Galois Theory notes

arnaucube

2025

Abstract

Notes taken while studying Galois Theory, mostly from Ian Stewart's book "Galois Theory" [1].

Usually while reading books and papers I take handwritten notes in a notebook, this document contains some of them re-written to $LaTeX$.

The notes are not complete, don't include all the steps neither all the proofs.

Contents

1 Galois Theory notes

1.1 Chapters 4-12

(Definitions, theorems, lemmas, corollaries and examples enumeration follows from Ian Stewart's book [1]).

Definition 4.10. A *simple extension* is $L : K$ such that $L = K(\alpha)$ for some $\alpha \in L$.

Example 4.11. Beware, $L = \mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) = \mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(i + \sqrt{5})$.

Definition 5.5 (Minimal polynomial)**.** Let $L : K$, suppose $\alpha \in L$ is algebraic over K. Then, the *minimal polynomial* of α over K is the unique monic polynomial m over K, $m(t) \in K[t]$, of smallest degree such that $m(\alpha) = 0$.
eg.: $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$. The minimal polynomial of i over $\mathbb{R}$ is $m(t) = t^2 + 1$, so that $m(i) = 0$.

Lemma 5.9. Every polynomial $a \in K[t]$ is congruent modulo m to a unique polynomial of degree $< \delta m$.

Proof. Divide a/m with remainder, $a = qm + r$, with $q, r \in K[t]$ and $\delta r < \delta m$. Then, $a - r = qm$, so $a \equiv r \pmod{m}$.

It remains to prove uniqueness.

Suppose $\exists\ r \equiv s \pmod{m}$, with $\delta r, \delta s < \delta m$. Then, $r - s$ is divisible by m, but has smaller degree than m.

Therefore, $r - s = 0$, so $r = s$, proving uniqueness. □

Theorem 5.10. $\forall 0 \neq f \in \frac{K[t]}{<m>}$, $\exists f^{-1}$ iff m is irreducible in $K[t]$.
Then $\frac{K[t]}{<m>}$ is a field.

Theorem 5.12. Let $K(\alpha) : K$ simple algebraic extension, let m minimal polynomial of α over K.
$K(\alpha) : K$ is isomorphic to $\frac{K[t]}{<m>}$.
The isomorphism $\frac{K[t]}{<m>} \longrightarrow K(\alpha)$ can be chosen to map t to α.

Corollary 5.13. Let $K(\alpha) : K$ and $K(\beta) : K$ be simple algebraic extensions.
If α, β have same minimal polynomial m over K, then the two extensions are isomorphic, and the isomorphism of the larger fields map α to β.

Proof. By 5.12, both extensions are isomorphic to $\frac{K[t]}{<m>}$. □

Lemma 5.14. Let $K(\alpha) : K$ be a simple algebraic extension, let m be the minimal polynomial of α over K, let $\delta m = n$.

Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K. In particular, $[K(\alpha) : K] = n$.

Definition 6.2. The degree $[L : K]$ of a field extension $L : K$ is the dimension of L considered as a vector space over K.

Equivalently, the dimension of L as a vector space over K is the number of terms in the expression for a general element of L using coefficients from K.

Example 6.3. 1. $\mathbb{C}$ elements are 2-dimensional over $\mathbb{R}$ ($p + qi \in \mathbb{C}$, with $p, q \in \mathbb{R}$), because a basis is $\{1, i\}$, hence $[\mathbb{C} : \mathbb{R}] = 2$.

2. $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}] = 4$, since the elements $\{1, \sqrt{5}, i, i\sqrt{5}\}$ form a basis for $\mathbb{Q}(i, \sqrt{5})$ over $\mathbb{Q}$.

Theorem 6.4. *(Short Tower Law)* If $K, L, M \subseteq \mathbb{C}$, and $K \subseteq L \subseteq M$, then $[M : K] = [M : L] \cdot [L : K]$.

Proof. Let $(x_i)_{i\in I}$ be a basis for L over K, let $(y_j)_{j\in J}$ be a basis for M over L.
$\forall i \in I, j \in J$, we have $x_i \in L, u_j \in M$.
Want to show that $(x_i y_j)_{i\in I, j\in J}$ is a basis for M over K.

i. prove linear independence:
Suppose that
$$\sum_{ij} k_{ij} x_i y_j = 0 \ (k_{ij} \in K)$$
rearrange
$$\sum_j (\underbrace{\sum_i k_{ij} x_i}_{\in L}) y_j = 0 \ (k_{ij} \in K)$$
Since $\sum_i k_{ij} x_i \in L$, and the $y_j \in M$ are linearly independent over L, then $\sum_i k_{ij} x_i = 0$.
Repeating the argument inside $L \longrightarrow k_{ij} = 0 \ \ \forall i \in I, j \in J$.
So the elements $x_i y_j$ are linearly independent over K.

ii. prove that $x_i y_j$ span M over K:
Any $x \in M$ can be written
$$x = \sum_j \lambda_j y_j$$
for $\lambda_j \in L$, because y_j spans M over L. Similarly,
$$\forall j \in J, \ \lambda_j = \sum_i \lambda_{ij} x_i y_j$$
for $\lambda_{ij} \in K$.
Putting the pieces together,
$$x = \sum_{ij} \lambda_{ij} x_i y_j$$
as required.

