit. It follows that p is irreducible. $\square$

Example The converse of Prop 2.3 is false. Consider $R = \mathbb{Z}[\sqrt{-5}]$ and $p = 1 + \sqrt{-5} \in R$. We showed that p is irreducible in R. But, p is NOT prime in R. Note that:

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

If p is prime then $p \mid 2$ or $p \mid 3$. If $p \mid 2$, say $2 = pq$ for some $q \in R$. It follows that :

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

which is not possible since $N(q) \in \mathbb{Z}$. Similarly $p \mid 3$ is not possible. Hence p is not prime in $R = \mathbb{Z}[\sqrt{-5}]$.

Lecture 4, 2024/01/15

In $\mathbb{Z}$, a prime p is both irreducible and prime. Similarly, in $F[x]$ where F is a field, an irreducible polynomial $f(x)$ is both prime and irreducible and prime.

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

Example Find a ring and find an element that is irreducible but not prime. (Piazza Exercises)

2.2 Ascending Chain Conditions

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

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

of principal ideals in R, then there exists an integer $n \in \mathbb{N}$ such that for all $k \geq n$ we have $(a_n) = (a_k)$. That is, $(a_n) = (a_{n+1}) = (a_{n+2}) \cdots$ stabilizes.

Example We claim that $\mathbb{Z}$ satisfies ACCP. If $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$ in $\mathbb{Z}$ then:

$$a_2 \mid a_1,\ a_3 \mid a_2,\ a_4 \mid a_3, \cdots$$

Taking absolute values gives $|a_1| \geq |a_2| \geq |a_3| \geq \cdots$. Since each $|a_i| \geq 0$ is an integer, by the well ordering principle, 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 $(a_n) = (a_k)$ for all $k \geq n$. hence $\mathbb{Z}$ satisfies ACCP.

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

$$(x) \subsetneq \left(\frac{1}{2}x\right) \subsetneq \left(\frac{1}{4}x\right) \subsetneq \cdots$$

Thus R does not satisfy ACCP.

Theorem 2.4 Let R be a doamin satisfying ACCP. If $a \in R$ with $a \neq 0$ and a is not a unit, then a is a product of irreducible elements of R.

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

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots$$

Since $a \not\sim a_1$ and $a_1 \not\sim a_2$ and so on, by Prop 2.1 we have:

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

which contradicts ACCP. Hence such a does not exist. The result follows. □

Theorem 2.5 If R is a domain satisfying ACCP, so is $R[x]$.

Lecture 5, 2024/01/17

Proof: Suppose that $R[x]$ does not satisfy ACCP. Then there exists a chain of principal ideals in $R[x]$:

$$(f_1) \subsetneq (f_2) \subsetneq (f_3) \subsetneq \cdots$$

Thus $f_{i+1} \mid f_i$ for all $i \in \mathbb{N}$. Let a_i denote the leading coefficient of f_i for each $i \in \mathbb{N}$. Since $f_{i+1} \mid f_i$, we have $a_{i+1} \mid a_i$ for each $i \in \mathbb{N}$. Why: Say $f_{i+1}(x) = a_{i+1}x^n + p(x)$ and $f_i(x) = a_i x^m + q(x)$, then $f_i = hf_{i+1}$ where $h(x) = h_s x^s + \cdots + h_1 x + h_0$ so:

$$a_i x^m + q(x) = (a_{i+1}x^n + p(x))(h_s x^s + \cdots + h_1 x + h_0) = a_{i+1}h_s x^{n+s} + \cdots$$

The leading coefficient on the LHS is a_i and the leading coefficient on the RHS is $a_{i+1}h_s$, so $a_{i+1}h_s = a_i$ and this is why $a_{i+1} \mid a_i$. Thus we have:

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

Since R satisfies ACCP, there exists $n \in \mathbb{N}$ such that $(a_n) = (a_k)$ for all $k \geq n$. Thus $a_n \sim a_{n+1} \sim a_{n+2} \sim \cdots$. For $m \geq n$, let $f_m = gf_{m+1}$ for some $g(x) \in R[x]$. If b is the leading coefficient of $g(x)$, then $a_m = ba_{m+1}$. Since $a_m \sim a_{m+1}$, b is a unit in R by Proposition 2.1. However, $g(x)$ is not a unit in $R[x]$ since $(f_m) \neq (f_{m+1})$. Thus $g(x) \neq b$ and we have $\deg(g) \geq 1$. by the product formula for $R[x]$, it implies that:

$$\deg(f_m) = \underbrace{\deg(g)}_{\geq 1} + \deg(f_{m+1}) \implies \deg(f_m) > \deg(f_{m+1})$$

and it is true for all $m \geq n$. Thus we have:

$$\deg(f_n) > \deg(f_{n+1}) > \deg(f_{n+2}) > \cdots$$

which leads to a contradiction since $\deg(f_i) \geq 0$ are nonnegative integers. It follows that $R[x]$ satisfies ACCP. $\square$

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

2.3 Unique Factorization Domains and Principal Ideal Domains

Definition A domain R is called a **unique factorization domain (UFD)** is it satisfies the following conditions:

1. If $a \in R$, $a \neq 0$ and 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 each p_i and q_j are irreducible, then $r = s$ and $p_i \sim q_j$ for each $i = 1, \cdots, r$ (after possible reordering).

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

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 $a = p_1 \cdots p_k$ and $b = q_1 \cdots q_l$ and $d = r_1 \cdots r_m$. (Here we allow k, l or m to be 0 to take care of the case that 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. It follows that $p \mid a$ 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 for $F[x]$.

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

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

where $1 \pm \sqrt{-5}$, 2, 3 are irreducibles. However $(1+\sqrt{-5}) \not\sim 2$ and $(1+\sqrt{-5}) \not\sim 3$ since $N(1+\sqrt{-5}) = 6$, $N(2) = 4$ and $N(3) = 9$. Thus the not every element in $\mathbb{Z}[\sqrt{-5}]$ admits a unqiue factorization.

Example Even though $R = \mathbb{Z}[\sqrt{-5}]$ is not a UFD, we claim that R satisfies ACCP. If $(a_1) \subseteq (a_2) \subseteq \cdots$ in R, then $a_2 \mid a_1$, $a_3 \mid a_2$ and so on. Taking their 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, there is a $n \geq N$ with $N(a_n) = N(a_k)$ for all $k \geq n$. Since $N(d) = 1$ if and only if d is a unit in R, it follows that $a_{i+1} \sim a_i$ for all $i \geq n$. Thus $(a_i) = (a_{i+1})$ for all $i \geq n$.

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

---------- Lecture 6, 2024/01/19 ----------

Proposition 2.7 If R is a UFD, and $a, b \in R \setminus \{0\}$. If $p_1, \cdots, p_k$ are the non-associate primes dividing a and b ($p_i \not\sim p_j$ for all $i \neq j$). Say:

$$a \sim p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \text{and} \quad b \sim p_1^{\beta_1} \cdots p_k^{\beta_k}$$

Then we have:

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

Proof: See Piazza Exercise. $\square$

Remark If R is a UFD with $d, a_1, \cdots, a_m \in R$, we have (exercise):

$$\gcd(da_1, \cdots, da_m) \sim d\gcd(a_1, \cdots, a_m)$$

Theorem 2.8 Let R be a domain, the following are equivalent:

1. R is a UFD.
2. R satisfies the ACCP and $\gcd(a, b)$ exists for all nonzero $a, b \in R$.
3. R satisfies the ACCP and every irreducible elements in R is prime.

Proof: (1) $\implies$ (2). By Prop 2.7, $\gcd(a, b)$ exists. Also suppose that there exists:

$$(0) \neq (a_1) \subsetneq (a_2) \subsetneq \cdots \quad \text{in } R$$

Since $(a_1) \neq R$, we know a_1 is not a unit and not a zero. 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:

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

where $0 \leq d_{i,j} \leq k_j$ for all $1 \leq j \leq r$. Thus there are only finitely many non-associated choices for a_i and so there exists $m \neq n$ with $a_m \sim a_n$. This implies that $(a_m) = (a_n)$ and this 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 $d = \gcd(a, p)$. 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 get $p \mid a$. In the second case, since $d = \gcd(a, p) \sim 1$, then $\gcd(ab, pb) \sim b\gcd(a, p) \sim b$. Since $p \mid ab$ and $p \mid pb$, we have $p \mid \gcd(ab, pb)$. Then it follows that $p \mid b$.

(3) $\implies$ (1). If R satisfies the ACCP, by Theorem 2.4, for $a \in R$ with $a \neq 0$ and a is not a unit, a is a product of irreducible elements of R. Thus it suffices to show such factorization is unique. Suppose we have:

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

where p_i and q_j are irreducible. Since p_1 is a prime, then $p_1 \mid q_j$ for some j, WLOG assume $j = 1$. Since q_1 is irreducible, by Prop 2.2 we have $p_1 \sim q_1$. Since $p_1 \sim q_1$ and $p_1 \cdots p_r \sim q_1 \cdots q_s$, we have $p_2 \cdots p_r \sim q_2 \cdots q_s$. Continue the above process to get $r = s$ and $p_2 \sim q_2$ and $p_r \sim q_r$. $\square$

Definition An integral domain R is a **principal ideal domain (PID)** if every ideal is **principal**, that is, every ideal is of the form $(a) = aR$ for some $a \in R$.

Example $\mathbb{Z}$ and $F[x]$ are PIDs.

Example Although all ideals of $\mathbb{Z}_n$ are principal, $\mathbb{Z}_n$ is not a PID unless n is a prime in $\mathbb{Z}$, since $\mathbb{Z}_n$ is not even a domain when n is not prime.

Example A field F is a PID since its only ideals are (0) and (1).

Proposition 2.9 Let R be a PID and let $a_1, \cdots, a_n$ be nonzero elements of R. Then $d \sim \gcd(a_1, \cdots, a_n)$ exists and there exists $r_1, \cdots, r_n \in R$ such that:

$$\gcd(a_1, \cdots, a_n) = r_1 a_1 + \cdots + r_n a_n$$

Proof: Let $A = (a_1, \cdots, a_n) = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\}$ which is an ideal of R. Since R is a PID, there exists $d \in R$ such that $A = (d)$. Thus:

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

for some $r_1, \cdots, r_n \in R$. We claim $d \sim \gcd(a_1, \cdots, a_n)$. Since $A = (d)$ and $a_i \in A$, we have $a_i \in (d) \iff d \mid a_i$ for all i. Also, if $r \mid a_i$ for all i, then $r \mid (r_1 a_1 + \cdots + r_n a_n)$, thus $r \mid d$. By definition of gcd, we have $d \sim \gcd(a_1, \cdots, a_n)$. $\square$

Lecture 7, 2024/01/22

Theorem 2.10 Every PID is a UFD.

Proof: If R is a PID, by Theorem 2.8 and Prop 2.9, it suffices to show R satisfies the ACCP. If we have $(a_1) \subseteq (a_2) \subseteq \cdots$ in R, wrtie $A = \bigcup_{i=1}^{\infty} (a_i)$. Then A is an ideal (Exercise). Since R is a PID, we can write $A = (a)$ for some $a \in R$. Then $a \in (a_n)$ for some $n \geq 1$ and hence:

$$(a) \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \cdots \subseteq A = (a_n)$$

Thus $(a_k) = (a_n)$ for all $k \geq n$, so R satisfies ACCP. It follows that R is a UFD. $\square$

Theorem 2.11 Let R be a PID. If $p \in R$ with $p \neq 0$ and not a unit. The following are equivalent:

1. p is prime.
2. $R/(p)$ is a field $\iff$ (p) is a maximal ideal.
3. $R/(p)$ is a domain $\iff$ (p) is a prime ideal.

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

Proof: (1) $\implies$ (2). Consider $a + (p) \neq 0 + (p)$ in $R/(p)$. Then $a \notin (p)$ and thus $p \nmid a$. Consider $A = (a, p) = \{ra + sp : r, s \in R\}$ which is an ideal in R. Since R is a PID, $A = (d)$ for some $d \in R$.

