7 Galois Extensions

Last Updated: 2026–03–02

This chapter develops the main results in Galois theory.

7.0 Galois Extensions

Which fields are characterized by normality and separability?

7.0.0 Definition. Let $K \subseteq L$ be a finite field extension with Galois group $\mathrm{Gal}(L/K)$. For every subgroup $H \subseteq \mathrm{Gal}(L/K)$, the subset

$$L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$$

is the *fixed field of* H.

We first justify this terminology.

7.0.1 Lemma. *Let $K \subseteq L$ be a finite field extension with Galois group $\mathrm{Gal}(L/K)$. The subset $L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha$ for all $\sigma \in H\}$ is a subfield of L containing K.*

Proof. Consider $\alpha, \beta \in L^H$. For each $\sigma \in H$, the properties of a ring homomorphism and the definition of L^H give

$$\sigma(\alpha - \beta) = \sigma(\alpha) - \sigma(\beta) = \alpha - \beta\,, \qquad \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta\,,$$

and $1 = \sigma(1)$, so L^H is a subring. The definition of $\mathrm{Gal}(L/K)$ implies that every automorphism in H restricts to the identity on K, which implies that $K \subseteq L^H$. Since we also have

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

the uniqueness of multiplicative inverses gives $\sigma(\alpha^{-1}) = \alpha^{-1}$. We conclude that L^H is a subfield. □

7.0.2 Theorem. *For every finite field extension $K \subseteq L$, the following are equivalent:*

(splitting) *The field L is the splitting field of a separable $f \in K[x]$.*
(fixed) *The field K is the fixed field of $\mathrm{Gal}(L/K)$ acting on L.*
(normal) *The inclusion $K \subset L$ is a normal separable extension.*

Proof.

(splitting) ⇒ (fixed): Suppose that M is the fixed field of $\mathrm{Gal}(L/K)$. We claim that $K = M$. Since L is the splitting field of a separable $f \in K[x]$, the same is true over the field M because $f \in M[x]$. It follows that $[L : K] = |\mathrm{Gal}(L/K)|$ and $[L : M] = |\mathrm{Gal}(L/M)|$. We have $\mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/M)$, because an automorphism of L that restricts to the identity on M also restricts to the identity on K. The reverse inclusion holds because the definition of M implies that every $\sigma \in \mathrm{Gal}(L/K)$ is the identity on M. We deduce that $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/M)$ and $[L : K] = [L : M]$. The Tower Theorem gives $[L : K] = [L : M][M : K]$, so $[M : L] = 1$ and $M = K$.

(fixed) ⇒ (normal): Suppose that K is the fixed field of $\mathrm{Gal}(L/K)$ and consider $\alpha \in L$. Let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_n$ be the distinct elements of L obtained by applying the elements of $\mathrm{Gal}(L/K)$ to α. Set

$$h := \prod_{j=1}^{n} (x - \alpha_j) \in L[x] .$$

We claim that $h \in K[x]$. To that end, we show that $\sigma \in \mathrm{Gal}(L/K)$ permutes that α_j. By definition, $\alpha_j := \tau(\alpha)$ for some $\tau \in \mathrm{Gal}(L/K)$. It follows that $\sigma(\alpha_j) = \sigma(\tau(\alpha_j)) = (\sigma \circ \tau)(\alpha)$ which is α_k for some k. Hence, σ maps $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ to itself, which gives a permutation because σ is injective. Since σ permutes the α_j, it also permutes the factors $x - \alpha_j$ of h. This shows that the coefficients of h are fixed by $\mathrm{Gal}(L/K)$ and hence lie in the fixed field, which is K by assumption. We deduce that $h \in K[x]$.

We next claim that h irreducible over K. Let $g \in K[x]$ be the irreducible factor of h that vanishes at α. It follows that $\sigma(\alpha)$ is also a root of g for all $\sigma \in \mathrm{Gal}(L/K)$. As the α_j are the distinct elements of L obtained this way, the product h divides g. Hence, h is irreducible over K because g is an irreducible factor of h.

We conclude that $h \in K[x]$ is the minimal polynomial of α over K. The defining formula for h also show that h is separable and splits completely over L. If $f \in K[x]$ is irreducible and has a root $\alpha \in L$, then f is the polynomial h (up to a constant factor). Thus, f splits completely over L, which proves normality. Similarly, if $\alpha \in L$, then its minimal polynomial is h. It follows that α is separable over K because h is, which proves separability.