□

Corollary 6.6. *(Tower Law)*
If $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ are subfields of $\mathbb{C}$, then
$$[K_n : K_0] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \ldots \cdot [K_1 : K_0]$$

Proof. From 6.4. □

Theorem 6.7. if $K(\alpha) : K$

- transcendental $\implies \quad [K(\alpha) : K] = \inf$
- algebraic $\implies \quad [K(\alpha) : K] = \delta m$

(where m is the minimal polynomial of α over K).

Definition 8.1. $L : K$, a K-*automorphism* of L is an automorphism α of L such that $\alpha(k) = k \ \ \forall k \in K$.
ie. α *fixes* k.

Theorem 8.2, 8.3. The set of all K-automorphisms of L forms a group, $\Gamma(L : K)$, the Galois group of $L : K$.

Definition 8.12. (Radical Extension) $L : K$ is radical if $L = K(\alpha_1, \ldots, \alpha_m)$ where for each $j = 1, \ldots, m$, $\exists\ n_j$ such that $\alpha_j^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1}) \ \ (j \geq 1)$

Lemma 8.18. Let $q \in L$. The minimal polynomial of q over K *splits* into linear factors over L.

Exercise E.8.7. TODO

Definition 9.1. For $K \subseteq \mathbb{C}$, and $f \in K[t]$, f *splits* over K if it can be expressed as a product of linear factors

$$f(t) = k \cdot (t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n)$$

where $k, \alpha_i \in K$.
$\implies$ (Thm 9.3) if f splits over Σ, Σ is the *splitting field.*
If $K \subseteq \Sigma' \subseteq \Sigma$ and f splits over Σ', then $\Sigma' = \Sigma$.

Theorem 9.6. TODO

Definition 9.8. $L : K$ is *normal* if every irreducible polynomial $f \in K[t]$ that has at least one zero in L, splits in L.

Theorem 9.9. TODO

Theorem 9.10. An irreducible polynomial $f \in K[t]$ $(K \subseteq \mathbb{C})$ is *separable over* K if it has simple zeros in $\mathbb{C}$, or equivalently, simple zeros in its splitting field.

Lemma 9.13. $f \in K[t]$ with splitting field Σ. f has multiple zeros (in Σ or $\mathbb{C}$) iff f and Df have a common factor of degree ≥ 1 in $\Sigma[t]$.
More details at Rolle's theorem (2.7) section.

Theorem 10.5. $|\Gamma(K : K_0)| = [K : K_0]$, where K_0 is the fixed field of $\Gamma(K : K_0)$.

Definition 11.1. $K \subseteq L$, $K \subseteq L$. A K-monomorphism of M into L is a field monomorphism

$$\phi : M \longrightarrow L$$

such that $\phi(k) = k \ \ \forall k \in K$.

Theorem 11.3. $L : K$ normal, $K \subseteq M \subseteq L$. Let τ any K-monomorphism $\tau : M \longrightarrow L$.
Then, $\exists$ a K-automorphism σ of L such that $\sigma\Big|_M = \tau$.

Proof. $L : K$ normal $\Longrightarrow$ by Thm 9.9, L splitting field for some poly $f \in K[t]$.

Hence, L is splitting field over M for f and over $\tau(M)$ for $\tau(f)$.

Since $\tau\Big|_K$ is the identity, $\tau(f) = f$.

We have

$$\begin{array}{ccc} M & \longrightarrow & L \\ \downarrow \tau & & \downarrow \\ \tau(M) & \longrightarrow & L \end{array}$$

with σ yet to be formed.

By Theorem 9.6, $\exists$ isomorphism $\sigma : L \longrightarrow L$ such that $\sigma\Big|_M = \tau$.

Therefore, σ is an automorphism of L, and since $\sigma\Big|_K = \tau\Big|_K = id$, σ is a K-automorphism of L. $\square$

Proposition 11.4. $L : K$ finite normal, $\alpha,\ \beta$ are zeros in L of the irreducible polynomial $p \in K[t]$.

Then, $\exists$ a K-automorphism σ of L such that $\sigma(\alpha) = \beta$.

Proof. By Corollary 5.13, $\exists$ isomorphism $\tau : K(\alpha) \longrightarrow K(\beta)$ such that $\tau\Big|_K$ is the identity, and $\tau(\alpha) = \beta$.

By Theorem 11.3, τ extends to a K-automorphism σ of L. $\square$

Lemma 11.8. $K \subseteq L \subseteq N \subseteq M$, $L : K$ finite, N normal closure of $L : K$.
Let τ any K-monomorphism $\tau : L \longrightarrow M$.
Then $\tau(L) \subseteq N$.

Proof. $\alpha \in L$, m minimal polynomial of α over K.
$\Longrightarrow \quad m(\alpha) = 0$, so $\tau(m(\alpha)) = 0$

(since τ is a K-automorphism, ie. maps the zeros of $m(t)$).

Since τ is a K-monomorphism, $\tau(m(\alpha)) = m(\tau(\alpha)) = 0$

$\Longrightarrow \quad \tau(\alpha)$ is a zero of m.

Therefore, $\tau(\alpha)$ lies in N, since $N : K$ is normal.
Henceforth, $\tau(L) \subseteq N$. $\square$

Theorem 11.9. The following are equivalent:

1. $L : K$ normal
2. $\exists$ finite normal extension N of K containing L,
   such that every K-monomorphism $\tau : L \longrightarrow N$ is a K-automorphism of L.
3. for every finite extension M of K containing L,
   every K-monomorphism $\tau : L \longrightarrow M$ is a K-automorphism of L.