Since $p \in A$, we have $d \mid p$. Since p is prime and thus irreducible, we have $d \sim 1$ or $d \sim p$. If $d \sim p$, then we have $(p) = (d) = A$. Since $a \in A$, we have $p \mid a$, contradiction. Thus we must have $d \sim 1$. It follows that $A = (1) = R$. In particular, $1 \in A$, say $1 = ba + cp$ for some $b, c \in R$. So $1 - ba = cp \in (p)$. Then we have:

$$(a + (p))(b + (p)) = ab + (p) = 1 + (p)$$

The last equality is because $1 - ab \in (p)$. It follows that $R/(p)$ is a field.

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

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

$$(a + (p))(b + (p)) = ab + (p) = 0 + (p) \text{ in } R/(p)$$

Since $R/(p)$ is a domain, we have either $a + (p) = 0 + (p)$ or $b + (p) = 0 + (p)$ in $R/(p)$. It follows that $p \mid a$ or $p \mid b$. Thus p is prime. □

Example $\mathbb{Z}[x]$ is not a PID. Consider $A = \{2n + xf(x) : n \in \mathbb{Z},\ f(x) \in \mathbb{Z}[x]\}$ which is an ideal of $\mathbb{Z}[x]$. Suppose that $A = (g(x))$ for some $g(x) \in \mathbb{Z}[x]$. Then since $2 \in A$, we have $g(x) \mid 2$. If follows that $g(x) \sim 1$ or $g(x) \sim 2$. Thus $A = \mathbb{Z}[x]$ or $A = (2)$, contradiction. Thus $\mathbb{Z}[x]$ is not a PID.

We have the following chain of rings:

ring $\supsetneq$ commutative ring $\supsetneq$ integral domain $\supsetneq$ ACCP $\supsetneq$ UFD $\supseteq$ PID $\supsetneq$ field

We will show that the inclusion "UFD $\supseteq$ PID" is a strict inclusion in the next section. (We will see a UFD that is not a PID).

Remark In a PID, maximal ideal $\iff$ prime ideal (in general, only $\implies$ true).

In a UFD, prime element $\iff$ irreducible elements (in general, only $\implies$ true).

2.4 Gauss' Lemma

Consider the polynomial $2x + 4$.

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

Note that $2 = \gcd(2, 4)$.

Definition If R is a UFD and $0 \neq f(x) \in R[x]$, a greatest common divisor of the nonzero coefficients of $f(x)$ is called a **content** of $f(x)$ and is denoted by $c(f)$. If $c(f) \sim 1$, we say $f(x)$ 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 $6+10x^2+15^3$ is primitive but $6+9x^2+15x^3$ is not.

Lecture 8, 2024/01/24

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

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 $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in R[x]$. By definition, $c = c(f) \sim \gcd(a_n, \cdots, a_0)$. This means $c \mid a_i$ for each $i = 1, \cdots, n$. Therefore there exist b_i for each $i = 1, \cdots, n$ such that $b_i c = a_i$. Then:

$$f(x) = b_n c x^n + \cdots + b_1 c x + b_0 c = c(b_n x^n + \cdots + b_1 x + b_0)$$

Define $f_1(x) = b_n x^n + \cdots + b_1 x + b_0$, then:

$$c \sim \gcd(a_n, \cdots, a_0) \sim \gcd(b_n c, \cdots, b_0 c) \sim c \gcd(b_n, \cdots, b_0)$$

Therefore $c(f_1) \sim \gcd(b_n, \cdots, b_0) \sim 1$, so $f_1(x)$ is primitive.

(2) Exercise. □

Lemma 2.13 Let R be a UFD and $l(x) \in R[x]$ be irreducible with $\deg(l) \geq 1$, then $c(l) \sim 1$.

Proof: By Lemma 2.12, write $l(x) = c(l)l_1(x)$ with $l_1(x)$ being primitive. Since $l(x)$ is irreducible, either $c(l)$ or $l_1(x)$ is a unit. Since $\deg(l_1) = \deg(l) \geq 1$, so $l_1(x)$ is not a unit. Thus $c(l)$ is a unit, which means $c(l) \sim 1$. □

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

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

In particular, the product of primitive polynomial is primitive.

Proof: Let $f = c(f)f_1$ and $g = c(g)g_1$ where f_1, g_1 are primitive. By Lemma 2.12 (2), we have:

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

It suffices to prove that $f(x)g(x)$ is primitive when $f(x)$ and $g(x)$ are primitive, that is, $c(f) \sim c(g) \sim 1$. Suppose that $f(x)$ 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 $f(x)g(x)$. We write:

$$f(x) = a_0 + a_1x + \cdots + a_mx^m$$
$$g(x) = b_0 + b_1x + \cdots + b_nx^n$$

Since $f(x)$ and $g(x)$ are primitive, p does not divide every a_i nor every b_j. Thus there exists $k, s \in \mathbb{Z}_{\geq 0}$ such that:

1. $p \nmid a_k$ but $p \mid a_i$ for all $0 \leq i < k$.
2. $p \nmid b_s$ but $p \mid b_j$ for all $0 \leq j < s$.

We picked the smallest a_i and b_j that are not divisible by p. Then the coefficient of x^{k+s} in $f(x)g(x)$ is $c_{k+s} = \sum_{i+j=k+s} a_ib_j$, expanding it:

$$c_{k+s} = \underbrace{a_0b_{k+s} + \cdots + a_{k-1}b_{s+1}}_{(S1)} + a_kb_s + \underbrace{a_{k+1}b_{s-1} + \cdots + a_{k+s}b_0}_{(S2)}$$

In (S1) every term is of the form a_ib_j with $i \leq k-1$ and $j \geq s+1$, by the choice of a_k, we know $p \mid a_i$ for $i \leq k-1$, thus $p \mid a_ib_j$ for all i, j in $S1$, thus $p \mid (S1)$. Similarly $p \mid (S2)$. We know $p \mid c_{k+s}$, thus $p \mid a_kb_s$, but since $p \nmid a_kb_s$, contradiction. Thus $f(x)g(x)$ is primitive. $\square$

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

Proof: Let $l(x) \in R[x]$ be irreducible, suppose $l(x) = g(x)h(x)$ in $F[x]$. If a and b are the product of the denominators of the coefficients of $g(x)$ and $h(x)$, then $g_1(x) = ag(x) \in R[x]$ and $h_1(x) = bh(x) \in R[x]$. Note that:

$$abl(x) = g_1(x)h_1(x)$$

is a factorization in $R[x]$. Since $l(x)$ is irreducible in $R[x]$, by Lemma 2.13, $c(l) \sim 1$. Also, by Gauss' Lemma:

$$ab \sim abc(l(x)) \sim c(abl(x)) \sim c(g_1(x)h_1(x)) \sim c(g_1)c(h_1) \qquad (*)$$

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

$$abl(x) = g_1(x)h_1(x) = c(g_1)c(h_1)g_2(x)h_2(x)$$

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

Lecture 9, 2024/01/26

Since $g_2(x) \sim 1$ in $R[x]$. Then $ag(x) = g_1(x) = c(g_1)g_2(x)$. Hence $g(x) = a^{-1}c(g_1)g_2(x)$ with $g_2(x) \sim 1$, which is a unit in $F[x]$. Similarly, if $h_2(x) \sim 1$, so $h(x)$ is a unit in F (thus in $F[x]$).

Thus $l(x) = g(x)h(x)$ in $F[x]$ implies that either $g(x)$ or $h(x)$ is a unit in $F[x]$. It follows that $l(x)$ is irreducible in $F[x]$. $\square$

Remark We have the following remarks:

1. We see from above proof, if $f(x) \in R[x]$ admits a factorization in $F[x]$ as $g(x)h(x)$, then by Gauss' Lemma, there exsits $\tilde{g}(x)$ and $\tilde{h}(x)$ in $R[x]$ such that $f(x) = \tilde{g}(x)\tilde{h}(\text{x})$ in $R[x]$. For example:
$$\begin{aligned} 2x^2 + 7x + 3 &= \left(x + \frac{1}{2}\right)(2x + 6) \text{ in } \mathbb{Q}[x] \\ &= (2x + 1)(x + 3) \text{ in } \mathbb{Z}[x] \end{aligned}$$
2. The converse of Theorem 2.15 (Gauss' Lemma) is false. $2x + 4$ is irreducible in $\mathbb{Q}[x]$ but $2x + 4 = 2(x + 3)$ is reducible in $\mathbb{Z}[x]$. Note that $c(2x + 4) = 2$, one may wonder?

Proposition 2.16 Let R be a UFD whose field of fraction is F. Regard $R \subseteq F$ as a subring of F. Let $f(x) \in R[x]$ with $\deg(f) \geq 1$. 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). Follows from Lemma 2.13 and Gauss' Lemma.

(2) $\implies$ (1). Suppose $f(x)$ 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 $d \not\sim 1$ (If both degree ≥ 1, then it would be a non-trivial factorization in $F[x]$). Since $d \mid f(x)$ and $d \not\sim 1$, d divides each coefficient of $f(x)$, which is a contradiction since $f(x)$ is primitive. Thus $f(x)$ is irreducible in $R[x]$. $\square$

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

Example $\mathbb{Z}[x]$ is a UFD since $\mathbb{Z}$ is a UFD. Since $\mathbb{Z}[x]$ is not a PID, we know PID $\subsetneq$ UFD (not all UFD are PID).

Definition Let R be a UFD and $x_1, \cdots, x_n$ be n commuting variables, that is, $x_i x_j = x_j x_i$ for all $i \neq j$. Define the **ring of polynomial in n variables** $R[x_1, \cdots, x_n]$ inductively by:

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

for each $n \geq 1$.

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

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

Theorem 2.20 (Eisenstein's Criterion for UFD) Let R be a UFD with the field of fractions F. Let $h(x) = c_n x^n + \cdots + c_1 x + c_0$ in $R[x]$ with $n \geq 1$. Let $l \in R$ be an irreducible element. If $l \mid c_i$ for all i with $0 \leq i \leq (n-1)$ and $l \nmid c_n$ and $l^2 \nmid c_0$ then $h(x)$ is irreducible in $F[x]$.

Remark Since $\mathbb{Z}$ is a UFD, Eisenstein's Criterion holds when $R = \mathbb{Z}$ and $F = \mathbb{Q}$.

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

Example Let p be a prime. We 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 unity. It is a root of the p-th **cyclotomic polynomial**:

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

Eisenstein's Criterion does not imply the irreducibility of $\Phi_p(x)$ immediately. However, we can consider:

$$\begin{aligned} \Phi_p(x+1) &= \frac{(x+1)^p - 1}{x} = x^p - 1 \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1} \end{aligned}$$

Since p is prime, we know $p \nmid 1$ and $p \mid \binom{p}{i}$ for all $1 \leq i \leq p-1$ and $p^2 \nmid p = \binom{p}{p-1}$. Thus by Eisenstein's Criterion, $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$. Note that the map $x \mapsto x+1$ is a ring isomorphism in $\mathbb{Q}[x]$, so $\Phi_p(x)$ is also irreducible in $\mathbb{Q}[x]$. Since $\Phi_p(x)$ is primtivie, by Prop 2.16, $\Phi_p(x)$ is also irreducible in $\mathbb{Z}[x]$.

