Galois Theory

Ikhan Choi

December 14, 2021

Contents

Part I

Finite group theory

Chapter 1

Extension theory

1.1 Semidirect product

Definition 1.1.1 (External semidirect product)**.** Suppose we have three data: groups $(N,+),(H,\cdot)$ and a group homomorphism $\varphi : H \to \mathrm{Aut}(N)$. The *semidirect product* $N \rtimes_\varphi H$ is a group defined on the set $N \times H$ by

$$(n,h)(n',h') = (n + \varphi(h)n', hh').$$

The motivation of the group structure of semidirect product is shown in the following theorem.

Theorem 1.1.1 (Internal semidirect product)**.** *Let N,H be subgroups of G such that*

$$N \trianglelefteq G, \quad N \cap H = 1, \quad NH = G.$$

Then, $G \cong N \rtimes_\varphi H$, where the action φ is given by conjugation

$$\varphi(h) : N \to N : n \mapsto hnh^{-1}.$$

Lemma 1.1.2. *Let N,H be groups. Let $\varphi_1, \varphi_2 : H \to \mathrm{Aut}(N)$ be group actions. If there are $\nu \in \mathrm{Aut}(N)$ and $\eta \in \mathrm{Aut}(H)$ such that a diagram*

$$\begin{array}{ccc} H & \xrightarrow{\varphi_1} & \mathrm{Aut}(N) \\ \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \nu \cdot \nu^{-1}} \\ H & \xrightarrow{\varphi_2} & \mathrm{Aut}(N) \end{array}$$

commutes, then a map

$$N \rtimes_\varphi H \to N \rtimes_{\varphi'} H : (n,h) \mapsto (\nu(n), \eta(h))$$

is an isomorphism.

Lemma 1.1.3. *Let Z, G be finite groups. If Z is cyclic, then two group actions $\varphi, \varphi' : Z \to \mathrm{Aut}(G)$ induces the isomorphic semidirect products if and only if their images are conjugate.*

1.2 Extensions

Proposition 1.2.1. *Let N and H be groups. Then, the following objects have one-to-one correspondences among each other.*

(a) *isomorphic types of groups G such that a sequence*

$$0 \to N \to G \to H \to 0$$

is exact and right split,

(b) *isomorphic types of groups G such that $N \trianglelefteq G \geq H$ with $G = NH$ and $N \cap H = 1$,*

(c) *group actions $H \to \mathrm{Aut}(N)$ preserving the group structure of N.*

Definition 1.2.1. The group G in the previous proposition is called the *semidirect product* of N and H.

$$0 \to F \to E \to G \to 0.$$

Four data $G, F, \varphi : G \to \mathrm{Aut}(F), c : G \times G \to F$ completely determine the extension E.

Suppose we have an extension $F \to E \to G$. There is a *set-theoretic section* $s : G \to E$. The number of s is $|G||F|$.

Definition of *action* φ: For two sections s and s', $s(g)$ and $s'(g)$ acts on F equivalently. Thus, we can define a *group homomorphism* $\varphi : G \to \mathrm{Aut}(F)$ independently on sections.

Definition of *2-cocycle* c: It is a *set-theoretic function* $c : G \times G \to F$ defined by $c(g, g') = s(g)s(g')s(gg')^{-1}$ for a section s. Actually, c depends on the section s, and c measures how much s fails to be a group homomorphism. It requires the cocycle condition for the associativity of group operation, i.e.

$$c(g,h)c(gh,k) = \varphi_g(c(h,k))c(g,hk)$$

should be satisfied. Conversely, a map $G \times G \to F$ satisfying the condition the cocycle condition gives a associative group operation on G.

If F is abelian, then the set of cocycles forms an abelian group, and is denoted by $Z^2(G, F)$. The boundaries are also defined in abelian F case.

(a) φ, c is trivial $\iff$ direct product,

(b) c is trivial $\iff$ s is a homomorphism $\iff$ semidirect product,

(c) φ is trivial $\iff$ central extension.

Group cohomology is defined for a group G and G-module A (three data: G, A, φ. What is important is that the cohomology depends on the action of G on A.

If φ is trivial so that A is just an abelian group, then the universal coefficient theorem can be applied.

Chapter 2

The Sylow theorems

2.1 The Sylow theorems

2.1 (The Sylow theorems)**.** Let G be a finite group of order $n = p^a m$ for a prime $p \nmid m$. A *Sylow p-subgroup* is a subgroup of order p^a. Denote $\mathrm{Syl}_p(G)$ the set of Sylow p-subgroups and $n_p(G)$ its cardinality.

(a) $n_p \geq 1$.

(b) $n_p \equiv 1 \pmod{p}$.

(c) $n_p \mid m$.

Proof. (a) Suppose $\mathrm{Syl}_p(G) \neq \varnothing$ for all finite groups G such that $|G| < n$. The class equation for the action of G on G by conjugation is

$$n = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|,$$

where r is the number of non-trivial orbits.

If $p \mid |Z(G)|$, then, by the Cauchy theorem for abelian groups, $Z(G)$ has a normal subgroup P_p of order p, and so is a normal subgroup of G. For $Q \in \mathrm{Syl}_p(G/P_p)$, the inverse image of Q under the projection $G \to G/P_p$ is a Sylow p-subgroup of G. If $p \nmid |Z(G)|$, then we have $p \nmid |G : C_G(g)|$ for some $g \in G$, and with this g, we have $\mathrm{Syl}_p(C_G(g)) \subset \mathrm{Syl}_p(G)$. Then, we are done by induction.

(b) For $P \in \mathrm{Syl}_p(G)$, the class equation for the action of P on $\mathrm{Syl}_p(G)$ by conjugation is

$$n_p = f + \sum_{i=1}^{r} |P : N_P(P_i)|,$$

where f is the number of fixed points and r the number of non-trivial orbits.