Theorem 11.10. $[L : N] = 1$, N normal closure of $L : K$. Then,
$\exists$ n K-monomorphisms $L \longrightarrow N$.
(the ones proven by Lemma 11.8).

Corollary 11.11. $|\Gamma(L : K)| = [L : K]$ (if $L : K$ is normal).
ie. there are precisely $[L : K]$ distinct K-automorphisms of L.

Theorem 11.12. $\Gamma(L : K) = G$. If $L : K$ normal, then K is the fixed field of G.

Proof. let K_0 be the fixed field of G. Let $[L : K] = n$.
By 11.11, $|G| = [L : K] = n$.
By 10.5, $[L : K_0] = n$ (K_0 fixed field).
Since $K \subseteq K_0$, we must have $K = K_0$.
$\implies$ thus K is the fixed field of G. $\square$

Theorem 11.14. if L any field, G any finite group of automorphisms of L, and K its fixed field,
then $L : K$ is *finite* and *normal*, with Galois group G.

Theorem 12.2. (Fundamental Theorem of Galois Theory) if $L : K$ finite and normal inside $\mathbb{C}$, with $\Gamma(L : K) = G$, then:

1. $|\Gamma(L : K)| = [L : K]$ (by Corollary 11.11)
2. the maps * and † are mutual inverses, and setup an order-reversing one-to-one correspondence between $\mathcal{F}$ and $\mathcal{G}$.
3. if M an intermediate field, then

$$[L : M] = |M^*| \qquad [M : K] = \frac{|G|}{|M^*|}$$

4. for M an intermediate field, $M : K$ normal iff

$$\underbrace{\Gamma(M : K)}_{=M^*} \lhd \underbrace{\Gamma(L : K)}_{=G}$$

5. for M intermediate, if $M : K$ normal, then

$$\Gamma(M : K) \cong \frac{G}{M^*}$$

ie.

$$\Gamma(M : K) \cong \frac{\Gamma(L : K)}{\Gamma(L : M)}$$

Proof. TODO ☐

1.2 Chapter 13 - Full example

(Chapter 13 is basically a full example. More examples can be found at section 3.1)

1.3 Detour: Isomorphism Theorems

Theorem i.1. (*First Isomorphism Theorem*)

If $\psi : G \longrightarrow H$ a group homomorphism, then $ker(\psi) \triangleleft G$. Let $\phi : G \longrightarrow G/ker(\psi)$ be the canonical homomorphism. Then $\exists$ unique isomorphism $\eta : G/ker(\psi) \longrightarrow \psi(G)$ such that $\psi = \eta\phi$.
$\Longleftrightarrow$ ie. $G/ker(\psi) \cong \psi(G)$.

$$\begin{tikzcd} G \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & H \\ & G/\ker(\psi) \arrow[ur, "\eta"'] & \end{tikzcd}$$

Proof. (proof from Thomas W. Judson book "Abstract Algebra" [5])

Let $K = ker(\psi)$. Since

$$\eta : G/K \longrightarrow \psi(G)$$

let

$$\eta : gK \longrightarrow \psi(g)$$

ie. $\eta(gK) = \psi(g)$.

i. show that η is a *well defined* map:

   if we have two representatives of the same coset, ie. $g_1K = g_2K$, we want to show that $\eta(g_1K) = \eta(g_2K)$, so that η is a well-defined map.

   By the coset properties for some $k \in K$, $g_1 = g_2k$, so

   $$\eta(g_1K) = \psi(g_1) = \psi(g_2k) = \eta(g_2kK) = \eta(g_2K)$$

   Thus, η does not depend on the choice of coset representatives, and the map $\eta : G/ker(\psi) \longrightarrow \psi(G)$ is uniquely defined since $\psi = \eta\phi$.

ii. show that η is a homomorphism:

Observe:

$$\eta(g_1Kg_2K) = \eta(g_1g_2K) = \psi(g_1g_2) = \psi(g_1)\psi(g_2) = \eta(g_1K)\eta(g_2K)$$

$\implies$ so η is a homomorphism.

iii. show that η is an isomorphism:

Since each element of $H = \psi(G)$ has at least a preimage, then η is *surjective* (onto $\psi(G)$).

Show that it is also *injective* (onet-to-one):

Suppose 2 different preimatges lead to the same image in $\psi(G)$, ie. $\eta(g_1K) = \eta(g_2K)$

then,

$$\psi(g_1) = \psi(g_2)$$

which implies $\psi(g_1^{-1}g_2) = e$, ie. $g_1^{-1}g_2 \in ker(\psi)$, hence

$$g_1^{-1}g_2K = K$$

$$g_1K = g_2K$$

so η is injective.

Since η is injective and surjective $\implies \eta$ is a bijective homomorphism, ie. η is an *isomorphism.* □

Theorem i.2. (*Second Isomorphism Theorem*) Let $H \subseteq G$, $N \triangleleft G$. Then

i. $HN \subseteq G$

ii. $H \cap N \triangleleft H$

iii. $\frac{H}{H\cap N} \cong \frac{HN}{N}$

Proof. (proof from Thomas W. Judson book "Abstract Algebra" [5])

i. show $HN \subseteq G$:
Note that $HN = \{hn : h \in H, n \in N\}$. Let $h_1n_1, h_2n_2 \in HN$.