Lecture 10, 2024/01/29

Proof of Theorem 2.20: Suppose for a contradiction that $h(x)$ is reducible in $F[x]$, by Gauss' Lemma for UFD, there exists $s(x)$ and $r(x)$ in $R[x]$ of degree ≥ 1 such that $h(x) = s(x)r(x)$. Write:

$$\begin{aligned} s(x) &= a_0 + a_1 x + \cdots + a_m x^m \\ r(x) &= b_0 + b_1 x + \cdots + b_k x^k \end{aligned}$$

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

$$c_0 = a_0 b_0,\ c_1 = a_0 b_1 + a_1 b_0,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 \cdots$$

Consider the constant term. Since $l \mid c_0$, we have $l \mid a_0b_0$. Since l is irreducible and R is a UFD, we have $l \mid a_0$ or $l \mid b_0$. WLOG suppose $l \mid a_0$. Since $l^2 \nmid c_0$, we have $l \nmid b_0$. Consider the coefficient of x. Since $l \mid c_1$, we have $l \mid (a_0b_1 + a_1b_0)$. Since $l \mid a_0$ we have $l \mid a_1b_0$. Since $l \nmid b_0$, we have $l \mid a_1$. By repeating the above argument, the conditions on coefficients of $h(x)$ imply that $l \mid a_i$ for all $0 \leq i \leq (m-1)$ and since $l \nmid c_n$, we get $l \nmid a_m$. Consider the reduction $\overline{h}(x) = \overline{s}(x)\overline{r}(x)$ in $(R/(l))[x]$. 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 $l \nmid b_0$, $\overline{s}(x)\overline{r}(x)$ contain the term $\overline{a_mb_0}x^m$, which leads to a contradiction. So $h(x)$ is not reducible in $F[x]$. $\square$

3 Field Extensions

3.1 Degree of Extensions

Definition If E is a field containing another field F, we say 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 other than (0) and E.

Definition If E/F is a field extension, we can view E as a vector space over F:

1. Addition: For $e_1, e_2 \in E$, define $e_1 \oplus e_2 = e_1 + e_2$. (The addition in vector space is just the addition in the field E).
2. Scalar Multiplication: For $c \in F$ and $e \in E$, define $c \star e = c \cdot e$. (The F-scalar multiplication in the vector space is just the multiplication in E).

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 E/F is a **finite extension**. Otherwise, we say E/F is an **infinite extension**.

Example $[\mathbb{C} : \mathbb{R}] = 2$ is a finite extension, since $\mathbb{C} = \text{Span}_{\mathbb{R}}\{1, i\}$.

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

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

Then $[F(x) : F] = \infty$ since $\{1, x, x^2, \cdots\}$ are 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 $[K:F]$ divides $[E:F]$.

Proof: Suppose $[E:K]=m$ and $[K:F]=n$. Let $\{a_1,\cdots,a_n\}$ be a basis of E/K and $\{b_1,\cdots,b_n\}$ be a basis for K/F. It suffices to prove:

$$\mathcal{B}=\{a_ib_j : 1\leq i\leq m,\ 1\leq j\leq n\}$$

is a basis of E/F. We claim $\operatorname{Span}_F\mathcal{B}=E$, that is, every element of E is a linear combination of $\{a_ib_j\}$ over F. For $e\in E$ we have:

$$e=\sum_{i=1}^m k_ia_i=k_1a_1+\cdots k_ma_m$$

with $k_i\in K$. For each $k_i\in K$ we have:

$$k_i=\sum_{j=1}^n c_{ij}b_j=c_{i1}b_1+\cdots+c_{in}b_n$$

with $c_ij\in F$. Thus we have:

$$e=\sum_{i=1}^m\sum_{j=1}^n c_{ij}b_ja_i$$

It follows that $\operatorname{Span}_F\mathcal{B}=E$. Now we claim $\mathcal{B}$ is linearly independent over F. Suppose that:

$$\sum_{i=1}^m\underbrace{\sum_{j=1}^n c_{ij}b_j}_{\in K}a_i=0\quad\text{with}\quad c_{ij}\in F$$

Since $\sum_{j=1}^n c_{ij}b_j\in K$ and $\{a_1,\cdots,a_m\}$ is linearly independent over K we have $\sum_{j=1}^n c_{ij}b_j=0$ for each i. Since $\{b_1,\cdots,b_n\}$ is linearly independent over F, we have $c_{ij}=0$ for each j. Thus $c_{ij}=0$ for all i,j. Therefore $\mathcal{B}$ is a basis of E/F and we have $[E:F]=mn=[E:K][K:F]$. □

Lecture 11, 2024/01/31

3.2 Algebraic and Transcendental Extensions

Definition Let E/F be a field extension and $\alpha\in E$. We say α is **algebraic** over F if there exists $0\neq f(x)\in F[x]$ with $f(\alpha)=0$. Otherwise we say α is **transcendental** over F.

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

Example Claim: $\alpha = \sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$. To prove the claim, write $\alpha - \sqrt{2} = \sqrt{3}$. By squaring both sides, we get:

$$\alpha^2 - 2\sqrt{2}\alpha + 2 = 3$$

It follows that $\alpha^2 - 1 = 2\sqrt{2}\alpha$, squaring both sides again:

$$\alpha^4 - 2\alpha^2 + 1 = 8\alpha^2 \implies \alpha^4 - 10\alpha^2 + 1 = 0$$

It follows that α is a root of $x^4 - 10x^2 + 1$.

Definition 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 $\alpha, \beta \in E$, define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ similarly.

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

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

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

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

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

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

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

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

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

$$\psi : F[x]/(p(x)) \to F[\alpha] \text{ with } \psi(x) = \alpha$$

From which we can conclude $F[\alpha] = F(\alpha)$.

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

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

Since α is algebraic, $I \neq (0)$. By the first isomorphism theorem, $F[x]/I \cong \operatorname{im}\psi$ and $\operatorname{im}\psi$ is a subring of the field $F(\alpha)$. Thus $\operatorname{im}\psi$ is a domain and it follows that $F[x]/I$ is a domain. This implies that I is a prime ideal and say $I = (p(x))$, then $p(x)$ is a irreducible. If we assume $p(x)$ is monic, then it is unique. It follows that:

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

Since $F[x]$ is a PID, the prime ideal $(p(x))$ is maximal. Thus $F[x]/(p(x))$ is a field 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 If α is algebraic over F, the unique monic irreducible polynomial $p(x)$ in Theorem 3.3 is called the **minimal polynomial** of α over F. From the proof of Theorem 3.3, we see that if $f(x) \in F[x]$ with $f(\alpha) = 0$, then $p(x) \mid f(x)$. As a direct consequence of Theorem 3.2 and 3.3, we have the following:

Theorem 3.4 Let E/F be a field extension and $\alpha \in E$.

1. α is transcendental over F if and only if $[F(\alpha) : F] = \infty$.
2. α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.

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

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

and that:

$$\{1, \alpha, \alpha^2, \cdots, \alpha^{\deg(p)-1}\}$$

is a basis of $F(\alpha)/F$.

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

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

Lecture 12, 2024/02/02

(2) ($\Rightarrow$). From Theorem 3.3, if α is algebraic over F, then:

$$F(\alpha) \cong F[x]/(p(x)) \ \text{ with } \ x \mapsto \alpha$$

Note that $F[x]/(p(x)) \cong \{r(x) \in F[x] : \deg(r) < \deg(p)\}$. Thus $\{1, x, \cdots, x^{\deg(p)-1}\}$ forms a basis of $F[x]/(p(x))$. It follows that $[F(\alpha) : F] = \deg(p)$ and:

$$\{1, \alpha, \cdots, \alpha^{\deg(p)-1}\}$$

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 $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. The field $\mathbb{Q}(\zeta_p)$ is the **p-th cyclotomic extension** of $\mathbb{Q}$.

Example Let $\alpha = \sqrt{2} + \sqrt{3}$. We have seen before that α is a root of the polynomial $x^4 - 10x^2 + 1$. One can show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since $\sqrt{2}$ is a root of $x^2 - 2$, which is irreducible, we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Also clearly $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. We have $\alpha \notin \mathbb{Q}(\sqrt{2})$, hence $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \geq 2$. Since α is a root of a polynomial of degree 4, it follows that:

$$4 \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})]}_{\geq 2} \underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{=2} \geq 4$$

Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $x^4 - 10x^2 + 1$ is the minimal polynomial of α over $\mathbb{Q}$. (Piazza Exericse) Check if we can use Eisenstein to show $x^4 - 10x^2 + 1$ is irreducible.

$$\mathbb{Q} \overset{2}{\text{———}} \mathbb{Q}(\sqrt{2}) \overset{2}{\text{———}} \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

Theorem 3.5 Let E/F be a field extension. If $[E : F] < \infty$, there exists $\alpha_1, \cdots, \alpha_n \in E$ such that we have:

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

Proof: We will prove it by induction on $[E : F]$. If $[E : F] = 1$, then 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 $a_1 \in E \setminus F$, by theorem 3.1:

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

Since $[F(\alpha_1) : F] > 1$, we have $[E : F(\alpha_1)] < [E : F]$. By induction, there exists $\alpha_2, \cdots, \alpha_n \in E$ such that:

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

Thus the result holds since $F \subsetneq F(\alpha_1)$. $\square$

Remark By Theorem 3.5, to understand a finite extension, it suffices to understand a finite simple extension.

Definition A field extension E/F is an **algebraic extension** if every $\alpha \in E$ is algebraic over F. Otherwise it is a **transcendental extension**.

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 $\{1, \alpha, \cdots, \alpha^n\}$ are NOT linearly independent over F (since $\dim(E/F) = n$ so the maximal linearly independent set has size n). Thus there exists $c_i \in F$ for $i = 1, \cdots, n$ not all 0 such that:

$$\sum_{i=0}^{n} c_i \alpha^i = c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$$

Thus α is a root of the polynomial $c_0 + c_1x + \cdots + c_nx^n$ in $F[x]$, thus it is algebraic over F. $\square$

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.

Definition Let E/F be a field extension. The set L above is called the **algebraic closure** of F in E.

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 $\mathbb{C}$, that is:

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

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

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

Since there are infinitely many primes, so $p \to \infty$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Hence the converse of Theorem 3.6 is false, that is, not all algebraic extension are finite.

Lecture 13, 2024/02/05

Proof of Theorem 3.7: If $\alpha, \beta \in L$, we need to show $\alpha \pm \beta,\ \alpha/\beta(\beta \neq 0) \in L$. 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 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 $F(\beta)$, that is, $p(x) \in F(\beta)[x]$ and $p(\alpha) = 0$). We have:

$$[F(\alpha, \beta) : F(\beta)] \leq [F(\alpha) : F]$$

Combine this with Theorem 3.1 we have:

$$[F(\alpha,\beta):F]=[F(\alpha,\beta):F(\beta)][F(\beta):F]\leq[F(\alpha):F][F(\beta):F]<\infty$$

Since $\alpha+\beta\in F(\alpha,\beta)$, it follows that:

$$[F(\alpha+\beta):F]\leq[F(\alpha,\beta):F]<\infty$$

This means $\alpha+\beta\in L$. Similarly, $\alpha,\beta,\alpha\cdot\beta$ and $\alpha/\beta(\beta\neq 0)$ are in L. It follows that L is a field, as desired. $\square$

4 Splitting Fields

Definition Let E/F be a field extension. We say $f(x)\in F[x]$ **splits over** E if E contains all roots of $f(x)$, that is, $f(x)$ is a product of linear factors in $E[x]$.

Definition 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.

Then we say E is the **splitting field** of $f(x)$ in $\tilde{E}$.

4.1 Existence of Splitting Fields

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

Proof: Since $p(x)$ is irreducible, the ideal $I=(p(x))$ is maximal (since $F[x]$ is a PID). Thus $E=F[x]/I$ is a field. Consider:

$$\psi:F\to E\ \text{ by }\ a\mapsto a+I$$

Since F is a field and $\psi\neq 0$, we get ψ is injective. Thus $F\cong\psi(F)\subseteq E$. By identifying F as $\psi(F)$, 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:

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

Then we have:

$$\begin{aligned}
p(\alpha) &= (a_0 + I) + (a_1 + I)\alpha + \cdots + (a_n + I)\alpha^n \\
&= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\
&= (a_0 + I) + (a_1 x + I) + \cdots + (a_n x^n + I) \qquad (1) \\
&= (a_0 + a_1 x + \cdots + a_n x^n) + I \\
&= p(x) + I = 0 + I
\end{aligned}$$

(1) is becasue $(x + I)^k = x^k + I$. Thus $\alpha = x + I \in E$ is a root of $p(x)$. □

Theorem 4.2 (Kronecker) Let $f(x) \in F[x]$, there exists a field E containing F such that $f(x)$ splits over $E[x]$.