(normal) $\Rightarrow$ *(splitting)*: Suppose that $K \subseteq L$ is normal and separable. We have $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ where the minimal polynomial p_j of α_j over K is separable. Let $q_1, q_2, \dots, q_r$ be the distinct elements of the set $\{p_1, p_2, \dots, p_n\}$ and set $f = q_1 q_2 \cdots q_r$. It follows that f is separable, and L is the splitting field of f over K. □

7.0.3 Definition. A field extension $K \subseteq L$ is a *Galois extension* if it is finite and satisfies the equivalent conditions in Theorem 7.0.2.

7.0.4 Remark. The field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois, because $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$. In contrast, the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is not Galois, because the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$ does not split completely over $\mathbb{Q}(\sqrt[3]{2})$.

7.0.5 Proposition. *For every Galois extension $K \subseteq L$ and every intermediate field $K \subseteq M \subseteq L$, the upper field extension $M \subseteq L$ is Galois.*

Proof. When $K \subseteq L$ is Galois, the field L is the splitting field of a separable $f \in K[x]$. By regarding f as an element of $M[x]$, it follows immediately that the same is true over the large field M. □

The lower field extension $K \subset M$ need not be Galois.

7.0.6 Remark. The field $\mathbb{Q}(\mathrm{i}, \sqrt[4]{2})$ is the splitting field of $x^4 - 2$ and thereby Galois. The intermediate field $\mathbb{Q}(\mathrm{i})$, as the splitting field of $x^2 + 1$, is Galois over $\mathbb{Q}$. In contrast, the $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ is not, because the irreducible $x^4 - 2$ does not split completely.

7.1 Galois Closure

What is the smallest extension that is Galois?

7.1.0 Theorem. *For every finite extension $K \subseteq L$, we have*

(divisibility) *The order* $|\mathrm{Gal}(L/K)|$ *divides* $[L : K]$.

(inequality) $|\mathrm{Gal}(L/K)| \leqslant [L : K]$

(characterization) $K \subseteq L$ *is Galois if and only if* $|\mathrm{Gal}(L/K)| = [L : K]$.

Proof. Let M be the fixed field of the Galois group $\mathrm{Gal}(L/K)$. Hence, we have $K \subseteq M \subseteq L$ and the proof of the first part of Theorem 7.0.2 implies that $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/K)$. In particular, the intermediate field M is also the fixed field of $\mathrm{Gal}(L/M)$, so $M \subseteq L$ is a Galois extension by Proposition 7.0.5. The Tower Theorem gives

$$[L : K] = [L : M][M : K] = |\mathrm{Gal}(L/M)|\,[M : K] = |\mathrm{Gal}(L/K)|\,[M : K]\,.$$

Thus, the order of $\mathrm{Gal}(L/K)$ divides $[L : K]$.

The second part follows immediately from the first part.

Theorem 6.1.0 proves one implication. For the converse, suppose that $K \subseteq L$ is a finite extension with $|\mathrm{Gal}(L/K)| = [L : K]$, and let M be the fixed field of $\mathrm{Gal}(L/K)$. It suffices to prove that $K = M$. The proof of the first part implies that $M \subseteq L$ is a Galois extension and $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/K)$. It follows that

$$[L : K] = |\mathrm{Gal}(L/K)| = |\mathrm{Gal}(L/M)| = [L : M]\,.$$

The Tower Theorem gives $[L : K] = [L : M][M : K]$, so $[M : L] = 1$ and $M = K$. □

Galois extensions lead to a characterization of finite separable extensions.

7.1.1 Proposition. *Let $K \subseteq L$ be a finite field extension. The field L is separable over K if and only if $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where each α_j is separable over K.*

Proof. Suppose that finite field extension $K \subseteq L$ is separable. The finite hypothesis implies that there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, each algebraic and separable over K, such that $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Conversely, suppose that $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where each α_j is separable over K. We claim that L can be embedded into a larger field that is separable over K. For all $1 \leqslant j \leqslant n$, let p_j denote the minimal polynomial of α_j over K, and let $q_1, q_2, \ldots, q_r$ be the distinct elements of the set $\{p_1, p_2, \ldots, p_n\}$. Applying Lemma 5.1.6, we see that $f = q_1 q_2 \cdots q_r$ is separable, since each q_j is. Writing M for the splitting field of f, regarded as a polynomial in $L[x]$, we have $M = L(\beta_1, \beta_2, \ldots, \beta_m)$ where $\beta_1, \beta_2, \ldots, \beta_m$ are the roots of f.