If $P_i \in \mathrm{Syl}_p(G)$ is fixed, then P normalizes P_i so that $P < N_G(P_i)$, and by passing P though the projection $N_G(P_i) \to N_G(P_i)/P_i$ we can show $P = P_i$. Therefore, P is the only fixed point, so it follows that $n_p \equiv 1 \pmod{p}$ from

$$n_p = 1 + \sum_{i=1}^{r} |P : N_P(P_i)|.$$

(c) Suppose there are $P, P' \in \mathrm{Syl}_p(G)$ that are not conjugate. The class equations for actions of P and P' on $\mathrm{Orb}_G(P) \subset \mathrm{Syl}_p(G)$ are

$$|\mathrm{Orb}_G(P)| = 1 + \sum_{i=1}^{r} |P : N_P(P_i)| = \sum_{i=1}^{r'} |P' : N_{P'}(P_i)|,$$

because only P can fix P as shown in the part (b). It deduces $|\mathrm{Orb}_G(P)| \equiv 0, 1 \pmod{p}$ simultaneously, which is a contradiction. Therefore, the action of G on $\mathrm{Syl}_p(G)$ by conjugation is transitive and its class equation is

$$n_p = |G : N_G(P)|$$

for all $P \in \mathrm{Syl}_p(G)$. □

(a) every pair of two Sylow p-subgroup is conjugate.

(b) every p-subgroup is contained in a Sylow p-subgroup.

(c) a Sylow p-subgroup is normal if and only if $n_p = 1$.

Investigation of a group of a given order is divided into two main parts: the existence of a subgroup of particular orders and the measurement of the size of conjugate subgroups.

In order to show the existence of subgroups of paricular orders:

(a) p-groups always exist,

(b) extension theory, (what can subgroups of subgroups do?)

(c) normalizers,

(d) Poincare theorem: kernel of permutation representation

In order to find the size of conjugacy classes:

(a) measure the order of normalizers, (find some groups normalize a subgroup)

(b) count elements,

2.2 Classification of small groups

2.2 (Classification of groups of order pq)**.**

2.3 (Classification of groups of order p^2)**.**

2.4 (Classification of groups of order pqr)**.**

2.5 (Conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_p)$)**.** (a) $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$: $\binom{q-1}{2} = \frac{(q-1)(q-2)}{2}$ classes of size $\frac{|G|}{(q-1)^2} = q(q+1)$.

(b) $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$: $q-1$ classes of size 1.

(c) $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$: $q-1$ classes of size $\frac{|G|}{q(q-1)} = q^2-1$.

(d) otherwise, the eigenvalues are in $\mathbb{F}_{q^2}$. So, $\frac{|\mathbb{F}_{q^2}|-|\mathbb{F}_q|}{2} = \frac{q(q-1)}{2}$ classes of size $\frac{q(q-1)}{2}$.

2.6 (Classification of groups of order p^2q)**.** Let G be a finite group of order p^2q for distinct primes p, q.

(a) If $p+2 \le q$, there are

$$\begin{cases} 2 & \text{if } \nu_p(q-1) = 0, \\ 4 & \text{if } \nu_p(q-1) = 1, \\ 5 & \text{if } \nu_p(q-1) \ge 2 \end{cases}$$

non-isomorphic groups of order p^2q.

(b) If $p > q$, there are

$$\begin{cases} 5 & \text{if } q = 2, \\ \frac{q+9}{2} & \text{if } q \neq 2,\ q \mid p-1, \\ 3 & \text{if } q \neq 2,\ q \mid p+1 \\ 2 & \text{otherwise} \end{cases}$$

non-isomorphic groups of order p^2q.

(c) There are five non-isomorphic groups of order 12.

Proof. (a) Sylow's theorem implies $n_q = 1$. For $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$,

$$P \cong Z_{p^2} \text{ or } Z_p^2, \quad \text{and} \quad Q \cong Z_q.$$

Let $G \cong Z_q \rtimes Z_{p^2}$, and consider actions of the form

$$\varphi : Z_{p^2} \to \mathrm{Aut}(Z_q) \cong Z_{q-1}.$$

We count the number of conjugacy classes that can be the image of φ. There are $\min\{v_p(q-1), 3\}$ distinct groups.

Let $G \cong Z_q \rtimes (Z_p \times Z_p)$, and consider actions of the form

$$\varphi : Z_p \times Z_p \to \mathrm{Aut}(Z_q) \cong Z_{q-1}.$$

There are $\min\{v_p(q-1), 2\}$ distinct groups.

(b) Sylow's theorem implies $n_p = 1$.

(a) Let $G \cong Z_{p^2} \rtimes Z_q$, and consider actions of the form

$$\varphi : Z_q \to \mathrm{Aut}(Z_{p^2}) \cong Z_{p(p-1)}.$$

There are

$$\min\{v_q(p-1), 1\} = \begin{cases} 1 & , q \mid p-1, \\ 0 & , \text{otherwise} \end{cases}$$

nonabelian groups.

(b) Let $G \cong (Z_p \times Z_p) \rtimes Z_q$, and consider actions of the form

$$\varphi : Z_q \to \mathrm{Aut}(Z_p \times Z_p) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

Note that $|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p) = (p-1)^2 p(p+1)$. The conjugacy class of subgroups are classified by the Jordan normal forms.

If $q = 2$, then the possible conjugacy classes are represented by

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

There are

$$\begin{cases} 2 & , q = 2 \\ 1 & , 2 \nmid q \mid p+1, \\ \frac{q+3}{2} & , 2 \nmid q \mid p-1, \\ 0 & , \text{otherwise} \end{cases}$$

nonabelian groups. Since the number of one-dimensional linear subspaces is $q+1$ and the number of symmetric subspaces is 2 in $\mathbb{F}_q^2$, we have $\frac{(q+1)-2}{2} + 2 = \frac{q+3}{2}$ conjugacy classes of subgroups of order q in $\mathrm{GL}_2(\mathbb{F}_p)$.

(c)

□

2.7 (Classification of groups of order p^3)**.**

$\lvert G\rvert = p^2q\ (p<q)$	12	20	28	44	45	52	63
# of groups	5	5	4	4	2	5	4

$\lvert G\rvert = p^2q\ (p>q)$	18	50	75
# of groups	5	5	3

$\lvert G\rvert = pqr$	30	42
# of groups	4	6

$\lvert G\rvert = \prod^4 p$	16	24	40	54	56	36	60
# of groups	14	15	14	15	13	14	13

$\lvert G\rvert = \prod^{5 \text{ or } 6} p$	32	48	64
# of groups	51	52	267

2.3 Special groups

2.3.1 Cyclic groups

1. A subgroup is also cyclic.
2. The number of subgroups = the number of divisors of its order.
3. Endomorphism ring is given by $\mathbb{Z}/n\mathbb{Z}$.
4. Automorphism group is given by $(\mathbb{Z}/n\mathbb{Z})^\times$.
5. The number elements of order d is $\phi(d)$.
6.