Proof: We prove this theorem by induction on $\deg(f)$ with any field. 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 $\deg(g) < \deg(f)$ ($g(x)$ need not 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. □

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

Proof: Let $f(x) \in F[x]$, by Theorem 4.2, there is a field extension E/F over which $f(x)$ splits, say $\alpha_1, \cdots, \alpha_n$ are roots of $f(x)$ in E. Consider $F(\alpha_1, \cdots, \alpha_n)$. 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 $F(\alpha_1, \cdots, \alpha_n)$ is the splitting field of $f(x)$ in E. Moreover, since α_i are all algebraic, $F(\alpha_1, \cdots, \alpha_n)/F$ is a finite extension. □

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 $x^3 - 2$.

Lecture 14, 2024/02/07

Remark If $f(x)$ splits in E, that is, $\alpha_1, \cdots, \alpha_n$ are roots of E. Then $F(\alpha_1, \cdots, \alpha_n)$ 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, $F(\alpha_1, \cdots, \alpha_n)$ is the splitting field of $f(x) \in F[x]$ and it is unique with E.

Question: If we change E/F to a different field extension, say E_1/F, what is the difference between the splitting field of $f(x)$ in E and the one in E_1?

Definition 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 homomorphism 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 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 isomorphic as rings. Thus we can say "the" splitting field of $f(x)$ over F.

Proof: Let $\phi : F \to F$ be the identity map and apply Theorem 4.4. $\square$

Proof of Theorem 4.4: We prove this by induction. If $[E : F] = 1$, then $E = F$, which means $f(x)$ splits in $F[x]$. Then $f(x)$ is a product of linear factors in $F[x]$ and so is $f_1(x)$ in $F_1[x]$ since Φ is an isomorphism. Thus $E = F$ and $E_1 = F_1$. Take $\psi = \phi$ and we are done. Suppose $[E : F] > 1$ and the statement is true for all field extensions $\tilde{E}/\tilde{F}$ 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:

$$F(\alpha) \cong F[x]/(p(x)) \text{ by } \alpha \mapsto x + (p(x))$$

Similarly, there is an F_1-isomorphism:

$$F_1(\alpha_1) \cong F_1[x]/(p_1(x)) \text{ by } \alpha_1 \mapsto x + (p_1(x))$$

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:

$$\tilde{\Phi} : F[x]/(p(x)) \to F_1[x]/(p_1(x)) \text{ by } x + (p(x)) \mapsto x + (p_1(x))$$

which extends ϕ. It follows that there exists a field isomorphism:

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

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.

$$\begin{tikzcd}
E \arrow[r, "\cong \text{ by } \psi"] \arrow[d, dash, "< n"'] & E_1 \arrow[d, dash, "< n"] \\
F(\alpha) \arrow[r, "\cong \text{ by } \tilde{\phi}"] \arrow[d, dash, "\geq 2"'] & F_1(\alpha_1) \arrow[d, dash, "\geq 2"] \\
F \arrow[r, "\cong \text{ by } \phi"] & F_1
\end{tikzcd}$$

where $n = [E : F]$, so if we let $\tilde{F} = F(\alpha)$ and $\tilde{F_1} = F_1(\alpha_1)$ as in the inductive step, we can use induction. $\square$

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 $[E : F] \mid 1$, so we are done. Suppose $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$. Two cases:

Lecture 15, 2024/02/09

1. If $f(x) \in F[x]$ is irreducible and $\alpha \in E$, a root of $f(x)$. By Theorem 3.3:
$$F(\alpha) \cong F[x]/(f(x)) \quad \text{and} \quad [F(\alpha) : F] = \deg(f) = n$$
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 $[E : F] = [E : F(\alpha)][F(\alpha) : F] = n[E : F(\alpha)]$, it follows that:
$$[E : F] \mid n(n-1)! \implies [E : F] \mid n!$$
2. If $f(x)$ is not irreducible, write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$ and $\deg(g) = m$ and $\deg(h) = k$ with $m + k = n$ and $1 \leq m, k < n$. Let K be the splitting field of $g(x)$ over F. Since

$\deg(m) < n$, by induction:

$$[K : F] \mid m!$$

Since E is the splitting field of $h(x)$ over K and $\deg(h) = k < n$, by induction:

$$[E : K] \mid k!$$

It follows that:

$$[E : F] = [E : K][K : F] \mid m!k!$$

and note that:

$$\frac{n!}{m!k!} = \frac{n!}{m!(n-m)!} = \binom{n}{m} \in \mathbb{Z}$$

So $m!k! \mid n!$ and we get $[E : F] \mid n!$. ☐

5 More Field Theory

5.1 Prime Fields

Definition 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 $p \in \mathbb{Z}$.

Proof: Let F_1 be a subfield of F. Consider the following ring map:

$$\chi : \mathbb{Z} \to F_1 \quad \text{by} \quad n \mapsto n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ times}}$$

where $1 \in F_1 \subseteq F$. Let $I = \operatorname{Ker} \chi$ be the kernel of χ. Since $\mathbb{Z}/I \cong \operatorname{im} \chi$, a subring of F_1, it is an integral domain. Thus I is a prime ideal. Two cases:

1. If $I = (0)$, then $\mathbb{Z} \subseteq F_1$. Since F_1 is a field, we get:

$$\mathbb{Q} = \operatorname{Frac}(\mathbb{Z}) \subseteq F_1$$

2. If $I = (p)$, by the isomorphism theorem:

$$\mathbb{Z}_p \cong \mathbb{Z}/(p) \cong \operatorname{im} \chi \subseteq F_1$$

Since the prime field is a subfield, done. ☐

Definition Given a field F, if its prime field is isomorphism to $\mathbb{Q}$, then we say F has **characteristic** 0. If its prime field is isomorphism to $\mathbb{Z}_p$, we say F has characteristic p. Denoted by $\mathrm{ch}(F) = 0$ or $\mathrm{ch}(F) = p$.

Note that if $\mathrm{ch}(F) = p$, for $a, b \in F$:

$$\begin{aligned}(a+b)^p &= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p \\ &= a^p + b^p\end{aligned}$$

The last equality follows since the coefficients $p \mid \binom{p}{i}$ for $1 \leq i \leq p-1$ and hence 0 in F since F has characteristic p.

Using this we can prove (see Piazza):

Proposition 5.2 Let F be a field with $\mathrm{ch}(F) = p$ and let $n \in \mathbb{N}$. Then the map:

$$\varphi : F \to F \ \text{ by } \ u \mapsto u^{p^n}$$

is an injective $\mathbb{Z}_p$-homomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-isomorphism.

5.2 Formal Derivatives and Repeated Roots

Definition If F is a field, then the mononiamls $\{1, x, x^2, \cdots\}$ form a F-basis of $F[x]$. Define the linear operator $D : F[x] \to F[x]$ by:

$$D(1) = 0 \ \text{ and } \ D(x^i) = ix^{i-1}$$

for $i \geq 1$. Thus for $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ where $a_i \in F$:

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

One can check that we have:

1. $D(f+g) = D(f) + D(g)$.
2. (Leibniz Rule). $D(fg) = D(f)g + D(g)f$. (Piazza Exercise).

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

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

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

Proof: ($\Leftarrow$) of (1). This is clear.

($\Rightarrow$) of (1). If $f(x) = a_0 + \cdots + a_n x^n$, then $f'(x) = 2a_2 x + \cdots + na_n x^{n-1} = 0$. This means $ia_i = 0$ for all $1 \le i \le n$. Since $\mathrm{ch}(F) = 0$ and $i \neq 0$, thus we must have $a_i = 0$ for all $i \geq 1$. Thus $f(x) = a_0$.

Lecture 16, 2024/02/12

($\Leftarrow$) of (1). Write $g(x) = b_0 + b_1 x + \cdots + b_m x^m \in F[x]$. Then:

$$f(x) = g(x^p) = b_0 + b_1 x^p + \cdots + b_m x^{pm}$$

Taking the derivative we have:

$$f'(x) = b_1 p x^{p-1} + \cdots + pmb_m x^{pm-1}$$

Since $\mathrm{ch}(F) = p$, we get $f'(x) = 0$ since every term has p.

($\Rightarrow$) of (2). For $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and:

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

This implies $ia_i = 0$ in F for all $1 \le i \le n$. Since $\mathrm{ch}(F) = p$:

$$ia_i = 0 \implies a_i = 0 \text{ unless } p \mid i$$

Thus we know:

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

where $g(x) = a_0 + a_p x + a_{2p} x^2 + \cdots + a_{mp} x^m \in F[x]$. $\square$

Definition 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 $f(x)$ if and only if $(x - \alpha)$ divides both f and f', that is, $(x - \alpha) \mid \gcd(f, f')$.

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

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)g'(x) = (x - \alpha)(2g(x) + g'(x))$$

Thus $(x - \alpha)$ divides both f and f' by definition.

($\Leftarrow$). Suppose that $(x - \alpha)$ divides both f and f'. Write:

$$f(x) = (x - \alpha)h(x) \text{ where } h(x) \in E[x]$$

Then we have:

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

Then since $f'(\alpha) = 0$, we get $h(\alpha) = 0$. Thus $(x - \alpha)$ is a factor of $h(x)$. Say $h(x) = (x - \alpha)g(x)$ for some $g(x) \in E[x]$, then:

$$f(x) = (x - \alpha)h(x) = (x - \alpha)^2 g(x)$$

It follows that α is a repeated root by definition. $\square$

Definition 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 root in any field extension of F.

Example $f(x) = (x - 2)(x + 9)$ is separable in $\mathbb{Q}[x]$.

Corollary 5.5 $f(x)$ is separable if and only if $\gcd(f, f') = 1$.

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

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

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

Example The p-th cyclotomic polynomial $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$ and hence separable. We recall the roots of $\Phi_p(x)$ are:

$$\zeta_p,\ \zeta_p^2, \cdots, \zeta_p^{p-1}$$

which are all distinct roots.

5.3 Finite Fields

Definition 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 dimensional vector space over $\mathbb{Z}_p$, say $\dim_{\mathbb{Z}_p} F = n \in \mathbb{N}$, then we know:

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

as vector spaces. This means $|F| = p^n$, as desired. □

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 finitely generated abelian groups, we get:

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

with $n_1 > 1$ and $n_1 \mid n_2 \mid \cdots \mid n_r$. Since:

$$n_r(\mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_r\mathbb{Z}) = 0$$

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 $G \cong \mathbb{Z}/n_r\mathbb{Z}$. □

Lecture 17, 2024/02/14

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

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

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

1. F is a finite field with $|F| = p^n$ if and only if 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: ($\Rightarrow$) of (1). 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 the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

($\Leftarrow$) of (1). Suppose F is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$, Since $\mathrm{ch}(F) = p$, we have $f'(x) = -1$. Thus $\gcd(f, f') = 1$, which means $f(x)$ is separable and $f(x)$ 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:

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

For $u \in F$, u is a root of $f(x)$ if and only if $\varphi(u) = u$. 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 cecall that:

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

Since $n = mk$, by this formula, we have:

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

For some $g \in \mathbb{Z}$, then we have:

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

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 $\tilde{K} \subseteq F$ is any subfield with $|\tilde{K}| = p^m$, 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 $|K| = p$ is unique. $\square$

As a direct consuqence of Theorem 5.10 and Corollary 4.5 we have:

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 $\text{ch}(F) = p$. 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 get $F = F^p$.

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

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

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

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

a contradiction since $r(x)$ is irreducible. Thus $r(x)$ is separable. $\square$

Example Let $\text{ch}(F) = p$ 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 $\beta \notin F$. We have that:

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

   which is not separable.

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

Lecture 18, 2024/02/26

Write $x^p - a = g(x)h(x)$ where $g(x), h(x) \in F[x]$ 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 F, we have $r = 0_F$ in F. Thus as an integer, $r = 0$ or $r = p$. It follows that either $g(x) = 1$ or $h(x) = 1$ in $F[x]$. Thus $f(x)$ is irreducible in $F[x]$.