We next claim that $M = K(\beta_1, \beta_2, \ldots, \beta_m)$. The inclusion

$$K(\beta_1, \beta_2, \ldots, \beta_m) \subseteq L(\beta_1, \beta_2, \ldots, \beta_m) = M$$

is trivial. Observe that the roots $\beta_1, \beta_2, \ldots, \beta_m$ include the elements $\alpha_1, \alpha_2, \ldots, \alpha_n$, so that $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K(\beta_1, \beta_2, \ldots, \beta_m)$. Thus,

the field $K(\beta_1, \beta_2, \dots, \beta_m)$ contains both L and $\beta_1, \beta_2, \dots, \beta_m$ which gives the inclusion

$$M = L(\beta_1, \beta_2, \dots, \beta_m) \subseteq K(\beta_1, \beta_2, \dots, \beta_m).$$

Thus, we deduce that $M = K(\beta_1, \beta_2, \dots, \beta_m)$.

In other words, M is the splitting field over K of the separable polynomial f. Hence, the field extension $K \subseteq M$ is Galois and thereby separable by Theorem 7.0.2. Since $L \subseteq M$, every element of L is separable over K, so that $K \subseteq L$ is separable. □

Building on the strategy of embedding a field into a larger Galois extension is unexpectedly fruitful.

7.1.2 Proposition. *For every finite separable field extension $K \subseteq L$, there exists a field extension $L \subseteq M$ such that*

(Galois) *M is Galois over K, and*

(minimal) *for any other field extension $L \subseteq M'$ such that M' is Galois over K, there is a field homomorphism $\varphi\colon M \to M'$ that is the identity on L.*

Proof. Since the field extension $K \subseteq L$ is a finite and separable, there exist elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$, each separable over K, such that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Following the proof of Proposition 7.1.1, there exists a field extension $L \subseteq M$ such that M is a splitting field over L of a separable $f = q_1 q_2 \cdots q_r \in K[x]$ where $q_1, q_2, \dots, q_r$ are the distinct elements among the minimal polynomials over K for the elements $\alpha_1, \alpha_2, \dots, \alpha_n$. As in the proof of Proposition 7.1.1, the field extension $K \subseteq M$ is Galois.

To show that $L \subseteq M$ satisfies the minimality condition, let $L \subseteq M'$ be a field extension where M' is Galois over K. By Theorem 7.0.2, the field extension $L \subseteq M'$ is normal, so the minimal polynomial of α_j splits completely over M'. It follows that f splits completely in M'. Let $M'' \subseteq M'$ be the subfield obtained by adjoining the roots of f to K. Since $\alpha_j \in L \subseteq M'$ is a root of f, we have $L \subseteq M''$. Thus, we can regard M'' as a splitting field of f over L. The uniqueness of splitting fields produces an isomorphism $\varphi\colon M \to M''$ that is the identity on L. Since $M'' \subseteq M'$, we can regard φ as a field homomorphism $\varphi\colon M \to M'$. □

7.1.3 Definition. The field constructed in Proposition 7.1.2 is called the *Galois closure* of L over K.

7.1.4 Problem. Prove that the field $\mathbb{Q}(\omega, \sqrt[3]{2})$ is the Galois closure of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.

Solution. Set $\alpha := \sqrt[3]{2}$. Since $x^3 - 2 = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$, the splitting field for the irreducible $x^3 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\omega, \alpha)$. Moreover, any splitting field must contain both α and ω. Because the field $\mathbb{Q}(\omega, \alpha)$ contains $\mathbb{Q}(\alpha)$, is Galois over $\mathbb{Q}$, and is the splitting field of the minimal polynomial of α over $\mathbb{Q}$, it follows that this field is the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. □

7.2 Conjugate Fields

How are normal subgroups related to normal field extensions?

7.2.0 Definition. Let $K \subseteq L$ be a finite field extension. For every intermediate field $K \subseteq M \subseteq L$ and each $\sigma \in \mathrm{Gal}(L/K)$, the subset $\sigma(M) := \{\sigma(\alpha) \in L \mid \alpha \in M\}$ is a *conjugate field of* M.

The image $\sigma(M)$ is a subfield of L because σ is a field automorphism.