2.3.2 Abelian groups

Fundamental theorem of finitely generated abelian groups

Theorem 2.3.1. *Let G be a finite group. If $G/Z(G)$ is cylic, then G is abelian.*

Theorem 2.3.2. *Let G be a finite group. If $x \mapsto x^3$ is a surjective endomorhpism, then G is abelian.*

2.3.3 Symmetric groups

2.3.4 Coxeter groups

2.3.5 Linear groups

Exercises

2.8. Alternative proof for existence of p-groups.

Proof. Let $|G| = p^{a+b}m$. Let $\mathcal{P}_{p^a}$ be the set of all p^a-sets in G. Give $G \to \mathrm{Sym}(\mathcal{P}_{p^a})$ by left multiplication. Since $\nu_p(|\mathcal{P}_{p^a}|) = \nu_p(\binom{p^a(p^bm)}{p^a}) = b$, there is an orbit $\mathcal{O}$ such that $\nu_p(|\mathcal{O}|) \leq b$. We have transitive action $G \to \mathrm{Sym}(\mathcal{O})$ and the stabilizer H satisfies $p^a \mid |G|/|\mathcal{O}| = |H|$. Since $H \to \mathrm{Sym}(\mathcal{O})$ trivially, $H \to \mathrm{Sym}(A)$ for $A \in \mathcal{O} \subset \mathcal{P}_{p^a}$. It is only possible when $H \subset A$, hence $|H| = p^a$. □

Chapter 3

Subnormal series

Part II

Field extentsions

Chapter 4

Algebraic extensions

4.1 Algebraic elements

4.1. *Algebraic elements.* Let E/F be a field extension. An element $\alpha \in E$ is called *algebraic over* F if there is a non-zero polynomial $f \in F[x]$ such that $f(\alpha) = 0$. If α is not algebraic over F, we call it *transcendental* over F. For $\alpha \in E$, the following statements are all equivalent:

(a) The element α is algebraic over F.

(b) The ring $F[\alpha]$ is a field.

(c) The equality $F(\alpha) = F[\alpha]$ holds.

(d) The simple extension $F(\alpha)/F$ is finite.

Proof. (a) $\Rightarrow$ (b) Note $F[\alpha] = F$ is a field if $\alpha = 0$. Let $\alpha \neq 0$. Define a ring homomorphism

$$\mathrm{eval}_\alpha : F[x] \to F[\alpha] : f(x) \mapsto f(\alpha),$$

which is called *evaluation*. The kernel of eval_α contains α, hence is non-zero, and it is a prime ideal because the quotient

$$F[x]/\ker(\mathrm{eval}_\alpha) \cong \mathrm{im}(\mathrm{eval}_\alpha) = F[\alpha]$$

is an integral domain. Since $F[x]$ is a principal ideal domain so that every non-zero prime ideal is maximal, the quotient $F[\alpha]$ is a field.

(b) $\Rightarrow$ (c) We clearly have $F[\alpha] \subset F(\alpha)$. Since $F(\alpha)$ is defined as the intersection of all subfields of E containing F and α, $F(\alpha) \subset F[\alpha]$.

(c) $\Rightarrow$ (a) There is $g \in F[x]$ such that $\alpha^{-1} = g(\alpha)$. Then, $f \in F[x]$ defined by $f(x) = xg(x) - 1$ satisfies $f(\alpha) = 0$.

(a),(c) $\Rightarrow$ (d) Let $f \in F[x]$ be non-zero with $f(\alpha) = 0$. For an element $g(\alpha)$ of $F(\alpha) = F[\alpha]$ for some $g \in F[x]$, there are $q, r \in F[x]$ such that $g = qf + r$ and $\deg r < \deg f$ by the Euclidean algorithm, so $g(\alpha) = r(\alpha)$. Since $r(\alpha)$ is a linear combination of $\{1, \alpha, \cdots, \alpha^{\deg f - 1}\}$ over F, we get $[F(\alpha) : F] \leq \deg f$.

(d) $\Rightarrow$ (a) Since $[F(\alpha) : F] < \infty$, we can find a linearly dependent finite subset of a set $\{1, \alpha, \alpha^2, \cdots\} \subset F(\alpha)$ over F. The coefficients on the linear dependency relation construct the polynomial. □

Since the ideal $\ker(\mathrm{eval}_\alpha) \subset F[x]$ for algebraic $\alpha \in E$ is maximal, the following definition makes sense:

Definition 4.1.1. Let E/F be a field extension and $\alpha \in E$ is algebraic. The unique monic irreducible polynomial $\mu_{\alpha,F} \in F[x]$ satisfying

$$\mu_{\alpha,F}(\alpha) = 0$$

is called the *minimal polynomial of α over F*.

Theorem 4.1.1. *Let E/F be a field extension and $\alpha \in E$ is algebraic. Then,*

$$F(\alpha) \cong F[x]/(\mu_{\alpha,F}).$$

In particular, $[F(\alpha) : F] = \deg \mu_{\alpha,F}$.

Proof. The kernel of $\mathrm{eval}_\alpha : F[x] \to F(\alpha)$ is characterized as the principal ideal generated by $\mu_{\alpha,F}$, so we find the isomorphism $F[x]/(\mu_{\alpha,F}) \cong F(\alpha)$.