6 Solvable Groups and Automorphism Groups

6.1 Solvable Groups

Definition A group G is **solvable** if there exists a tower:

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

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

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

Example Consider the symmetric 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 $K \triangleleft G$. Then HK is a subgroup of G, $K \triangleleft HK$, $H \cap K \triangleleft H$ and:

$$HK/K \cong H/(H \cap K)$$

Theorem 6.2 (Third Isomorphism Theorem) Let $K \subseteq H \subseteq G$ be groups with $K \triangleleft G$ and $H \triangleleft G$. Then $H/K \triangleleft G/K$ 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 the normal subgroup of G, then the quotient group G/N is solvable.

Proof: 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} is abelian for all $0 \le i \le m-1$.

(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 to G_i, we have:

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

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 towers:

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

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:

$$G_{i+1}N/N \triangleleft G_iN/N$$

By third isomorphism theorem:

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

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 quotient 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 G_{i+1} is contained in the kernel of π, 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 quotient. Since G_i/G_{i+1} is abelian, so is $G_i/(G_i \cap G_{i+1}N)$. Thus:

$$(G_iN/N)/(G_{i+1}N/N) \text{ is abelian}$$

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

Lecture 19, 2024/02/28

Theorem 6.4 Let N be a normal subgroup of G. If both 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:

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

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

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

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

$$\sigma : \mathrm{Sub}_N(G) \to \mathrm{Sub}(G/N) \;\text{ by }\; H \mapsto H/N$$

For $i = 0, 1, \cdots, r$, define $G_i = \sigma^{-1}(\overline{G_i})$. Since $N \lhd G$ and $\overline{G_{i+1}} \lhd \overline{G_i}$, we have $G_{i+1} \lhd G_i$ (Exercise). By the third isomorphism theorem:

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

It follows that:

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

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

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

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

Example One can show that the alternating group A_5 is simple (see Bonus 4). In fact A_n is simple for all $n \neq 4$.

By this fact, we know $A_5 \supseteq \{1\}$ is the only possible tower of A_5, but $A_5/\{1\} \cong A_5$ is NOT abelian, so A_5 is not solvable. Thus S_5 is also not solvable by Theorem 6.3.

Moreover, since all S_n with $n \geq 5$ contains a subgroup that is isomorphic to S_5, which is not solvable, by Theorem 6.3, we get S_n is not solvable for all $n \geq 5$.

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

Proof: If G is solvable there is 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} is abelian for all $0 \leq i \leq (m-1)$. Consider $A = G_i/G_{i+1}$, a finite abelian group. We have:

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

with 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. $\square$

Remark By the Chinese Remainder Theorem, we can further require the quotient G_i/G_{i+1} to be a cyclic group of prime order.

6.2 Automorphism Groups

Definition Let E/F be a field extension. If ψ is an automorphism of E, that is, $\psi : E \to E$ is an isomorphism. If $\psi|_F = \mathrm{id}_F$ (ψ fixes elements in F), we say ψ is an ***F*-automorphism of** E. By maps composition, the set:

$$\mathrm{Aut}_F(E) = \{\psi \in \mathrm{Aut}(E) : \psi \text{ is a } F\text{-automorphism}\}$$

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:

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

As desired. □

Lemma 6.7 Let $E = F(\alpha_1, \cdots, \alpha_n)$ 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:

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

where $f(x_1, \cdots, x_n), g(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ with $g \neq 0$. Thus the lemma follows. □

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:

$$E = F(\alpha_1, \cdots, \alpha_n)$$

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. □

Remark The converse of Corollary 6.8 is false. For example, $\mathbb{R}/\mathbb{Q}$ is an infinite extension. But one can show $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{1\} = \{\mathrm{id}\}$. Indeed, if $\psi \in \mathrm{Aut}(\mathbb{R})$ then $\psi(1) = 1$. This implies $\psi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.

6.3 Automorphism Groups of Splitting Fields

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

By Theorem 4.4 and Assignment 4, we have:

Theorem 6.9 Let E/F be the splitting field of a nonzero polynomial $f(x) \in F[x]$. We have:

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

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

Lecture 20, 2024/03/01

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, $|\mathrm{Aut}_F(E)|$ divides $n!$.

Proof: Let $X = \{a_1, \cdots, a_n\}$ be distinct roots of $f(x)$ in E. By Lemma 6.6, if $\psi \in \operatorname{Aut}_F(E)$, 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:

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

is a group homomorphism. Moreover, by Lemma 6.7, it is injective. Thus $\operatorname{Aut}_F(E)$ is isomorphic to a subgroup of S_n, as desired. $\square$

Example Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $E/\mathbb{Q}$ be the splitting field of $f(x)$. Then we have $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and:

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = 2 \cdot 3 = 6$$

Since $\operatorname{ch}(\mathbb{Q}) = 0$ and $f(x)$ is irreducible, so $f(x)$ is separable. By Theorem 6.9, $|\operatorname{Aut}_F(E)| = [E : F] = 6$. Also, since $f(x)$ has 3 distinct roots in E, by Theorem 6.10, $|\operatorname{Aut}_{\mathbb{Q}}(E)|$ is a subgroup of S_3. Since $|S_3| = 6 = |\operatorname{Aut}_{\mathbb{Q}}(E)|$ and $\operatorname{Aut}_{\mathbb{Q}}(E)$ is a subgroup, we get $\operatorname{Aut}_{\mathbb{Q}}(E) \cong S_3$.

Example Let F be a field with $\operatorname{ch}(F) = p$ 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:

$$f(x) = (x - \beta)^p \text{ for some } \beta \in E \setminus F$$

Thus $E = F(\beta)$. Since β can only map to β under any $\psi \in \operatorname{Aut}_F(E)$, thus $|\operatorname{Aut}_F(E)| = 1$, while:

$$[E : F] = [E : F(\beta)] = \deg(f(x)) = p$$

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

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

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

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

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

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 $G = \operatorname{Aut}_F(E)$, then $E^G = F$.

Proof: Let $L = E^G$. Since $F \subseteq L$, we have $\operatorname{Aut}_L(E) \subseteq \operatorname{Aut}_F(E)$. On the other hand, if $\psi \in \operatorname{Aut}_F(E)$, by definition of L, for all $a \in L$, we have $\psi(a) = a$. This implies $\psi \in \operatorname{Aut}_L(E)$. Thus $\operatorname{Aut}_F(E) = \operatorname{Aut}_L(E)$. Note that 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 we have:

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

It follows that $[E : F] = [E : L]$ and since:

$$[E : F] = [E : L][L : F]$$

we have $[L : F] = 1$. Thus $L = F$, that is, $E^G = F$. $\square$

7 Separable Extensions and Normal Extensions

7.1 Separable Extensions

Definition Let E/F be an algebraic field extension. For $\alpha \in E$, let $p(x) \in F[x]$ be the minimal polynomial of α over F. We say α is **separable over** F if its minimal polynomial $p(x)$ is separable. We say 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 $p(x) \in F[x]$ the minimal polynomial of α. Let:

$$\{\alpha = \alpha_1, \cdots, \alpha_n\}$$

be all of the distinct roots of $p(x)$ in E. Define:

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

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

Lecture 21, 2024/03/04

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

$$\psi(\tilde{p}(x)) = (x - \psi(a_1)) \cdots (x - \psi(a_n)) = (x - a_1) \cdots (x - a_n) = \tilde{p}(x)$$

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

Corollary 7.2 Let E/F be a finite extension and $E = F(\alpha_1, \cdots, \alpha_n)$. 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 $E = F(\alpha_1, \cdots, \alpha_n)$ is a subfield of L, we get E is also separable. $\square$

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 field.

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

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

Definition If $E = F(\gamma)$ is a simple extension, we say 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 F is an infinite field. Since $E = F(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_1, \cdots, \alpha_n \in E$, it suffices to consider when $E = F(\alpha, \beta)$ and the result follows from induction. Let $E = F(\alpha, \beta)$ and $\alpha, \beta \notin F$.

Claim: there exists $\lambda \in F$ such that $\gamma = \alpha + \lambda\beta$ and $\beta \in F(\gamma)$.

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

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

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 $\gamma = \alpha + \lambda\beta$ and define:

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

since $\gamma \in F(\gamma)$ and $\lambda \in F$. Then we have:

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

Since $a(x)$ is the minimal polynomial of α. However, for any $\tilde{\beta} \neq \beta$, since:

$$\gamma - \lambda\tilde{\beta} = \alpha + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha}$$

by our choices of λ, we have:

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

Lecture 22, 2024/03/06

Thus $h(x)$ and $b(x)$ have β as a common root, but no other root 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 $\beta \in F(\gamma)$ as required. $\square$

7.2 Normal Extensions

Definition 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 root in E or $p(x)$ has all roots in E.

In other words, if $p(x)$ has a root in E, then $p(x)$ splits in E.

Example Let $\alpha \in \mathbb{R}$ with $\alpha^4 = 5$. Since the roots $x^4 - 5$ are $\pm\alpha$ and $\pm\alpha i$ and $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. And $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not a normal extension.

Let $\beta = (1+i)\alpha$. We claim $\mathbb{Q}(\beta)/\mathbb{Q}$ is also not normal. Note that:

$$\beta^2 = 2i\alpha^2 \implies \beta^4 = -4\alpha^4 = -20$$

Since $\pm\beta$ and $\pm\beta i$ satisfies $x^4 + 20 = 0$, to show $\mathbb{Q}(\beta)$ is not normal, it suffices to show $i \notin \mathbb{Q}(\beta)$. Since the minimal polynomial of β over $\mathbb{Q}$ is $p(x) = x^4 + 20$. We have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Also, the roots of $p(x)$ are $\pm\beta$ and $\pm\beta i$. Since the minimal polynomial of α is $x^4 - 5$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Note if $\alpha \in \mathbb{Q}(\beta)$, since:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [\mathbb{Q}(\beta) : \mathbb{Q}]$$

we have $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, which is not possible since $\beta = \alpha + i\alpha \notin \mathbb{Q}(\alpha)$. Thus $\alpha \notin \mathbb{Q}(\beta)$. It implies $i \notin \mathbb{Q}(\beta)$, since otherwise, then:

$$\alpha = \frac{\beta}{1+i} \in \mathbb{Q}(\beta)$$

contradiction. It follows that the factorization of $p(x)$ over $\mathbb{Q}(\beta)$ is:

$$(x-\beta)(x+\beta)(x^2 - \beta^2)$$

Since $p(x)$ does not split over $\mathbb{Q}(\beta)$, we know $\mathbb{Q}(\beta)/\mathbb{Q}$ is not normal.

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

Proof: ($\Rightarrow$). Suppose that E/F is normal, wrtie $E = F(\alpha_1, \cdots, \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i. Define $f(x) = p_1(x) \cdots p_n(x)$. Since E/F is normal, each $p_i(x)$ splits over E. For $1 \leq i \leq n$ let:

$$\alpha_i = \alpha_{i,1}, \cdots, \alpha_{i,r_i}$$

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

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

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

($\Leftarrow$). Let E/F be the splitting field of $f(x) \in F[x]$. Let $p(x) \in F[x]$ by irreducible and has a 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 $0 \neq c \in F$ and $\alpha = \alpha_1 \in E$ and $\alpha_2, \cdots, \alpha_n \in K = E(\alpha_1, \cdots, \alpha_n)$. Since we know:

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

we have the F-isomorphism $\theta : F(\alpha) \to F(\alpha_2)$ with $\theta(\alpha) = \alpha_2$. Note that $p(x)f(x) \in F[x] \subseteq F(\alpha)[x]$ and $p(x)f(x) \in F(\alpha_2)[x]$. 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, $\psi \in \mathrm{Aut}_F(K)$.

$$\begin{tikzcd}
K \arrow[r, "\psi \text{ extending } \theta"] \arrow[d, dash] & K \arrow[dd, dash] \\
E \arrow[d, dash] & \\
F(\alpha) \arrow[r, "\theta"] \arrow[d, dash] & F(\alpha_2) \arrow[d, dash] \\
F \arrow[r, "1"] & F
\end{tikzcd}$$

Lecture 23, 2024/03/08

Since $\psi \in \mathrm{Aut}_F(K)$, we know 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 prove $\alpha_i \in E$ for all $3 \leq i \leq n$. Thus $K = E$ and $p(x)$ splits over E. It follows that E/F is normal. $\square$

Example Every quadratic extension is normal. Let E/F be the 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:

$$p(x) = (x - \alpha)(x - \beta) = x - (\alpha + \beta)x + \alpha\beta$$

Thus $\beta = -a - \alpha$ is the other root of $p(x)$ and $\beta \in E$. Hence E/F is normal.