Since N normal $\implies$ $h_2^{-1}n_1h_2 \in N$, so

$$(h_1n_1)(h_2n_2) = h_1h_2(h_2^{-1}n_1h_2) \cdot n_2 \in HN$$

[Recall: since $N \triangleleft G$, $gN = Ng$ $\forall g \in G \implies gn = n'g$ for some $n' \in N$.]

To see that $(hn)^{-1} \in HN$:
since $(hn)^{-1} = h^{-1}n^{-1} = h^{-1}(hn^{-1}h^{-1})$, thus $(hn)^{-1} \in HN$.

Thus $HN \subseteq G$.

In fact,

$$HN = \bigcup_{h \in H} hN$$

(TODO: diagram)

ii. show that $H \cap N \triangleleft H$:
Let $h \in H,\ n \in H \cap N$ (recall: $H \cap N \subseteq H$).
Then $h^{-1}nh \in H \longleftarrow$ since $h^{-1}, n, h \in H$.
Since $N \triangleleft G$, $h^{-1}nh \in N$.
Therefore, $h^{-1}nh \in H \cap N \implies H \cap N \triangleleft H$

iii. show that $\frac{H}{H \cap N} \cong \frac{HN}{N}$:
Define a map

$$\begin{aligned} \phi : & H \longrightarrow \frac{HN}{N} \\ \text{by } \phi : & h \longmapsto hN \end{aligned}$$

ϕ is surjective (onto), since any coset $hnN = hN$ is the image of $h \in H$, ie. $\phi(h)$

ϕ is a homomorphism, since

$$\phi(hh') = hh'N = hNh'N = \phi(h)\phi(h')$$

By the First Isomorphism Theorem i.1,

$$\frac{HN}{N} \cong \frac{H}{ker(\phi)}$$

and since

$$\begin{aligned} & ker(\phi) = \{h \in H : h \in N\} \\ & \text{then } \ ker(\phi) = H \cap N \end{aligned}$$

so then,

$$\frac{HN}{N} = \phi(H) \cong \frac{H}{ker(\phi)} = \frac{H}{H \cap N}$$

thus

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

□

Theorem i.3. (*Third Isomorphism Theorem*)
Let $H \subseteq K$ and $K \triangleleft G,\ H \triangleleft G$.
Then $\frac{K}{H} \triangleleft \frac{G}{H}$ and

$$\frac{G/H}{K/H} \cong \frac{G}{K}$$

Proof. *(proof from Dummit and Foote book "Abstract Algebra" [6])*

Easy to see that $\frac{K}{H} \triangleleft \frac{G}{H}$.
Define

$$\psi : \frac{G}{H} \longrightarrow \frac{G}{K}$$
$$\text{by } \psi : gH \longmapsto gK$$

To show that ψ is *well defined*:
suppose $g_1H = g_2H$, then $g_1 = g_2h$ for some $h \in H$.
Since $H \subseteq K \implies h \in K$, hence $g_1K = g_2K$,
ie. $\psi(g_1H) = \psi(g_2H)$, which shows that ψ is well defined.

Since $g \in G$ may be chosen arbitrarily in G, ψ is a surjective homomorphism.

Finally,

$$\begin{aligned} ker(\psi) &= \{gH \in \frac{G}{H} \mid \psi(gH) = 1K\} \\ &= \{gH \in \frac{G}{H} \mid gK = 1K\} \\ &= \{gH \in \frac{G}{H} \mid g \in K\} \\ &= \frac{K}{H} \end{aligned}$$

By the First Isomorphism Theorem (i.1),

$$\begin{tikzcd}
\frac{G}{H} \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & \frac{G}{K} \\
& \frac{G/H}{\ker(\psi)} = \frac{G/H}{K/H} \arrow[ur, "\eta"'] &
\end{tikzcd}$$

So, by

$$\eta : \frac{G/H}{K/H} \longrightarrow \frac{G}{K}$$

since η is bijective (we know it by the First Isomorphism Theorem), η it is the isomorphism:

$$\frac{G/H}{K/H} \cong \frac{G}{K}$$

$\square$

1.4 Chapter 14

Definition 14.1. a group G is soluble if it has a finite series of subgroups

$$1 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$$

such that

i. $G_i \lhd G_{i+1}$ for $i = 0, \ldots, n-1$

ii. $\frac{G_{i+1}}{G_{i+1}}$ is Abelian for for $i = 0, \ldots, n-1$

(Note: $G_i \lhd G_{i+1} \lhd G_{i+2}$ does not imply $G_i \lhd G_{i+2}$)

Theorem 14.4. $H \subseteq G$, $\quad N \lhd G$, then

1. if G soluble $\Longrightarrow H$ soluble
2. if G soluble $\Longrightarrow G/N$ soluble
3. if N and G/N soluble $\Longrightarrow G$ soluble

Proof. 1. Since G soluble, by definition: $\exists \;\; 1 = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G$ with Abelian quotients $\frac{G_{i+1}}{G_i}$.