Now we claim the dimension of $F[x]/(f)$ over F is the degree of $f \in F[x]$. It is enough to show $\{1, x, \cdots, x^{d-1}\}$ is a basis where $d = \deg f$. We can check this with the Euclidean algorithm. □

Example 4.1.1. Consider a field extension $\mathbb{C}/\mathbb{Q}$. The minimal polynomial of $\sqrt{2} \in \mathbb{C}$ over $\mathbb{Q}$ is

$$\mu_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$$

since it is monic irreducible and has a root $\sqrt{2}$. Similarly, the minimal polynomial of $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ over $\mathbb{Q}$ is

$$\mu_{\omega,\mathbb{Q}}(x) = x^2 + x + 1.$$

Example 4.1.2. We can compute the degree of a field extension by finding minimal polynomial. Since the minimal polynomial $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is

$$\mu_{\sqrt{2}+\sqrt{3},\mathbb{Q}}(x) = x^4 - 10x^2 + 1,$$

we have

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = \deg(x^4 - 10x^2 + 1) = 4.$$

On the other hand, we have

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\cdot 2 = 4.$$

Since $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ implies $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \leq \mathbb{Q}(\sqrt{2},\sqrt{3})$ and the dimensions as vector spaces are equal, we get $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. We can also directly check

$$\sqrt{2} = \frac{1}{2}\left(\alpha - \frac{1}{\alpha}\right) \quad \text{and} \quad \sqrt{3} = \frac{1}{2}\left(\alpha + \frac{1}{\alpha}\right),$$

where $\alpha = \sqrt{2}+\sqrt{3}$. This kind of *dimension argument* is one of powerful tools to attack field theory. It will be discovered later that the dimension argument has an analogy with computation of group orders in finite group theory.

Example 4.1.3. The base field is important: we have

$$\mu_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2, \quad \text{but} \quad \mu_{\sqrt{2},\mathbb{Q}(\sqrt{2})}(x) = x - \sqrt{2}.$$

Example 4.1.4. Although $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1+\sqrt{2})$, the minimal polynomials of $\sqrt{2}$ and $1+\sqrt{2}$ over $\mathbb{Q}$ are x^2-2 and $(x-1)^2-2$ respectively. Polynomials are usually used in order to be provided as a computational tool, so we frequently want to find a suitable minimal polynomial for a given field extension. However, note that a finite simple extension does not specify only one minimal polynomial as the above example. It is enough to find only one minimal polynomial that is effective in computation.

4.1.1 Conjugates

Definition 4.1.2. Let E/F be a field extension and $\alpha, \beta \in E$ be algebraic over F They are said to be *conjugate over* F if they share a common minimal polynomial over F.

In other words, conjugates share the maximal ideal ker(eval), hence we get that $F(\alpha)$ and $F(\beta)$ are isomorphic. For the practical isomorphism map, we have the following theorem. It is also useful when we compute field automorphisms explicitly.

Theorem 4.1.2 (Conjugation isomorphism)**.** *Let E/F be a field extension. Two elements $\alpha, \beta \in E$ are conjugate over F iff there is a field isomorphism $\phi : F(\alpha) \to F(\beta)$ such that*

$$\phi : \alpha \mapsto \beta \quad \textit{and} \quad \phi|_F = \mathrm{id}|_F.$$

Proof. ($\Rightarrow$) Let $\mu \in F[x]$ be the common minimal polynomial of α and β over F and define a map

$$\phi : F(\alpha) \xrightarrow{\sim} F[x]/(\mu) \xrightarrow{\sim} F(\beta) : \alpha \mapsto x + (\mu) \mapsto \beta.$$

Since it is clearly a field homomorphism and we can define the inverse in the same manner, so is an isomorphism. It is easy to check $\phi(\alpha) = \beta$ and $\phi|_F = \mathrm{id}_F$. In particular, the two conditions uniquely determine ϕ.

($\Leftarrow$) Suppose $\phi : F(\alpha) \to F(\beta) : \alpha \mapsto \beta$ is a field homomorphism fixing F. Then, ϕ commutes with a polynomial function with coefficients in F. From

$$\mu_{\alpha,F}(\beta) = \mu_{\alpha,F}(\phi(\alpha)) = \phi(\mu_{\alpha,F}(\alpha)) = \phi(0) = 0,$$

we get $\mu_{\beta,F} \mid \mu_{\alpha,F}$. The irreducibility of $\mu_{\alpha,F}$ implies $\mu_{\alpha,F} = \mu_{\beta,F}$. □

Corollary 4.1.3. *Let $\phi : F \to F$ is a field automorphism. Then, α and $\phi(\alpha)$ are always conjugates.*

Example 4.1.5. The base fields are important. There are two conjugates of $\sqrt{2} \in \mathbb{C}$ over $\mathbb{Q}$: $\{\pm\sqrt{2}\}$. However, there is only one conjugate of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$ or $\mathbb{C}$: itself $\{\sqrt{2}\}$.

Example 4.1.6. There are two conjugates of $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ over $\mathbb{Q}$: $\{\omega, \overline{\omega} = \omega^{-1}\}$. It implies that there are at most two field automorphisms on $\mathbb{Q}(\omega)$ fixing $\mathbb{Q}$. In fact, there are exactly two; one is identity, and the other is the complex conjugation.

Example 4.1.7. For almost every case in applications, the number of conjugates is same as the degree of its minimal polynomial. However, there are counterexamples; two field isomorphisms $\phi_1 : \alpha \mapsto \beta_1$ and $\phi_2 : \alpha \mapsto \beta_2$ may be the same even for $\beta_1 \neq \beta_2$. See Section 3 for the detailed discussion.

Example 4.1.8. The isomorphism does not have to be an automorphism. There are four conjugates of $\sqrt[4]{2}$ over $\mathbb{Q}$: $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. However, $\mathbb{Q}(\sqrt[4]{2}) \neq \mathbb{Q}(i\sqrt[4]{2})$ even though they are isomorphic. See Section 4.

4.2 Algebraic extensions

Algebraic extension is a generalization of finite extensions, for instance, every finite extension. In Galois theory, which will be studied later, we will not care elements that are not algebriac. Therefore, it is natural to think of a field extension that only consists of algebraic elements, which is called also algebraic. The main interests in Galois theory will be restricted to algebraic extensions. To people who know the category theory, an algebraic extension is just a direct limit of finite simple extensions.

Definition 4.2.1. A field extension E/F is called *algebraic* if all elements $\alpha \in E$ are algebraic over F.

The easiest example of an algebraic extension is a finite extension. The relations between finite extensions and algebraic extension are as follows.