Example The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal. Since the irreducible polynomial $p(x) = x^4 - 2$ has a root in $\mathbb{Q}(\sqrt[4]{2})$, but $p(x)$ does not split over $\mathbb{Q}(\sqrt[4]{2})$, as there are some roots that are complex numbers.

Remark Note that $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is made up of two quadratic extensions:

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

which are both normal. Thus, if E/K and K/F are normal extensions, 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: If $p(x) \in K[x]$ 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. Let:

$$F = \mathbb{Q}, \quad K = \mathbb{Q}(\sqrt[4]{2}), \quad E = \mathbb{Q}(\sqrt[4]{2}, i)$$

Then E/F is the splitting field of $x^4 - 2$, hence E/F is normal. Also, E/K is normal but $K/\mathbb{Q}$ is not normal.

Proposition 7.7 Let E/F be a finite normal extension and $\alpha, \beta \in E$. The followings 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 of α over F and $\psi \in \mathrm{Aut}_F(E)$ with $\psi(\alpha) = \beta$. By Lemma 6.6, β is also a root of $p(x)$. Since $p(x)$ is monic and irreducible, it is the minimal polynomial of β over F. Hence α and β have the same minimal polynomial.

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

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

we have the F-isomorphism $\theta : F(\alpha) \to F(\beta)$ with $\theta(\alpha) = \beta$. Since E/F is a finite normal extension, by Theorem 7.5, E is the splitting field of some $f(x) \in F[x]$ over F. We can also view E as the splitting field of $f(x)$ over $F(\alpha)$ and $F(\beta)$, respectively. Thus 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 $\psi(\alpha) = \beta$. □

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 A **normal closure** of a finite extension E/F is a finite normal extension N/F satisfying the following properties:

1. E is a subfield of N.
2. Let L be an intermediate field of N/E. If L is normal over F, then $L = N$.

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

Theorem 7.8 Every finite extension E/F has a normal closure N/F which is unique, up to E-isomorphism.

Proof: Since E/F is finite ,we can write $E = F(\alpha_1, \cdots, \alpha_n)$.

Let $p_i(x)$ be the minimal polynomial of α_i over F for all $1 \leq i \leq n$. Let:

$$f(x) = p_1(x) \cdots p_n(x)$$

and let N/E be the splitting field of $f(x)$ over E. Since $\alpha_1, \cdots, \alpha_n$ are roots of $f(x)$, N is also the splitting field of $f(x)$ over F. By Theorem 7.5, N is normal over F. Let $L \subseteq N$ be a subfield containing E, then L contains all α_i. If L is normal over F, each $p_i(x)$ splits over L. Thus $N \subseteq L$ and $L = N$.

Lecture 24, 2024/03/11

To show uniqueness, let N/E be the splitting field of $f(x)$ over E. Let N_1/F be another normal closure of E/F. Since N_1 is normal over F and contains all α_i, then 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 definition of normal closure, $\tilde{N} = N_1$. Thus N and N_1 are E-isomorphic. □

8 Galois Correspondence

8.1 Galois Extensions

We recall for a finite extension E/F we have:

Theorem 7.5 E is the splitting field of some $f(x) \in F[x] \iff E/F$ is normal.

Theorem 7.1 E is the splitting field of some separable $f(x) \in F[x] \implies E/F$ is separable.

Note If E is the splitting field of some $f(x) \in F[x]$, then we have the other implication in Theorem 7.1.

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

Remark We note that:

1. By Theorem 7.1 and 7.5, a finite Galois extension E/F is equivalent to the splitting field of a $f(x) \in F[x]$ 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 a separable $f(x) \in F[x]$ with $\deg(f) = n$. By Theorem 6.10, $\mathrm{Gal}_F(E)$ is a subgroup of S_n.

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

$$\psi(\sqrt{2}) \in \{\pm\sqrt{2}\} \quad \text{and} \quad \psi(\sqrt{3}) \in \{\pm\sqrt{3}\} \quad \text{and} \quad \psi(\sqrt{5}) \in \{\pm\sqrt{5}\}$$

Since $|\mathrm{Gal}_{\mathbb{Q}}(E)| = [E : \mathbb{Q}] = 8$ we have:

$$\mathrm{Gal}_{\mathbb{Q}}(E) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Definition Let $t_1, \cdots, t_n$ be variables. We define the **elementary symmetric functions** in $t_1, \cdots, t_n$ as $s_1, \cdots, s_n$ where for $1 \leq m \leq n$ we have:

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

For example, we have:

$$s_1 = t_1 + \cdots + t_n \quad \text{and} \quad s_2 = \sum_{1 \leq i < j \leq n} t_i t_j \quad \text{and} \quad s_n = t_1 \cdots t_n$$

Then, for $f(x) = (x - t_1) \cdots (x - t_n)$ we have:

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

Theorem 8.1 (E.Artin) Let E be a field and G a finite subgroup of $\mathrm{Aut}(E)$, the automorphism group of 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 we have that $[E : E^G] = |G|$.

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

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

where each α_i is distinct. Note that $m \leq n$. Let $f(x) = (x - \alpha_1) \cdots (x - \alpha_m)$. For any $\psi \in G$, we know ψ permutes the roots of $\alpha_1, \cdots, \alpha_m$. Since the coefficients of $f(x)$ are symmetric with respect to α_i for $1 \leq i \leq m$, they are fixed by all $\psi \in G$. Thus $f(x) \in E^G[x] = F[x]$. To show $f(x)$ is the minimal polynomial of α, consider a factorization $g(x) \in F[x]$ of $f(x)$. WLOG 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, there exists $\psi \in G$ such that:

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

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 E/F is Galois.

Lecture 25, 2024/03/13

We claim that $[E : F] \leq n$. Suppose for a contradiction that $[E : F] > n = |G|$, we can choose $\beta_1, \cdots, \beta_n, \beta_{n+1} \in E$ which are linearly independent over F. For all $G = \{\psi_1, \cdots, \psi_n\}$, 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 $v_1, \cdots, v_{n+1}$. Thus it has a nonzero solution in E (More columns than rows so nullity at least 1). Let $(\gamma_1, \cdots, \gamma_{n+1})$ 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 zero). WLOG assume $\gamma_1, \cdots, \gamma_r \neq 0$ and $\gamma_{r+1}, \cdots, \gamma_{n+1} = 0$. Thus:

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

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

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

this is because 1 is an automorphism, so we can take $\psi_i = 1$ for some i. There existst at least one $\gamma_i \notin F$. Since $r \geq 2$, WLOG we assume $\gamma_1 \notin F$. Choose $\phi \in G$ such that $\phi(\gamma_1) \neq \gamma_1$. 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 $j \in \{1, \cdots, n\}$. Since $\phi \in G$, therefore by the property of group we have:

$$\{\phi \circ \psi_1, \cdots, \phi \circ \psi_n\} = \{\psi_1, \cdots, \psi_n\} = G$$

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 $j \in \{1, \cdots, n\}$. Then by subtracting (3) from (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:

$$(\gamma_1 - \phi(\gamma_1), \cdots, \gamma_{r-1} - \phi(\gamma_{r-1}))$$

is a non-zero solution with fewer non-zero coordinates, which is a contradiction.

Using the claim we see that:

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

By “squeeze theorem” we get $[E : F] = n$ and $\operatorname{Gal}_F(E) = G$ as required. $\square$

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

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

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

Lecture 26, 2024/03/15

Our goal now is to find E^G. 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, w can get some hints about E^G. The G-orbit of t_1 is $\{t_1, \cdots, t_n\}$. By the above remark we know:

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

is the minimal polynomial of t_1 over E^G. Let $s_1, \cdots, s_n$ be the elementary symmetric functions of $t_1, \cdots, t_n$. 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 $L = F(s_1, \cdots, s_n)$. We claim that $L = E^G$. Note that $L \subseteq E^G$ and 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:

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

Since $L \subseteq E^G$, we have:

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

Thus $[E^G : L] = 1$ and $E^G = L$.

8.2 The Fundamental Theorem

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

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

and:

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

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

$$[L_1 : L_2] = [\mathrm{Gal}_{L_2}(E) : \mathrm{Gal}_{L_1}(E)] \ \text{ and } \ [H_1 : H_2] = [E^{H_2} : E^{H_1}]$$

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

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

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

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

$$(H^*)^* = (E^H)^* = \mathrm{Gal}_{E^H}(E) = H$$

Thus the maps $H \mapsto H^*$ and $L \mapsto L^*$ are inverses of each other.

Let $L_1, L_2 \in \mathrm{Int}(E/F)$. Since E/F is the splitting field of $f(x) \in F[x]$ 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:

$$L_2 \subseteq L_1 \implies \mathrm{Gal}_{L_1}(E) \subseteq \mathrm{Gal}_{L_2}(E)$$

Thus $L_1^* \subseteq L_2^*$. Also we have:

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

For $H_1, H_2 \in \text{Sub}(G)$, we have:

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

Thus $H_1^* \subseteq H_2^*$. Also we have:

$$[H_1 : H_2] = \frac{|H_1|}{|H_2|} = \frac{|\operatorname{Gal}_{E^{H_1}}(E)|}{|\operatorname{Gal}_{E^{H_2}}(E)|} = \frac{[E : E^{H_1}]}{[E : E^{H_2}]} = [E^{H_2} : E^{H_1}] = [H_2^* : H_1^*]$$

As desired. $\square$

Remark Consider the intermediate field between $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}$. Since we know $\operatorname{Gal}_{\mathbb{Q}}(E) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and it has finitely many subgroups, so there are only finitely many intermediate fields between E and $\mathbb{Q}$.

Lecture 27, 2024/03/18

We have seen that if E/F is a finite Galois extension and $L \in \operatorname{Int}(E/F)$, then L/F is not always Galois. For example:

$$E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3),\ L = \mathbb{Q}(\sqrt[3]{2}),\ F = \mathbb{Q}$$

Remark We have the following diagram:

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

From the picture, if L/F is Galois, it corresponds to the group G/L^*, which is only defined only if L^* is normal in G.

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

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

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

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

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

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

Since we have:

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

It follows that $\operatorname{Gal}_{\psi(L)}(E) = \psi \operatorname{Gal}_L(E)\psi^{-1}$. $\square$

Theorem 8.4 Let E/F, L, L^* be defined as in the fundamnetal theorem. Then L/F is a Galois extension if and only if L^* is normal subgroup of $G = \operatorname{Gal}_F(E)$. In this case, we have:

$$\operatorname{Gal}_F(L) \cong G/L^* = \operatorname{Gal}_F(E)/\operatorname{Gal}_L(E)$$

Proof: To get the "if and only if":

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

In this case, if L/F is a Galois extension, the restriction map:

$$G = \operatorname{Gal}_F(E) \to \operatorname{Gal}_F(L), \quad \text{by} \quad \psi \mapsto \psi|_L$$

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

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 $\alpha \to \alpha^p$. 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 $\mathbb{F}_q$, there exists $\alpha \in E$ such that $\alpha^{p^m} - \alpha \neq 0$. Thus $\sigma_p^m \neq 1$. Hence σ_p has order n. Let $G = \operatorname{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$, 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 a subgroup H of G of order d, then $d \mid n$ and $[G : H] = n/d$. By Theorem 8.2:

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

Thus $H^* = \mathbb{F}_q^H = \mathbb{F}_{p^{n/d}}$. Picture as follow:

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

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 Exericse).