7.2.1 Lemma. *The conjugate field $\sigma(M)$ is a subfield of L containing K, and $[M : K] = [\sigma(M) : K]$.*

Proof. Since $K \subseteq M$ and the map σ restricts to the identity on K, we have the inclusion $K \subseteq \sigma(M)$. For all $a \in K$ and all $\alpha \in M$, we also have $\sigma(a\alpha) = \sigma(a)\sigma(\alpha) = a\sigma(\alpha)$, so $\sigma|_M : K \to \sigma(K)$ is K-linear. Hence, $\sigma|_M$ is an isomorphism of K-vector spaces, which yields

$$[M : K] = \dim_K M = \dim_K \sigma(M) = [\sigma(M) : K]\,. \qquad \square$$

7.2.2 Remark. Consider $\mathbb{Q} \subset \mathbb{Q}(\omega, \alpha)$ where $\omega := \exp(2\pi\mathrm{i}/3)$ and $\alpha := \sqrt[3]{2}$. The intermediate fields are $\mathbb{Q}(\omega)$, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\omega\alpha)$, $\mathbb{Q}(\omega^2\alpha)$, and $\mathbb{Q}$. The map $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\omega, \alpha)/\mathbb{Q}\big)$ is uniquely determined by

$$\sigma(\omega) \in \{\omega, \omega^2\} \qquad \text{and} \qquad \sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}\,,$$

and all possible combinations actually occur. The conjugate fields of $\mathbb{Q}(\sqrt[3]{2})$ are $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$, $\mathbb{Q}(\omega^2\sqrt[3]{2})$, whereas $\mathbb{Q}(\omega)$ equals all of its conjugates.

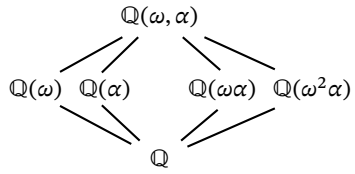

Figure 7.1: The Hasse diagram intermediate fields

7.2.3 Lemma. *Let $K \subseteq L$ be a finite field extension. For each intermediate field $K \subseteq M \subseteq L$, the group $\mathrm{Gal}(L/M)$ is a subgroup of $\mathrm{Gal}(L/K)$. For all $\sigma \in \mathrm{Gal}(L/K)$, we also have $\mathrm{Gal}\big(L/\sigma(M)\big) = \sigma\,\mathrm{Gal}(L/M)\,\sigma^{-1}$.*

Proof. Each map $\sigma \in \mathrm{Gal}(L/M)$ is an automorphism of L that is the identity on M. Since $K \subseteq M$, it follows that $\sigma \in \mathrm{Gal}(L/K)$, so we have the inclusion $\mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/K)$. Since both are groups under composition, we conclude that $\mathrm{Gal}(L/K)$ is a subgroup.

For the second part, let $\rho \in \sigma\,\mathrm{Gal}(L/M)\,\sigma^{-1}$ and $\beta \in \sigma(M)$. By definition, there exists $\tau \in \mathrm{Gal}(L/M)$ such that $\rho = \sigma \circ \tau \circ \sigma^{-1}$, and $\beta = \sigma(\alpha)$ for some $\alpha \in M$. It follows that

$$\rho(\beta) = (\sigma \circ \tau \circ \sigma^{-1})(\sigma(\alpha)) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \beta\,.$$

Thus, ρ is the identity on $\sigma(M)$ and $\sigma\,\mathrm{Gal}(L/M)\,\sigma^{-1} \subseteq \mathrm{Gal}\big(L/\sigma(M)\big)$. Conversely, for every $\tau' \in \mathrm{Gal}\big(L/\sigma(M)\big)$, it follows that

$$(\sigma^{-1} \circ \tau' \circ \sigma)(\alpha) = \sigma^{-1}(\tau'(\beta)) = \sigma^{-1}(\beta) = \alpha\,,$$

so we see that $\sigma^{-1} \circ \tau' \circ \sigma$ is the identity on M. We conclude that $\mathrm{Gal}\big(L/\sigma(M)\big) = \sigma\,\mathrm{Gal}(L/M)\,\sigma^{-1}$. $\square$

7.2.4 Theorem. *Let $K \subseteq M \subseteq L$ be finite field extensions. When $K \subseteq L$ is a Galois extension, the following are equivalent:*

(conjugate) *$M = \sigma(M)$ for all $\sigma \in \mathrm{Gal}(L/K)$.*
(subgroup) *$\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$.*
(Galois) *The field extension $K \subseteq M$ is Galois.*
(normal) *The field extension $K \subseteq M$ is normal.*

Proof. We establish three distinct equivalences.