Proposition 4.2.1. *For finite extensions and algebraic extensions, we have:*

(a) *a finite extension is algebraic,*

(b) *a simple algebraic extension is finite.*

Proof. Easy. □

Now, we are going to get some basic criteria for determining or constructing algebraic extensions. If summarized, we can just say any basic operations of algebraic extensions are algebraic. Before that, we introduce a good notion about algebraic extensions: the set of all algebraic elements in a given field.

In the rest of this subsection, assume that we have fixed a sufficiently large ambient field L. Restricting the "domain of discourse" by assuming a large entire field is a greatly helpful idea in order not to be confused in the theory of extensions. For example, if we do not fix such a field L, we might be able to consider useless large fields which may grow without limits. Moreover, we cannot think about the number of field extensions satisfying particular properties.

Note that the following definition *depends on the choice of* L, and we will use it *only in this subsection*.

Definition 4.2.2. Let $\overline{F}$ denote the set of all algebraic elements in L over F.

Proposition 4.2.2. *The set* $\overline{F}$ *of* F *in* L *is always a field.*

Proof. An element is algebraic over F if and only if it is contained in a finite extension E/F because $\alpha \in E$ is equivalent to $F(\alpha) \leq E$.

Let $\alpha, \beta \in L$ be nonzero algebraic elements over a field F. Since $\alpha+\beta$, $\alpha\beta$, and α^{-1} are all in $F(\alpha,\beta)$, which is a finite extension of F with degree $\deg_F(\alpha)\deg_F(\beta)$, the set of algebraic elements over F in L is a field. □

Remark. The field $\overline{F}$ is called the *relative algebraic closure of F in L*. Since we have not defined algebraic closures yet, we will only adopt the notation. The reason of the word "relative" is explained later. Also, honestly, the notation $\overline{F}$ is not so good that it is often used to represent an algebraic closure, not a relative one. We, however, proceed with this notation to grasp concepts of algebraic extensions.

Lemma 4.2.3. *Let L be any field containing two fields E, F. Then,*

(a) *$F \leq E$ implies $\overline{F} \leq \overline{E}$,*

(b) *$\overline{\overline{F}} = \overline{F}$.*

Proof. (a) Suppose $\alpha \in \overline{F}$ so that there is $f \in F[x]$ such that $f(\alpha) = 0$. Since $f \in F[x] \subset E[x]$, the element α is also algebraic over E, hence $\alpha \in \overline{E}$.

(b) It is enough to show $\overline{\overline{F}} \subset \overline{F}$. Let $\alpha \in \overline{\overline{F}}$ so that we can find $f \in \overline{F}[x]$ such that

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0.$$

If we consider the field $E = F(a_0, \cdots, a_n)$ of coefficients, then $f \in E[x]$. In other words, α is algebraic over E.

The field extension E/F is finite since all generators a_i are algebraic over F, and $E(\alpha)/E$ is also finite since α is algebraic over E. Therefore, the field extension $E(\alpha)/F$ is finite, and $F(\alpha)/F$ is also finite, hence the algebraicity of α over F. □

Theorem 4.2.4. *Let E/F be a field extension.*

(a) *Fix any $L \geq E$. Then, E/F is algebraic iff $\overline{E} = \overline{F}$.*

(b) *Let $F \leq K \leq E$. Then, E/F is algebraic iff E/K and K/F are algebraic.*

(c) *The compositum E_1E_2/F is algebriac if E_1/F and E_2/F are algebraic.*

Proof. (a) If E/F is algebraic, then $F \leq E \leq \overline{F}$ implies $\overline{F} \leq \overline{E} \leq \overline{\overline{F}} = \overline{F}$. Conversely, if $\overline{E} = \overline{F}$, then $\alpha \in E$ implies $\alpha \in E \leq \overline{E} = \overline{F}$, hence E is algebraic over F.

(b) Choose a big L. Since $\overline{E} \geq \overline{K} \geq \overline{F}$, we have $\overline{E} = \overline{F}$ iff $\overline{E} = \overline{K}$ and $\overline{K} = \overline{F}$.

(b') A direct proof uses the argument in the proof of above lemma as follows: if we take $\alpha \in E$ that is algebraic over K, and if a_i denotes the coefficients of $\mu_{\alpha,K}$, then the field extension $F(a_1, \cdots, a_n, \alpha)/F$ is finite, so α is algebriac over F.

(c) Choose a big L. Since $E_1, E_2 \leq \overline{F}$, we have $E_1E_2 \leq \overline{F}$, so $\overline{E_1E_2} = \overline{F}$. □

Remark. An algebraic extension is a direct limit of finite extensions. In other words, a field E is algebraic over F if and only if there is a tower of fields $\{K_\alpha\}_\alpha$ such that K_α/F are all finite and the ascending union is E. We skip the proof.

Example 4.2.1. For a transcendental number such as π, the extension $\mathbb{Q}(\pi)/\mathbb{Q}$ is not algebraic since it contains an element that is not algebraic. It is also because a simple extension is algebraic if and only if it is finite but $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$.

Example 4.2.2. Finite extensions are not only the algebraic extensions. For examples,

$$\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \cdots), \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \cdots)$$

are infinite algebraic extensions.

4.3 Algebraic closures

Algebraic closure is intuitively a maximal algebraic extension. It is well described using the notion of algebraically closed fields. Although the existence will be proved later, we give definitions.

4.3.1 Algebraically closed fields

Definition 4.3.1. A field F is called *algebraically closed* if it has no proper algebraic extension.

Proposition 4.3.1. *For a field F, the following statements are all equivalent:*

(a) *F is algebraically closed,*

(b) *every polynomial in $F[x]$ has a root in F,*

(c) *every polynomial in $F[x]$ is linearly factorized in F; every root is in F.*

Proof. (a) ⇒ (b) If $f \in F[x]$ does not have root in F, then the proper finite extension $(F[x]/(f))/F$ shows that F is not algebraically closed.

(b) $\Rightarrow$ (c) If f has a root α, then we can inductively apply this theorem for a new polynomial $f(x)/(x-\alpha)$ of a lower degree to make the complete linear factorization.

(c) $\Rightarrow$ (a) If F is not algebraically closed so that there is a proper algebraic extension E/F, then the minimal polynomial $\alpha \in E \setminus F$ should be irreducible with degree bigger than 1. □

Remark. In particular, this proposition implies that algebraically closedness can be described in itself by factorizations. Namely, it is an internal property; it is preserved under isomorphisms.