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

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

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

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

and $\tau = \psi_{0,2}$ is:

$$\psi_{0,2} : \alpha \mapsto \alpha \ \text{ and } \ \zeta_5 \mapsto \zeta_5^2$$

It can be checked that $\tau\sigma = \sigma^2\tau$ (exericse) and we have:

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

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 Sylow's Theorem, we have $n_5 \mid 4$ and $n_5 \equiv 1 \pmod 5$. Hence $n_5 = 1$. Also $n_2 \mid 5$ and $n_2 \equiv 1 \pmod 2$. Hence $n_2 = 1$ or 5. If $n_2 = 1$, then $G \cong \mathbb{Z}_4 \times \mathbb{Z}_5$, which is abelian, and this contradicts that G is not abelian. Thus there are 5 Sylow-2 groups.

Lecture 28, 2024/03/20

We have seen that $\tau \in G$ is of order 4. Thus the cyclic group $\langle \tau \rangle$ is a Sylow-2 group and all other Sylow-2 groups are conjugate to it. Note that all elements of G are of the form $\sigma^a\tau^b$. Hence 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:

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

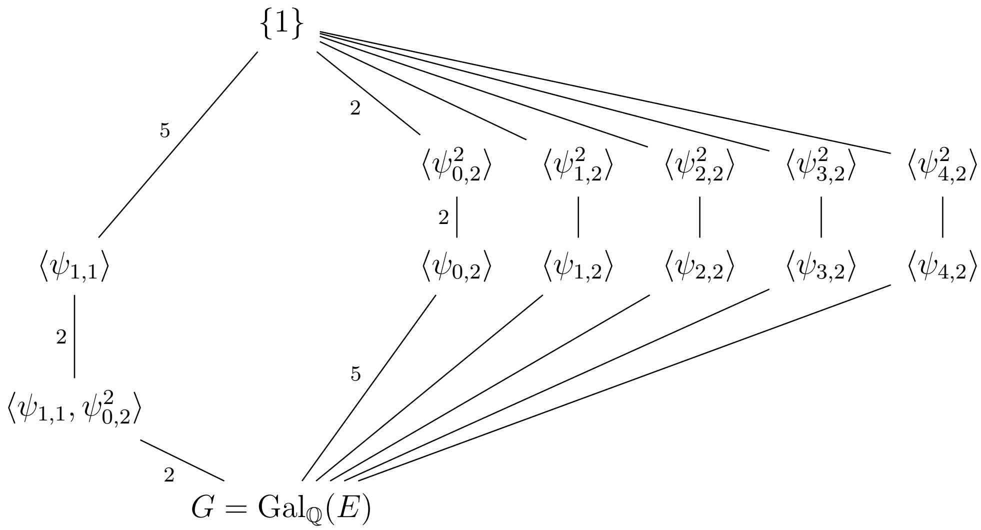
Using the same argument we see that the Sylow-2 subgroups are (exercise):

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

Moreover, since a subgroup of G of order of 2 are contains in a Sylow-2 subgroups:

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

are all subgroups of order 2.



For a subgroup H of G of order 10, since P_5 is the only subgroup 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. Hence $H = \langle \sigma\tau^2 \rangle$.

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:

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

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

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

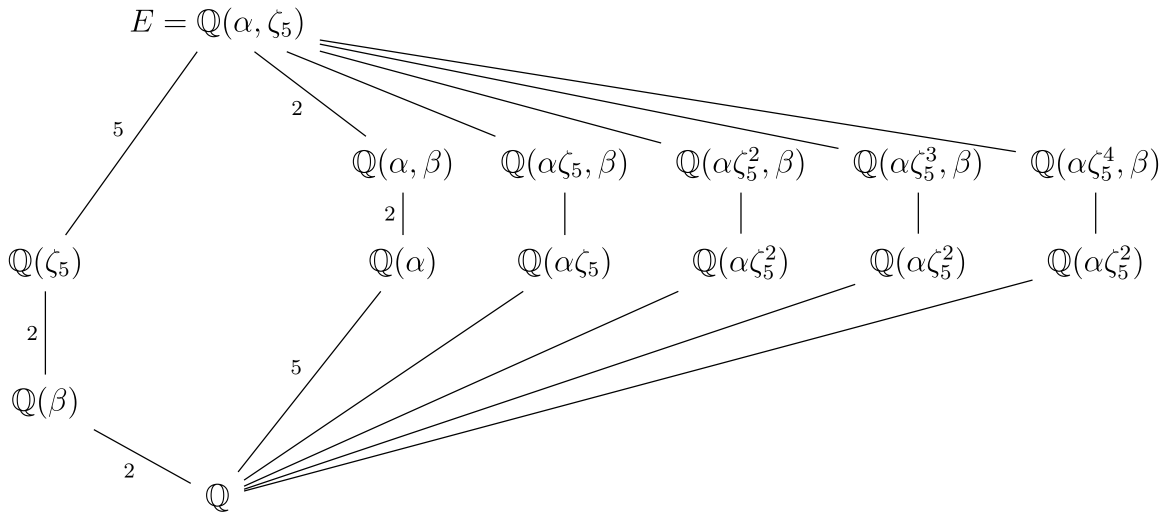
If $\psi_{1,2}$ fixed $\alpha\zeta_5^r$, then $r \equiv 2r + 1 \pmod 5$, that is, $r \equiv 4 \pmod 5$. Thus we have $\mathbb{Q}(\alpha\zeta_5^4)^* \supseteq \langle \psi_{1,2} \rangle$. Since:

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

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

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

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 $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Similarly $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$. Therefore, we have the following corresponding diagram of the intermediate fields of $E/\mathbb{Q}$.



Lecture 29, 2024/03/22

9 Cyclic Extension

Definition A Galois extension E/F is called **cyclic**, **abelian** 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 $\psi_i : L \to K$ be the distinct non-zero homomorphisms. If $c_i \in K$ and:

$$c_1\psi_1(\alpha) + \cdots + c_n\psi_n(\alpha) = 0$$

for all $\alpha \in L$, then $c_1 = \cdots = c_n = 0$.

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

$$c_1\psi_1(\alpha) + \cdots + c_n\psi_n(\alpha) = 0 \tag{1}$$

for all $\alpha \in L$. Let $m \geq 2$ be the minimal positive integer such that:

$$c_1\psi_1(\alpha) + \cdots + c_m\psi_m(\alpha) = 0$$

for all $\alpha \in L$. Since m is minimal, we have $c_i \neq 0$ for all $1 \leq i \leq m$. Since $\psi_1 \neq \psi_2$, we can choose $\beta \in L$ such that $\psi_1(\beta) \neq \psi_2(\beta)$. Moreover, we can assume $\psi_1(\beta) \neq 0$. By (1) we have:

$$c_1\psi_1(\alpha\beta) + \cdots + c_m\psi_m(\alpha\beta) = 0$$

for all $\alpha \in L$. By dividing the above equation by $\psi_1(\beta)$ we have:

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha) \cdot \frac{\psi_2(\beta)}{\psi_1(\beta)} + \cdots + c_m\psi_m \cdot \frac{\psi_m(\beta)}{\psi_1(\beta)} = 0 \tag{2}$$

for all $\alpha \in L$. Consider (1) $-$ (2), we obtain:

$$c_2\left(1 - \frac{\psi_2(\beta)}{\psi_1(\beta)}\right)\psi_2(\alpha) + \cdots + c_m\left(1 - \frac{\psi_m(\beta)}{\psi_1(\beta)}\right)\psi_m(\alpha) = 0$$

for all $\alpha \in L$. As $c_2(1 - \psi_2(\beta)/\psi_1(\beta)) \neq 0$, we have a contradiction with the minimal choice of m. Thus such $c_1, \cdots, c_m$ do not exist, and the lemma holds. $\square$

Theorem 9.2 Let F be a field and $n \in \mathbb{N}$. Suppose $\mathrm{ch}(F) = 0$ 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 $\{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}\}$ 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 $c_1 = 1, c_2 = \zeta_n^{-1}, \cdots, \zeta_n^{-(n-1)}$. 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:

$$\psi(\alpha) = \psi(u) + \zeta_n^{-1}\psi^2(u) + \cdots + \zeta_n^{-(n-1)}\psi^n(u) = \alpha\zeta_n$$

$$\psi^2(\alpha) = \alpha\zeta_n^2 \quad \cdots \quad \psi^{n-1}(\alpha) = \alpha\zeta_n^{n-1}$$

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

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

Since $\zeta_n \in F$ and $\alpha^n \in F$. 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 get $E = F(\alpha)$, as desired.

(2). Suppose $\alpha^n \in F$, 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 $p(x) \mid (x^d - \alpha^d)$. Since $\deg(p(x)) = d$ and $p(x)$ is monic, we have $p(x) = x^d - \alpha^d$.

Claim: $d \mid n$.

Lecture 30, 2024/03/25

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 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 $\deg(p(x)) = d > r$. Thus $d \mid n$, write $n = md$. Since $p(x) = x^d - \alpha^d$, then roots of $p(x)$ are:

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

Since $\zeta_n \in F$, so $E = F(\alpha)$ is the splitting field of the separable polynomial $p(x)$ over F, thus 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. $\square$

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 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 $\mathrm{ch}(F) = p$.

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

Thus $\alpha+1$ is also a root of $f(x)$. Similarly:

$$\alpha+2,\cdots,\alpha+(p-1)$$

are roots of $f(x)$. Since $f(x)$ has at most p distinct roots, thus:

$$\alpha,\ \alpha+1,\cdots,\alpha+(p-1)$$

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

$$\psi|_F=1|_F \ \text{ and } \ \psi(\alpha)=\alpha+1$$

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

$$\beta:=v+\psi(v)+\psi^2(v)+\cdots+\psi^{p-1}(v)\neq 0$$

Note that $\psi^i(\beta)=\beta$ for all $\psi^i\in G$ where $1\leq i\leq p-1$, we have $\beta\in F$. Set $u=v/\beta$. Since $\beta\in F$, we have:

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

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 hvae $[F(\alpha):F]$ 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 (x^p-x-a) is the minimal polynomial of α over F. $\square$

Lecture 31, 2024/03/27

10 Solvability by Radicals

10.1 Radical Extensions

Definition 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 $1 \leq i \leq m$.

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:

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E \tag{1}$$

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 $\beta = \beta_1, \cdots, \beta_n$ be roots of $p(x)$. By definition of normal closure and Theorem 7.5, we know:

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

Also there is an F-isomorphism $\sigma_j : F(\beta) \to F(\beta_j)$ by $\beta \mapsto \beta_j$ for all $2 \leq j \leq n$. 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 $2 \leq j \leq n$. Thus $\psi_j \in \mathrm{Gal}_F(N)$ and $\psi_j(\beta) = \beta_j$. We have the following tower of fields:

$$E = F(\beta_1) = F(\beta_1)\psi_2(F_0) \subseteq \cdots \subseteq F(\beta_1)\psi_2(F_m) = F(\beta_1, \beta_2) \tag{2}$$

For the last equality, it is because $F_m = F(\beta_1)$ and $\psi_2(\beta_1) = \beta_2$. Continue this way:

$$F(\beta_1, \beta_2) = F(\beta_1, \beta_2)\psi_3(F_0) \subseteq F(\beta_1, \beta_2)\psi(F_1) \subseteq \cdots \subseteq F(\beta_1, \cdots, \beta_n) = N \tag{3}$$

Appending (1), (2), and (3) we get the tower from F to N. To show this is radical, note that since $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$, we have:

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

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. $\square$

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

Definition 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 addition, subtraction, multiplication, division and taking n-th root is radical. Let F be a field and $f(x) \in F[x]$ be separable. If $f(x)$ is solvable by radicals, by the definition of radical extensions, $f(x)$ has a radical roots. Conversely, if $f(x)$ has a radical root, it is in some radical extension E/F. By Lemma 10.1, the normal closure N/F of E/F is radical. Since $f(x)$ splits over N and $f(x)$ is solvable by radical.