Let $H_i = G_i \cap H$, then H has a series $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_r = H$, next we show that the quotients $\frac{H_{i+1}}{H_i}$ are Abelian (so that H is soluble):

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} \overset{(*)}{=} \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \overset{(**)}{\cong} \frac{G_i(G_{i+1} \cap H)}{G_i} \subseteq \frac{G_{i+1}}{G_i}$$

(*): to see why, $H_i = G_i \cap H = G_i \cap H_i = G_i \cap H_{i+1} = G_i \cap (G_{i+1} \cap H)$.
(**): by the 2nd Isomorphism Theorem (i.3).

[TODO: diagram of subgroups]

Notice that $\frac{G_{i+1}}{G_i}$ is Abelian, thus the left-hand-side of the congruence is also Abelian. Therefore, $\frac{H_{i+1}}{H_i}$ is Abelian, thus H is soluble.

2. For G/N to be soluble, (by definition) it would have the series $\frac{N}{N} = G_0 \frac{N}{N} \lhd G_1 \frac{N}{N} \lhd \ldots \lhd G_r \frac{N}{N} = \frac{G}{N}$, and any quotient being $\frac{G_{i+1}\frac{N}{N}}{G_i\frac{N}{N}}$.

   The series clearly exists, so now we show that the quotients are Abelian, so that G/N is soluble:

$$\frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \overset{(*)}{\cong} \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i}$$

   (*): by the 2nd Isomorphism Theorem (i.3).

   The last quotient is a quotient of the Abelian group G_{i+1}/G_i, so it is Abelian.

   Hence, $\frac{G_{i+1}N}{G_iN}$ is also Abelian; so $\frac{G}{N}$ is soluble.

3. By the definition of N and G/N being soluble,

$$N \text{soluble} \implies \quad 1 = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_r = N$$
$$G/N \text{soluble} \implies \quad 1 = \frac{N}{N} = \frac{G_0}{N} \triangleleft \frac{G_1}{N} \triangleleft \ldots \triangleleft \frac{G_r}{N} = \frac{G}{N}$$

both with Abelian quotients.

Consider the series of G given by combining the two previous series:

$$1 = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_r = N = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_r = G$$

the quotients are either

- $\frac{N_{i+1}}{N_i}$, Abelian
- $\frac{G_{i+1}}{G_i}$, isomorphic to $\frac{G_{i+1}/N}{G_i/N}$, which is Abelian.

Therefore, the quotients are always Abelian; hence G is soluble. □

Definition 14.5. G is *simple* if it's nontrivial and it's only normal subgroups are 1 and G.

Theorem 14.6. A *soluble* group is *simple* iff it is cyclic of prime order.

Theorem 14.7. if $n \geq 5$, then $\mathbb{A}_n$ is simple.

Corollary 14.8. $\mathbb{S}_n$ is not soluble if $n \geq 5$.

Proof. if $\mathbb{S}_n$ were soluble, then $\mathbb{A}_n$ would be soluble by Theorem 14.1(i), and simple by Theorem 14.7, hence of prime order by Theorem 14.6.

But observe: $|\mathbb{A}_n| = \frac{1}{2}(n!)$ is not prime if $n \geq 5$.
Thus $\mathbb{S}_n$ is not soluble if $n \geq 5$. □

Lemma 14.14. if A finite and abelian group with $p \Big| |A|$ (p prime), then A has an element of order p.

Proof. i. if $|A|$ prime and Abelian $\implies$ then A is cyclic.

Since $p||A| \quad \implies \quad \exists!\ B \subseteq A$ such that $|B| = p$, where $B =< b >$ with $ord(b) = p$. So the lemma is proven.

ii. if $|A|$ non-prime:

take $M \subseteq A$ with $|M| = m$, m maximal. Then

a. if $p|m \quad \implies \quad \exists!\ B' =< b' >,\ b' \in A$ with $|B'| = p$ and $ord(b') = p$.
b. if $p \nmid m$: Let $b \in A \not{/}M$ and $B =< b >$.
Then $MB \supseteq M$, and by maximility must be $MB = A$.
By the 1st Isomorphism Theorem (i.1),

$$|A| = |MB| = \frac{|M| \cdot |B|}{|M \cap B|}$$

both $|A|$ and $|B|$ are divisible by p (but recall that $p \nmid m = |M|$), since B is cyclic and $p||B|$
$\Longrightarrow$ thus, B has an element of order p.
So, if $|B| = r$, and $p|r \quad \Longrightarrow \quad ord(b^{r/p}) = p$.

Hence, in all cases i, ii.a, ii.b, A contains an element of order p.

$\square$

Theorem 14.15. (Cauchy's Theorem) if $p \Big| |G|$ (p prime), then $\exists\ x \in G$ such that $ord(x) = p$.

Proof. (induction on $|G|$)
For $|G| = 1, 2, 3$, trivial.
Induction step: class equation

$$|G| = 1 + |C_2| + \ldots + |C_r|$$

since $p \Big| |G|$, must have $p \nmid |C_j|$ for some $j \geq 2$.