Definition 4.3.2. A field $\overline{F}$ is called an *algebraic closure* of a field F if $\overline{F}$ is algebraically closed field and $\overline{F}/F$ is algebraic.

Proposition 4.3.2. *Let E/F be a field extension with E algebraically closed. Then the set of all algebraic elements in E over F is the only algebraic closure of F contained in E.*

Proof. For a while in this proof, let $\overline{F}$ denote the set of all algebraic elements of F in E.

Step 1: Algebraic closure. We will show that $\overline{F}$ is algebraically closed because the extension $\overline{F}/F$ is clearly algebraic. Let $f \in \overline{F}[x]$ and take a root $\alpha \in E$. Since both $\overline{F}(\alpha)/\overline{F}$ and $\overline{F}/F$ are algebraic, α is algebraic over F. Thus we have $\alpha \in \overline{F}$, and by the previous proposition, $\overline{F}$ is algebraically closed.

Step 2: Uniqueness. Suppose K is an algebraic closure of F in E. We have $\overline{F} \leq K$ since every algebraic element α with $f(\alpha) = 0$ for $f \in F[x] \subset K[x]$ should be contained in K. Also, $K/\overline{F}$ is algebraic because K/F is algebraic. Since $\overline{F}$ is algebraically closed, $K = \overline{F}$. □

This is a relation with relative algebraic closure: the relative algebraic closure in a algebraically closed field is really an algebraically closure. The proposition allows us to choose a standard algebraic closure when provided a large superfield like $\mathbb{C}$. In number theory, it is convenient for all algebraically closed fields to be considered that they are in $\mathbb{C}$.

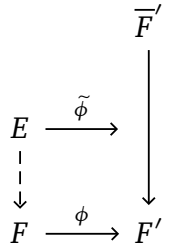
Example 4.3.1. The set of all complex numbers $\mathbb{C}$ is an algebraically closed field by the fundamental theorem of algebra.

Example 4.3.2. The set of all algebraic numbers (over $\mathbb{Q}$) is an algebraically closed field by the proposition above and is a subfield of $\mathbb{C}$.

4.3.2 Uniqueness and existence

Here is a useful lemma that allows to apply the axiom of choice to field theory.

Theorem 4.3.3 (Isomorphism extension theorem)**.** *Let E/F be an algebraic extension. Let $\phi : F \cong F'$ be a field isomorphism. Let $\overline{F}'$ be an algebraic closure of F'. Then, there is an embedding $\widetilde{\phi} : E \to \overline{F}'$ which extends ϕ.*



Proof. Let S be the set of all field homomorphisms $K \to \overline{F}'$ which extends ϕ and satisfies $K \leq E$. The set S is nonempty since $\phi \in S$ and satisfies the chain condition since the increasing union defines the upper bound of chain. Use the Zorn lemma on S to obtain a maximal element $\widetilde{\phi} : K \to \overline{F}'$. We want to show $K = E$.

Suppose K is a proper subfield of E and let $\alpha \in E \setminus K$. Let $\alpha' \in \overline{F}'$ be a root of the pushforward polynomial $\phi_*(\mu_{\alpha,F}) \in F'[x]$. Then, we can construct a field homomorphism $K(\alpha) \to \overline{F}' : \alpha \mapsto \alpha'$. It leads a contradiction to the maximality of $\widetilde{\phi}$. Therefore, $K = E$. □

Theorem 4.3.4 (Uniqueness of algebraic closure)**.** *Algebraic closure is unique up to isomorphism.*

Proof. Suppose there are two algebraic closures $\overline{F}_1, \overline{F}_2$ of a field F. By the isomorphism extension theorem, we have a field homomorphism $\phi : \overline{F}_1 \to \overline{F}_2$ which extends the identitiy map on F. Since the image $\phi(F_1)$ is also algebraically closed and the field extension $F_2/\phi(F_1)$ is algebraic, we must have $\phi(F_1) = F_2$ by the definition of algebraically closedness. Thus, ϕ is surjective so that it is an isomorphism. □

Theorem 4.3.5 (Existence of algebraic closure)**.** *Every field has an algebraic closure.*

Proof. Let F be a field.

Step 1: Construct an algebraically closed field containing F. At first we want to construct a field $K_1 \geq F$ such that every $f \in F[x]$ has a root in K_1. This is satisfied by $K_1 := R/\mathfrak{m}$, where a ring R and its maximal ideal $\mathfrak{m}$ is defined as follows: Let S be the set of all nonconstant irreducibles in $F[x]$. Define $R := F[\{x_f\}_{f \in S}]$. Let I be

an ideal in R generated by $f(x_f)$ as f runs through all S. It has a maximal ideal $\mathfrak{m} \supset I$ in R since I does not contain constants. If $f \in F[x]$, then $\alpha = x_f + \mathfrak{m} \in K_1$ satisfies $f(\alpha) = f(x_f) + \mathfrak{m} = \mathfrak{m}$.

Construct a sequence $\{K_n\}_n$ of fields inductively such that every nonconstant $k \in K_n[x]$ has a root in K_{n+1}. Define $K := \lim_{\to} K_n$ as the inductive limit. It is in other word just the directed union of K_n through all $n \in \mathbb{N}$. Then, K is easily checked to be algebraically closed.

Step 2: Construct the algebraic closure of F. Let $\overline{F}$ be the set of all algebraic elements of K over F. Then, this is an algebraic closure. □

Remark. In fact, this K_1 is already algebraically closed, but it is hard to prove directly, so we are going to construct another algebraically closed field, K.

Problems

4.2 (Minimal polynomials in a simple extension)**.** Let $F(\alpha)/F$ be a finite simple extension of a field F and let $\beta \in F(\alpha)$. In light of elementary linear algebra, we Let

(a)

(b) small problem

4.3 (Title)**.** Problem

Chapter 5

Separable extensions

5.1 Separable polynomials

Definition 5.1.1. Let F be a field. A polynomial $f \in F[x]$ is called *separable* if it is square-free in $\overline{F}[x]$. An element $\alpha \in \overline{F}'$ is called *separable* over F if $\mu_{\alpha,F}$ is separable.