10.2 Radical Solutions

Lemma 10.2 Let E/F be a field extension and K, L be intermediate fields of E/F. Suppose K/L 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 KL is the splitting field of $f(x)$ over L, thus it is also Galois. Consider the map:

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

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 Γ is an injection. Thus by the first isomorphism theorem, $\mathrm{Gal}_L(KL) \cong \mathrm{im}\Gamma$, a subgroup of $\mathrm{Gal}_F(K)$. $\square$

Definition Let E/F be the splitting field of a polynomial $f(x) \in F[x]$ whose irreducible factor is 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 radical if and only if its Galois group $\mathrm{Gal}(f)$ is a solvable group.

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 $\mathrm{Gal}(f) \cong S_p$.

Example Consider $f(x) = x^5 + 2x^3 - 24x - 2 \in \mathbb{Q}[x]$, which is irreducible by Eisenstein with $p = 2$. Since $f(-1) = 19,\ f(1) = -23$ and:

$$\lim_{x\to\infty} f(x) = \infty \quad\text{and}\quad \lim_{x\to-\infty} f(x) = -\infty$$

By IVT we see $f(x)$ has at least 3 real roots. Let $\alpha_1, \cdots, \alpha_5$ be roots of $f(x)$, so:

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_5)$$

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 3 real roots and 2 non-real roots. By Proposition 10.4, we know $\mathrm{Gal}(f) \cong S_5$. Since S_5 is not solvable, by Theorem 10.3, the polynomial $x^5 + 2x^3 - 24x - 2$ is NOT solvable by radicals.

Lecture 32, 2024/04/01

Proof of Theorem 10.3: ($\Leftarrow$). Suppose $G = \mathrm{Gal}(f)$ is solvable, and let E/F be the splitting field of $f(x)$ and $n = |G|$. Let L/E be the splitting field of $(x^n - 1)$ over E and $\zeta_n \in L$, a primitive n-th root of unity. Set $K = F(\zeta_n)$ and we have $L = E(\zeta_n) = KE$. Since $L = KE$ and E/F is a finite Galois extension, by Lemma 10.2, L/K is a finite Galois extension and $H = \mathrm{Gal}_K(L)$ is isomorphic to a subgroup of G. By Theorem 6.3, H is solvable. Write:

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

where $H_i \triangleleft H_{i-1}$ and $H_{i-1}/H_i \cong C_{d_i}$, a cyclic group of order d_i, for all $1 \le i \le m$. Since H is a subgroup of G, we have $d_i \mid n$. Let $K_i = H_i^* = L^{H_i}$ for $0 \le i \le m$. By Theorem 6.11, we have $\mathrm{Gal}_{K_i} = H_i$. We have a tower of fields by reversing (1):

$$F \subseteq F(\zeta_n) = K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L = E(\zeta_n) \tag{2}$$

Since $H_i \triangleleft H_{i-1}$, by Theorem 8.4, K_i/K_{i-1} is Galois and:

$$\mathrm{Gal}_{K_{i-1}}(K_i) \cong H_{i-1}/H_i \cong C_{d_i}$$

Since ζ_n, thus $\zeta_{d_i} = \zeta_n^{n/d_i}$ is in K_{i-1}. By Theorem 9.2, there is $\alpha_i \in K_i$ with:

$$K_i = K_{i-1}(\alpha_i) \text{ and } \alpha_i^{d_i} \in K_{i-1}$$

Moreover, $K_0 = K = F(\zeta_n)$ and $\zeta_n^n = 1 \in F$. It follows that L/F is a radical extension. Since all roots of $f(x)$ are in E, thus in L, we conclude that $f(x)$ is solvable by radicals.

($\Rightarrow$). Suppose $f(x)$ is solvable by radicals, that is, $f(x)$ splits over some extension E/F satisfying:

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

with $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$. By Lemma 10.1, WLOG we can assume E/F is Galois. Thus E/F is the splitting field of some $\tilde{f}(x) \in F[x]$. Let:

$$n = \prod_{i=1}^{m} d_i = d_1 \cdots d_m$$

Let L/E be the splitting field of $(x^n - 1)$ over E and $\zeta_n \in L$ a primitive n-th root of unity. Set $K = F(\zeta_n)$ and we have $L = E(\zeta_n) = KE$. Define $K_i = KF_i = F_i(\zeta_n)$. Then we have:

$$F \subseteq F(\zeta_n) = K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = F_m(\zeta_n) = L$$

Since $F_i = F_{i-1}(\alpha_i)$, we have $K_i = K_{i-1}(\alpha_i)$. Since $\alpha_i^{d_i} \in F_{i-1} \subseteq K_{i-1}$ and $\zeta_n \in K_{i-1}$, thus $\zeta_{d_i} = \zeta_n^{n/d_i} \in K_{i-1}$. By Theorem 9.1, K_i/K_{i-1} is a cyclic Galois extension. Note that L is the splitting field of $\tilde{f}(x)(x^n - 1)$ over F (also K_i). Hence L/F (also L/K_i) is Galois. We have:

$$G = \operatorname{Gal}_F(L) \supseteq \operatorname{Gal}_{K_0}(L) \supseteq \operatorname{Gal}_{K_1}(L) \supseteq \cdots \supseteq \operatorname{Gal}_{K_m}(L) = \{1\}$$

Since K_i/K_{i-1} is a Galois extension, by Theorem 8.4, $\operatorname{Gal}_{K_i}(L)$ is normal in $\operatorname{Gal}_{K_{i-1}}(L)$ and we have:

$$\operatorname{Gal}_{K_{i-1}}(L)/\operatorname{Gal}_{K_i}(L) \cong \operatorname{Gal}_{K_{i-1}}(K_i)$$

which is cyclic, thus abelian. Also:

$$\operatorname{Gal}_F(L)/\operatorname{Gal}_{K_0}(L) = \operatorname{Gal}_F(L)/\operatorname{Gal}_K(L) \cong \operatorname{Gal}_F(K) = \mathbb{Z}_n^*$$

is abelian. Thus $\operatorname{Gal}_F(L)$ is solvable. Let $\tilde{E}$ be the splitting field of $f(x)$ over F, which is a subfield of L. Since $\tilde{E}/F$ is a Galois extension, by Theorem 8.4, we have:

$$\operatorname{Gal}(f) = \operatorname{Gal}_F(\tilde{E}) \cong \operatorname{Gal}_F(L)/\operatorname{Gal}_{\tilde{E}}(L)$$

Since $\operatorname{Gal}(f)$ is a quotient group of the subgroup $\operatorname{Gal}_F(L)$, by Theorem 6.3, $\operatorname{Gal}(f)$ is solvable. $\square$

Lecture 33, 2024/04/03

Proof of Proposition 10.4: We recall that the symmetric group S_n can be generated by (12) and $(12\cdots n)$. Thus to show $\operatorname{Gal}(f) \cong S_p$, it suffices to find a p-cycle and a 2-cycle in $\operatorname{Gal}(f)$. Since

$\deg(f) = p$, by Theorem 6.10, $\mathrm{Gal}(f)$ is a subgroup of S_p. 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, that is, a p-cycle. Also, the complex conjugate map $\sigma(a + bi) = a - bi$ will interchange two non-real roots of $f(x)$ and fixed all real roots. Thus it is an element of $\mathrm{Gal}(f)$, which is of order 2 (a 2-cycle). By changing notation if necessary, we have $(12),\ (12\cdots p) \in \mathrm{Gal}(f)$. It follows that $\mathrm{Gal}(f) \cong S_p$. $\square$

Example Recall that we have proved:

$$\mathrm{Gal}(x^5 + 2x^3 - 24x - 5) \cong S_5$$

From this 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 have:

Theorem 10.5 (Abel-Ruffini Theorem) A general polynomial $f(x) \in \mathbb{Q}[x]$ with $\deg(f) \geq 5$ is not solvable by radicals.

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

Remark Indeed, one can show that "almost all" polynomials $f(x)$ of degree n satisfies $\mathrm{Gal}(f) \cong S_n$. More precisely, let:

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

Then by using 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 " (density = 1) $f(x) \in \mathbb{Z}[x]$ with $\deg(f) = n$, we have $\mathrm{Gal}(f) \cong S_n$. So "almost all" polynomials are not solvable by radicals. This is the Probabilistic Galois Theory.

Lecture 34, 2024/04/05

11 Additional Topic: Cyclotomic Extensions

For a prime p, we have seen that a p-th cyclotomic polynomial:

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

is irreducible in $\mathbb{Q}[x]$. However, for a general $n \in \mathbb{N}$ with $n \geq 2$:

$$\frac{x^n - 1}{x - 1} = x^{n-1} + \cdots + x + 1$$

is not always irreducible. For example:

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

Thus $(x^4 - 1)$ is reducible in $\mathbb{Q}[x]$. Note that:

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

where $\zeta_p = e^{2\pi i/p}$. For each $k = 1, \cdots, (p-1)$, we have $\gcd(k, p) = 1$, therefore we can rewrite:

$$\Phi_p(x) = \prod_{\substack{1 \leq k \leq p \\ \gcd(k,p)=1}} (x - \zeta_p^k)$$

Let $\zeta_n = e^{2\pi i/n}$. For a general $k \in \mathbb{Z}$, the order of ζ_n^k is $\frac{n}{\gcd(n,k)}$. Then the order of ζ_n^k is the same the order of ζ_n if and only if $\gcd(n, k) = 1$.

Definition The n**-th cyclotomic polynomial** $\Phi_n(x)$ is defined by:

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \zeta_n^k)$$

where $\zeta_n = e^{2\pi i/n}$.

Proposition 11.1 $x^n - 1 = \prod_{d|n} \Phi_d(x)$

Theorem 11.2 (Gauss) $\Phi_n(x) \in \mathbb{Z}[x]$ and $\Phi_n(x)$ is irreducible.

Theorem 11.3 (Gauss) We have $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) = (\mathbb{Z}/n\mathbb{Z})^*$.

Definition For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $\gcd(k, n) = 1$, the field $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^k)$ is called the n**-th cyclotomic extension over** $\mathbb{Q}$.

Theorem 11.4 Let A be a finite abelian group. Then there exists a Galois extension $E/\mathbb{Q}$ with $E \subseteq \mathbb{Q}(\zeta_n)$ and $\mathrm{Gal}_{\mathbb{Q}}(E) \cong A$.

Lemma 11.5 Let p be a prime and $m \in \mathbb{N}$ with $p \nmid m$. Then for $a \in \mathbb{Z}$, p divides $\Phi_m(x)$ if and only if $p \nmid a$ and a has order m in $\mathbb{F}_p^*$.

We recall Euclid's Theorem that there are infinitely many primes. Since there is only one even prime, there are infinitely many primes of the form $p \equiv 1 \pmod 2$.

How about $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$? Are there infinitely many primes of either form?

Remark The original proof of Euler's Theorem works for $p \equiv 3 \pmod 4$ but not $p \equiv 1 \pmod 4$.

Question: For any positive integer m and $k \in \mathbb{Z}$ with $\gcd(k, m) = 1$. Are there infinitely many primes p of the form $p \equiv k \pmod m$?

Another way to formulate the question is to ask for $f(x) = mx + k$, the set of prime divisors of the sequence $(f(n))_{n=1}^{\infty} = \{f(1), f(2), \cdots\}$ is infinite.

Lemma 11.6 If $f(x) \in \mathbb{Z}[x]$ is monic and $\deg(f(x)) \geq 1$, then the set of prime divisors of the nonzero integer in the sequence $\{f(1), f(2), \cdots\}$ is infinite.

Theorem 11.7 (Dirichlet's Theorem) For $m, k \in \mathbb{N}$ with $m \geq 2$ and $\gcd(k, m) = 1$, there are infinitely many primes p such that $p \equiv k \pmod m$.

Remark Let $\pi(x) = \#\{p \text{ prime} : p \leq x\}$, and $\pi(x) \sim x/\log x$. Dirichlet proved that for $\gcd(k, m) = 1$, we have that:

$$\pi(x; m, k) := \#\{p \text{ prime} \leq x : p \equiv k \pmod{m}\} \sim \frac{\pi(x)}{\varphi(m)}$$

where φ is the Euler function.