If $x \in C_j \quad \Longrightarrow p \Big| |C_G(x)|$ (since $|C_j| = |G|/|C_G(x)|$, recall $p \Big| |G|$).

i. if $C_G(x) \neq G$:
   (by induction) since $p \Big| |C_G(x)|$,
   $\exists a \in C_G(x)$ with $ord(a) = p$, and $a \in G$ (since $C_G(x) \subset G$).

ii. otherwise, $C_G(x) = G$:
   implies $x \in Z(G)$, by choice $x \neq 1$, so $Z(G) \neq 1$.
   Then either

   I. $p \Big| |Z(G)| \quad \longrightarrow$ Abelian case, Lemma 14.14.

   II. $p \Big| \!\!\not |Z(G)|$: by induction, $\exists x \in G$ such that $\hat{x} \in G/Z(G)$, with $ord(\hat{x}) = p$. (where $\hat{x}$ is the image of x).
   $\Longrightarrow \quad x^p \in Z(G)$, but $x \notin Z(G)$.
   Let $X =< x >$, cyclic.
   $XZ(G)$ is Abelian, and $p \Big| |XZ(G))|$
   $\Longrightarrow$ by Lemma 14.14, it has an element of order p, and this element belongs to G.

$\square$

Definition 15.1. (Soluble by radicals) let $f \in K[t],\ K \subseteq \mathbb{C}$, and Σ a splitting field of f over K.

f is *soluble by radicals* if

$\exists$ a field M with $\Sigma \subseteq M$ such that $M : K$ is a radical extension (8.12).

Note: not required $\Sigma : K$ to be radical.

Lemma 15.3. $L : K$ radical extension $\mathbb{C}$, and M normal enclosure of $L : K$, then $M : K$ is radical.

Proof. let $L = K(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{j-1})$ (by definition of $L : K$ being a radical extension).

Let f_i be the minimal polynimal of α_i over K.

Then, $M \supseteq L$ is splitting field of ${}_{i=1}^{r} f_i$, since M is normal enclosure of $L : K$.

For every zero β_{ij} of f_i in M,

$\exists$ an isomorphism $\sigma : K(\alpha_i) \longrightarrow K(\beta_{ij})$ by Corollary 5.13.

By Proposition 11.4, since $K(\alpha_i),\ K(\beta_{ij}) \subset M$, σ extends to a K-automorphism

$$\tau : M \longrightarrow M$$

since M is splitting field (ie. contains the zeros of f_i).

Since α is a member of radical sequence for a subfield of M, so it is β_{ij}.

By combining the sequences for M, $M : K$ is a radical extension. $\square$

The next two lemmas show that certain Galois groups are Abelian.

Lemma 15.4.

Proof. $\square$

2 Tools

This section contains tools that I found useful to solve Galois Theory related problems, and that don't appear in Stewart's book.

2.1 De Moivre's Theorem and Euler's formula

Useful for finding all the roots of a polynomial.

Euler's formula:

$$e^{i\psi} = cos\psi + i \cdot sin\psi$$

The n-th roots of a complex number $z = x + iy = r(cos\theta + i \cdot sin\theta)$ are given by

$$z_k = \sqrt[n]{r} \cdot \left(cos(\frac{\theta + 2k\pi}{n}) + i \cdot sin(\frac{\theta + 2k\pi}{n}) \right)$$

for $k = 0, \ldots, n-1$.

So, by Euler's formula:

$$z_k = \sqrt[n]{r} \cdot e^{i(\frac{\theta+2k\pi}{n})}$$

Usually we will set $\alpha = \sqrt[n]{r}$ and $\zeta = e^{\frac{2\pi i}{n}}$, and find the $\mathbb{Q}$-automorphisms from there (see 3.1 for examples).

2.2 Einsenstein's Criterion

reference: Stewart's book

Let $f(t) = a_0 + a_1 t + \ldots + a_n t^n$, suppose there is a prime q such that

1. $q \nmid a_n$
2. $q | a_i$ for $i = 0, \ldots, n-1$
3. $q^2 \nmid a_0$

Then, f is irreducible over $\mathbb{Q}$.

TODO proof & Gauss lemma.

2.3 Elementary symmetric polynomials

TODO from orange notebook, page 36

2.4 Cyclotomic polynomials

2.4.1 From Elmyn Berlekamp's "Algebraic Coding Theory" book

The notes in this section are from the book "Algebraic Coding Theory" by Elmyn Berlekamp [3].

Some times we might find polynomials that have the shape of $t^n - 1$, those are *cyclotomic polynomials*, and have some properties that might be useful.

Observe that in a finite field of order q, factoring $x^q - x$ gives

$$x^q - x = x(x^{q-1} - 1)$$

The factor $x^{q-1} - 1$ is a special case of $x^n - 1$: if we assume that the field contains an element α of order n, then the roots of $x^n - 1 = 0$ are

$$1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{n-1}$$

and $\deg(x^n - 1) = n$, thus $x^n - 1$ has at most n roots in any field, henceforth the powers of α must include all the n-th roots of unity.

There fore, in any field which contains a primitive n-th root of unity we have:

Theorem 4.31.

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i) = \prod_{i=1}^{n} (x - \alpha^i)$$

If $n = k \cdot d$, then $\alpha^k, \alpha^{2k}, \alpha^{3k}, \dots, \alpha^{dk}$ are all roots of $x^d - 1 = 0$

Every element with order dividing n, must be a power of α, since an element of order d is a d-th root of unity.

Every power of α has order which divides n, and every field element whose order divides n is a power of α. This suggests that we partition the powers of α according to their orders:

$$x^n - 1 = \prod_{\substack{d, \\ d|n}} \prod_{\beta} (x - \beta)$$

where at each iteration, β is a field element of order d for each d.