The separability of a polynomial does not depend on coefficient fields, but their characteristic. We can consider the algebraic closure of the smallest field containing coefficients of the polynomial and its characteristic when we check separability of a polynomial.

5.1.1 Formal derivatives

Definition 5.1.2. Let $f \in F[x]$ for a field F such that

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

The *formal derivative* of f is defined as a polynomial $f' \in F[x]$ such that

$$f'(x) := \sum_{i=1}^{n} i a_i x^{i-1}.$$

We can easily check that this definition satisfies the Leibniz rule.

Proposition 5.1.1. *Let $f \in F[x]$ for a field F. Then, f is separable iff f and f' are coprime in F.*

Proof. The polynomials f, f' is linearly factorized in $\overline{F}$.

($\Leftarrow$) Suppose f is not separable so that it has a multiple root $\alpha \in \overline{F}$ and

$$f(x) = (x-\alpha)^m g(x)$$

for an integer $m \geq 2$ and a polynomial $g \in F[x]$. Its derivative is

$$f'(x) = m(x-\alpha)^{m-1} g(x) - (x-\alpha)^m g'(x).$$

Since $f(\alpha) = f'(\alpha) = 0$, we have $\mu_{\alpha,F} \mid \gcd(f, f')$. They are not coprime in F.

($\Rightarrow$) Suppose f and f' are not coprime in F so that they has a common factor. Let $\alpha \in \overline{F}$ be a root of the common factor. If we write

$$f(x) = (x-\alpha)g(x), \qquad f'(x) = g(x) + (x-a)g'(x),$$

then we can see $g(\alpha) = 0$ and $(x-\alpha) \mid g$ in $\overline{F}[x]$. Hence $(x-\alpha)^2 \mid f$, so f is not separable. □

Remark. This is a powerful checking tool because the proposition do not requires that f and f' are coprime in $\overline{F}$, but in just F.

Example 5.1.1. Let $f(x) = x^{p^n} - x$ be a polynomial over a field of characteristic $p > 0$. Since $f'(x) = -1$, f is separable.

5.1.2 Relation to irreducibles

Definition 5.1.3. A *perfect field* is a field over which every irreducible is separable.

Corollary 5.1.2. *A polynomial over a perfect field is separable iff it is a product of distinct irreducibles.*

Proposition 5.1.3. *Let F be a field of characteristic 0. Then, F is perfect.*

Proof. Let $f \in F[x]$ be an irreducible of degree n. Notice that f and g are not coprime iff $f \mid g$. Since F has characteristic 0, f' has degree $n-1$ and is nonzero, so we have $f \nmid f'$. Hence f is separable. □

Proposition 5.1.4. *Let F be a field of characteristic $p > 0$. Then, F is perfect iff F has the Frobenius automorphism.*

Proof. ($\Leftarrow$) Let $f \in F[x]$ be an inseparable irreducible. Since we must have $f' = 0$ by the irreducibility of f, we can find $g \in F[x]$ such that $f(x) = g(x^p)$. The coefficients of g are p-powers of elements of F, so there is $h \in F[x]$ such that $g(x^p) = h(x)^p$. It is a contradiction to the irreducibility of f. □

Corollary 5.1.5. *The rational field $\mathbb{Q}$ and every finite fields are perfect.*

Proposition 5.1.6. *Let F be a field of characteristic $p > 0$. For an irreducible $f \in F[x]$, there is a unique separable irreducible $f_{\text{sep}} \in F[x]$ such that $f(x) = f_{\text{sep}}(x^{p^k})$ for some k.*

Example 5.1.2. The Frobenius endomorphism is not surjective in the field of rational functions $\mathbb{F}_p(t)$, where t is not algebraic over $\mathbb{F}_p$. For example, t is not in the image of $\mathbb{F}_p(t) \to \mathbb{F}_p(t) : x \mapsto x^p$. Then, the polynomial $x^p - t \in \mathbb{F}_p(t)[x]$ is inseparable irreducible since it is factorized as

$$x^p - t = (x - t^{\frac{1}{p}})^p$$

in $\overline{\mathbb{F}_p(t)}[x]$.

5.2 Separable extensions

Definition 5.2.1. A field extension E/F is called *separable* if all elements in E is separable over F.

Theorem 5.2.1 (Primitive element theorem)**.** *A finite separable extension is simple.*

5.3 Separable closures

Definition 5.3.1. Let E/F be a field extension. The *separable degree* of E/F is the number $[\overline{F}^{\text{sep}} : F]$.

5.3.1 Field embeddings

Theorem 5.3.1. *The separable degree of a field extension E/F is the number of field embeddings $E \hookrightarrow \overline{F}$ fixing F.*

Lemma 5.3.2. *All roots of an irreducible polynomial has same multiplicity.*

Proof. □

Theorem 5.3.3. *Let K be an intermediate field of a finite extension E/F. Then,*

$$[E : F]_{\text{sep}} \mid [E : F]$$

Proof. □

Theorem 5.3.4. *A finite field extension E/F is separable if and only if*

$$[E : F]_{\text{sep}} = [E : F].$$

Proof. □

multiplcation formula

Chapter 6

Normal extensions

6.1 Automorphism group

6.2 Normal extensions

6.3 Galois correspondence

Part III

Abelian extensions

Chapter 7

Abelian extensions

7.1 Finite fields

Lemma 7.1.1 (Frobenius endomorphism)**.** *Let F be a field of characteristic p. Then, the map $\sigma : x \mapsto x^p$ is a field endomorphism on F.*

Theorem 7.1.2. *Let L denote an algebraically closed field of characteristic $p > 0$. In L, the set of all finite subfields is described as a totally ordered set*

$$\{\mathbb{F}_p, \mathbb{F}_{p^2}, \mathbb{F}_{p^3}, \cdots\},$$

where $\mathbb{F}_q$ denotes a field of order q.

Proof. Step 1: Non-existence. The identity 1 is contained in every finite subfield of L, so is the field $\mathbb{F}_p$, hence the finite dimensional vector space over $\mathbb{F}_p$. Thus, the order of a finite field of characteristic p is a power of p.

Step 2: Existence. Let $q = p^n$ for $n \in \mathbb{Z}_{>0}$. Consider the set F of roots of the polynomial

$$f(x) = x^q - x$$

in L. We claim that F forms a field, the splitting field of f.