(conjugate) ⇔ (subgroup): Suppose that the intermediate field M is equal to all its conjugate fields. For all $\sigma \in \mathrm{Gal}(L/K)$, Lemma 7.2.3 shows that $\mathrm{Gal}(L/M) = \mathrm{Gal}\big(L/\sigma(M)\big) = \sigma\,\mathrm{Gal}(L/M)\,\sigma^{-1}$. Since σ was an arbitrary element of the ambient group $\mathrm{Gal}(L/K)$, the subgroup $\mathrm{Gal}(L/M)$ is normal.

Suppose that $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. For all $\sigma \in \mathrm{Gal}(L/K)$, Lemma 7.2.3 implies that

$$\mathrm{Gal}(L/M) = \sigma\,\mathrm{Gal}(L/M)\,\sigma^{-1} = \mathrm{Gal}\big(L/\sigma(M)\big)\,.$$

Since $M \subseteq L$ and $\sigma(M) \subseteq L$ are Galois extensions, Theorem 7.0.2 shows that the intermediate field M is the fixed field of $\mathrm{Gal}(L/M)$ and the conjugate field $\sigma(M)$ is the fixed field of $\mathrm{Gal}\big(L/\sigma(M)\big)$. We deduce that $M = \sigma(M)$.

(Galois) ⇔ (normal): Since every Galois extension is normal and separable, the forward implication follows. Conversely, since $K \subseteq L$ is Galois, it also separable and every intermediate filed is also separable. When M is normal over K, this field extension is normal and separable and hence Galois.

(conjugate) ⇔ (normal): Suppose that the field M is equal to all its conjugate fields. Let $f \in K[x]$ be an irreducible polynomial over K with a root $\alpha \in M$. It suffices to show that f splits completely over K. The proof of Theorem 7.0.2 shows that, up to a constant, f is the polynomial

$$h := \prod_{j=1}^{n} (x - \alpha_j)$$

where $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ are the distinct elements of L obtained by applying the elements of $\mathrm{Gal}(L/K)$ to α. Since $\alpha \in M$, each α_i lies in a conjugate field of K. It follows that $\alpha_j \in K$ for all j, so h and f split completely over M.

Lastly, suppose that $K \subseteq M$ is a normal extension. Consider $\alpha \in M$ and $\sigma \in \mathrm{Gal}(L/K)$. Let p be the minimal polynomial of α over K. The image $\sigma(\alpha)$ is also a root of p. Since $K \subseteq M$ is normal, the polynomial p splits completely over M, which implies that $\sigma(\alpha) \in M$ and $\sigma(M) \subseteq M$. Since $[M : K] = [\sigma(M) : K]$, we conclude that $\sigma(M) = M$. □

7.2.5 Remark. Consider $\mathbb{Q} \subset L := \mathbb{Q}(\omega, \alpha)$ where $\omega := \exp(2\pi\mathrm{i}/3)$ and $\alpha := \sqrt[3]{2}$. There are automorphisms $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that

$$\sigma(\omega) = \omega\,, \qquad \sigma(\alpha) = \omega\alpha\,, \qquad \tau(\omega) = \omega^2\,, \qquad \tau(\alpha) = \alpha\,.$$

and $\langle \sigma, \tau \rangle = \mathrm{Gal}(L/\mathbb{Q})$. The intermediate field M corresponds to the subgroup $\mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/\mathbb{Q})$. In particular, we have

$$\begin{aligned} L &\mapsto \{\mathrm{id}_L\}, & \mathbb{Q}(\omega) &\mapsto \langle \sigma \rangle\,, & \mathbb{Q}(\alpha) &\mapsto \langle \tau \rangle\,, \\ \mathbb{Q}(\omega\alpha) &\mapsto \langle \sigma^2 \circ \tau \rangle\,, & \mathbb{Q}(\omega^2\alpha) &\mapsto \langle \sigma \circ \tau \rangle\,, & \mathbb{Q} &\mapsto \langle \sigma, \tau \rangle\,. \end{aligned}$$

The subgroup $\mathrm{Gal}\big(L/\mathbb{Q}(\omega)\big) = \langle \sigma \rangle$ is normal, and

$$|\mathrm{Gal}\big(L/\mathbb{Q}(\omega)\big)| = [L : \mathbb{Q}(\omega)] = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\omega) : \mathbb{Q}]} = \frac{6}{2} = 3\,.$$

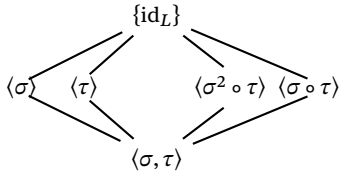

Figure 7.2: The Hasse diagram subgroups