The polynomial whose roots are the field elements of order d is called the *cyclotomic polynomial*, denoted by $Q^{(d)}(x)$.

Theorem 4.32.

$$x^n - 1 = \prod_{\substack{d, \\ d|n}} Q^{(d)}(x)$$

2.4.2 From Ian Stewart's "Galois Theory" book

Notes from Ian Stewart's book [1].

Consider the case $n = 12$, let $\zeta = e^{\pi i/6}$ be a primitive 12-th root of unity. Classify its powers (ζ^j) according to their minimal power d such that $(\zeta^j)^d = 1$ (ie. when they are primitive d-th roots of unity).

$d = 1, \quad 1$

$d = 2, \quad \zeta^6$

$d = 3, \quad \zeta^4, \zeta^8$

$d = 4, \quad \zeta^3, \zeta^9$

$d = 6, \quad \zeta^2, \zeta^{10}$

$d = 12, \quad \zeta, \zeta^5, \zeta^7, \zeta^{11}$

Observe that we can factorize $t^{12} - 1$ by grouping the corresponding zeros:

$$\begin{aligned} t^{12} - 1 = &(t-1)\times \\ &(t-\zeta^6)\times \\ &(t-\zeta^4)(t-\zeta^8)\times \\ &(t-\zeta^3)(t-\zeta^9)\times \\ &(t-\zeta^2)(t-\zeta^{10})\times \\ &(t-\zeta)(t-\zeta^5)(t-\zeta^7)(t-\zeta^{11}) \end{aligned}$$

which simplifies to

$$t^{12} - 1 = (t-1)(t+1)(t^2+t+1)(t^2+1)(t^2-t+1)F(t)$$

where $F(t) = (t-\zeta)(t-\zeta^5)(t-\zeta^7)(t-\zeta^{11}) = t^4 - t^2 + 1$ (this last step can be obtained either by multiplying $(t-\zeta)(t-\zeta^5)(t-\zeta^7)(t-\zeta^{11})$ together, or by dividing $t^{12} - 1$ by all the other factors).

Let $\Phi_d(t)$ be the factor corresponding to primitive d-th roots of unity, then we have proved that

$$t^{12} - 1 = \Phi_1\Phi_2\Phi_3\Phi_4\Phi_6\Phi_{12}$$

Definition 21.5. The polynomial $\Phi_d(t)$ defined by

$$\Phi_n(t) = \prod_{a \in \mathbb{Z}_n, (a,n)=1} (t - \zeta^a)$$

is the n-th *cyclotomic polynomial* over $\mathbb{C}$.

Corollary 21.6. $\forall n \in \mathbb{N}$, the polynomial $\Phi_n(t)$ lies in $\mathbb{Z}[t]$ and is monic and irreducible.

Theorem 21.9.

1. The Galois group $\Gamma(\mathbb{Q}(\zeta) : \mathbb{Q})$ consists of the $\mathbb{Q}$-automorphisms ψ_j defined by

   $$\psi_j(\zeta) = \zeta^j$$

   where $0 \leq j \leq n-1$ and j is prime to n.

2. $\Gamma(\mathbb{Q}(\zeta) : \mathbb{Q}) \overset{iso}{\cong} \mathbb{Z}_n^*$, and is an abelian group.

3. its order is $\phi(n)$

4. if n is prime, $\mathbb{Z}_n^*$ is cyclic

2.4.3 Examples

Examples of cyclotomic polynomials:

$$\Phi_n(x) = x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1 = \sum_{i=0}^{n-1} x^i$$

$$\Phi_{2p}(x) = x^{p-1} + \ldots + x^2 - x + 1 = \sum_{i=0}^{p-1} (-x)^i$$

$$\Phi_m(x) = x^{m/2} + 1, \quad \text{when } m \text{ is a power of 2}$$

2.5 Lemma 1.42 from J.S.Milne's book

Lemma from J.S.Milne's book [2].

Useful for when dealing with $x^p - 1$ with p prime.

Observe that

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + 1)$$

Notice that

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

is the p-th Cyclotomic polynomial.

Lemma 1.42. If p prime, then $x^{p-1} + \ldots + 1$ is irreducible; hence $\mathbb{Q}[e^{2\pi i/p}]$ has degree $p-1$ over $\mathbb{Q}$.

Proof. Let $f(x) = (x^p - 1)/(x-1) = x^{p-1} + \ldots + 1$ then

$$f(x+1) = \frac{(x+1)^p - 1}{x+1-1} = \frac{(x+1)^p - 1}{x} = x^{p-1} + \ldots + a_i x^i + \ldots + p$$

with $a_i = \binom{p}{i+1}$.

We know that $p | a_i$ for $i = 1, \ldots, p-2$, therefore $f(x+1)$ is irreducibe by Einsenstein's Criterion.

This implies that $f(x)$ is irreducible. □

2.6 Dihedral groups - Groups of symmetries

Source: Wikipedia and [4].

Dihedral groups ($\mathbb{D}_n$) represent the symmetries of a regular n-gon.