Clearly F is nonempty: $0 \in F$. Let $\alpha, \beta \in F$. Since $\sigma^n : x \mapsto x^q$ gives a field homomorphism, we have

$$(\alpha - \beta)^q = \alpha^q - \beta^q = (\alpha - \beta)$$

and

$$(\alpha\beta)^q = (\alpha\beta).$$

Also, we have $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$ if we define $\alpha^{-1} := \alpha^{q-2}$ for nonzero $\alpha \in F$. Therefore, F is a field.

Step 3: Uniqueness. Let F be a finite subfield of L of order q. Then, every nonzero element $\alpha \in F$ satisfies $\alpha^{q-1} = 1$ since q is contained in a group $\mathbb{F}^\times$ of order $q-1$, and it implies α satisfies $x^q - x = 0$ for all $\alpha \in F$. Since the number of roots of $x^q - x = 0$ is less or equal than q, we can conclude every finite subfield of L is characterized as the splitting field of a polynomial of the form $x^q - x$. □

Theorem 7.1.3. *The multiplicative group of $\mathbb{F}_{p^n}^\times$ is cyclic.*

Proof. The group $\mathbb{F}_{p^n}^\times$ is characterized by

$$\mathbb{F}_{p^n}^\times = \{\, x \in \overline{\mathbb{F}}_p : x^{p^n-1} = 1 \,\}.$$

We will count the number of elements of each order. Let y be any element of $\mathbb{F}_{p^n}^\times$ of order d. Then,

$$d = |\langle y \rangle| \leq |\{x : x^d = 1\}| \leq d$$

implies the subgroup $\{x : x^d = 1\}$ is cyclic with a generator y. Thus, the number of elements of order d is given by either 0 or the Euler totient $\phi(d)$.

Suppose there is no elements of order $p^n - 1$. Then,

$$p^n - 1 = |\mathbb{F}_{p^n}^\times| \leq \sum_{\substack{d \,|\, p^n-1 \\ d \neq p^n-1}} \phi(d) < \sum_{d \,|\, p^n-1} \phi(d) = p^n - 1$$

leads a contradiction. □

Theorem 7.1.4. *The Galois group* $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ *is cyclic.*

7.2 Cyclic extensions

7.3 Cyclotomic extensions

7.4 Kummer theory

Part IV

Insolvability of quintics

Chapter 8

Galois groups of polynomials

Chapter 9

Radical extensions

Chapter 10

Computational strategies

- reducible case, irreducible<=>transitivity
- resolvent polynomial1: discriminant
- resolvent polynomial2: cubic resolvent
- double quadratic, reciprocal equation: finding symmetry
- number of imaginary roots=2n: composition of n transpositions
- radiacal extension : Jacobson-Velez,
- semidirect product
- reduction modulo p (over $\mathbb{F}_p$)

10.1 Quartic

In this section, we assume the following setting:

- F is a perfect field,
- f is an irreducible quartic over F,
- E is the splitting of f over F,
- $G = \mathrm{Gal}(E/F)$,
- $H = G \cap V_4$.

Theorem 10.1.1. *There are only five isomorphic types of transitive subgroups of the symmetric group S_4.*

Corollary 10.1.2. $G \cong S_4,\ A_4,\ D_4,\ V_4,\ or\ C_4$.

Proposition 10.1.3. *Two groups A_4 and V_4 are only transitive normal subgroups of S_4.*

Now we define our resolvent polynomial.

Proposition 10.1.4. *Let K be the fixed field of H. Then,*

$$K = F(\alpha_1\alpha_2 + \alpha_3\alpha_4,\ \alpha_1\alpha_3 + \alpha_2\alpha_4,\ \alpha_1\alpha_4 + \alpha_2\alpha_3).$$

Definition 10.1.1. Let K be the fixed field of H. A *resolvent cubic* is a cubic R_3 that has K as the splitting field over F.

Theorem 10.1.5. *We have*

(a) $G \cong S_4$ *if* R_3 *is irreducible and ,*

(b) $G \cong A_4$ *if* R_3 *is irreducible and ,*

(c) $G \cong D_4$ *if* R_3 *has only one root in* K *and* f *is irreducible over* K*,*

(d) $G \cong C_4$ *if* R_3 *has only one root in* K *and* f *is reducible over* K*,*

(e) $G \cong V_4$ *if* R_3 *splits in* K.

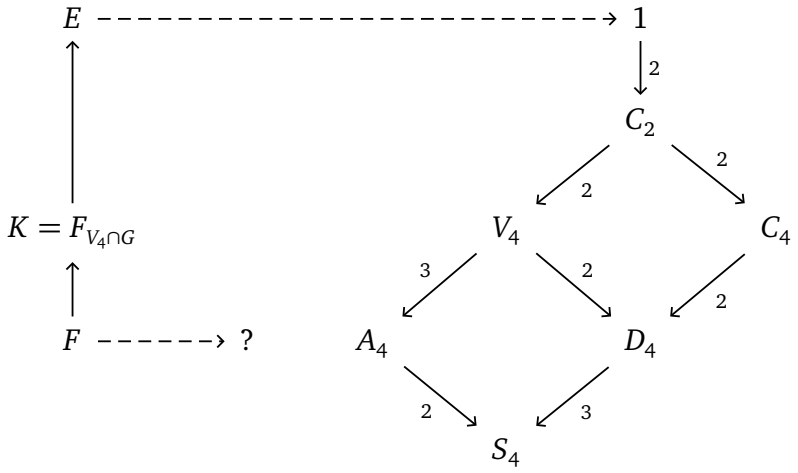
Proof. There are five possible cases:

$$(G,H) = (S_4,V_4),\ (A_4,V_4),\ (D_4,V_4),\ (V_4,V_4),\ (C_4,C_2).$$

We have

$$[K:F] = |G/H|, \qquad [E:K] = |H|.$$

If f is reducible over K, then $\mathrm{Gal}(E/K)$ is no more a transitive subgroup of S_4 so that $H \neq V_4$ and $G \cong C_4$. □


E
1
2
C_2
2
2
K = F_{V_4∩G}
V_4
C_4
3
2
2
F
?
A_4
D_4
2
3
S_4