Properties:

- are non-abelian (for $n > 2$), ie. $rs \neq sr$
- order $2n$
- generated by a rotation r and a reflection s

- $r^n = s^2 = id, \quad (rs)^2 = id$

Subgroups of $\mathbb{D}_n$:

- rotation form a cyclic subgroup of order n, denoted as $< r >$
- for each d such that $d|n$, $\exists\ \mathbb{D}_d$ with order $2d$
- normal subgroups
  - for n odd: $\mathbb{D}_n$ and $< r^d >$ for every $d|n$
  - for n even: 2 additional normal subgroups
- Klein four-groups: $\mathbb{Z}_2 \times \mathbb{Z}_2$, of order 4

Total number of subgroups in $\mathbb{D}_n$: $d(n) + s(n)$, where $d(n)$ is the number of positive disivors of n, and $s(n)$ is the sum of those divisors.

Example . For $\mathbb{D}_6$, we have $\{1, 2, 3, 6\}|6$, so $d(n) = d(6) = 4$, and $s(6) = 1+2+3+6 = 12$; henceforth, the total amount of subgroups is $d(n)+s(n) = 4+12 = 16$.

For $n \geq 3, \quad \mathbb{D}_n \subseteq \mathbb{S}_n$ (subgroup of the Symmetry group).

2.7 Rolle's theorem

Theorem . (Rolle's Theorem) if a real-valued function f is

- *continuous* on a proper closed interval $[a, b]$
- *differentiable* on the open interval (a, b)
- $f(a) = f(b)$

then, $\exists$ at least one c in (a, b) such that $Df(c) = 0$.

Proof. (proof source: cue math website) Notice that when $Df(x_i) = 0$ occurs, is a maximum or minimum (extrema) value of f. $\Longrightarrow$ if a function is continuous, it is guaranteed to have both a maximum and a minimum point in the interval.

Two possibilities:

i. f is constant
$\Longrightarrow$ ie. a horizontal line ($f(a) = f(b)$), ie. no slope $\Longrightarrow Df = 0$ everywhere in $[a, b]$.

ii. f is not constant:
since f not constant, must change directions in ordder to start and end at the same y-value ($f(a) = f(b)$).
Thus at some point between a and b it will either have a minimum, maximum or both.

a. does the maximum occur at a point where $Df > 0$?
   No, because if $Df > 0$, then f is increasing, but it can not increase since we're at its maximum point.

b. does the maximum occur at a point where $Df < 0$?
   No, because if $Df < 0$, then f is deccreasing, which means that at our left it was larger, but we're at a maximum point, so a contradiction.

Same with minimus.
$\implies$ Hence, since $Df \not< 0$ and $Df \not> 0$, and Df exists, then $Df = 0$.

Thus, f must have extrema (either max or min or both), and at that extrema Df must be zero. $\square$

Consequence of Rolle's Theorem:

Corollary . (Zero separation property) Between any two distinct consecutive zeros of f, there lies at least one zero of Df.

Example . If $f(t)$ has zeros t_1, t_2, with $t_1 < t_2$, and f is derivable, then by Rolle'z theorem:
$\exists c \in (t_1, t_2)$ such that $Df(c) = 0$.
Hence, the zeros of Df *separate* the zeros of f.

3 Exercises

3.1 Galois groups

3.1.1 $t^6 - 7 \in \mathbb{Q}$

This exercise comes from a combination of exercises 12.4 and 13.7 from [1].

First let's find the roots. By De Moivre's Theorem (2.1), $t_k = \sqrt[6]{7} \cdot e^{i\frac{2\pi k}{6}}$.

From which we denote $\alpha = \sqrt[6]{7}$, and $\zeta = e^{\frac{2\pi i}{6}}$, so that the roots of the polynomial are $\{\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4, \alpha\zeta^5\}$, ie. $\{\alpha\zeta^k\}_0^5$.

Hence the *splitting field* is $\mathbb{Q}(\alpha, \zeta)$.

Degree of the extension

In order to find $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}$, we're going to split it in tow parts. By the Tower Law (6.6),

$$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

To find each degree, we will find the minimal polynomial of the adjoined term over the base field of the extension:

i. minimal polynomial of α over $\mathbb{Q}$
   By Einsenstein's Criterion (2.2), with $q = 7$ we have that $q \nmid 1$, $7|-7, 0, 0, \ldots$, and $7^2 \nmid -7$, hence $f(t)$ is irreducibe over $\mathbb{Q}$, thus is the minimal polynomial

   $$m_i(t) = f(t) = t^6 - 7$$

   which has roots $\{\alpha\zeta^k\}_0^5$.

ii. minimal polynomial of ζ over $\mathbb{Q}(\alpha)$
   Since ζ is the primitive 6th root of unity, we know that the minimal polynomial will be the 6th cyclotomic polynomial (2.4):

   $$m_{ii}(t) = \Phi_6(t) = t^2 - t + 1$$

   which has roots $\zeta, -\zeta$.

   Since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, and the roots of $\Phi_6(t) = t^2 - t + 1$ are in $\mathbb{C}$, $\Phi_6(t)$ remains irreducible over $\mathbb{Q}(\alpha)$.

Therefore, by the tower of law,

$$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = \deg \Phi_6(t) \cdot \deg f(t) = 2 \cdot 6 = 12$$

and by the Fundamental Theorem of Galois Theory, we know that

$$|\Gamma(\mathbb{Q}(\alpha, \zeta) : \mathbb{Q})| = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 12$$

which tells us that there exist 12 $\mathbb{Q}$-automorphisms of the Galois group.

Let's find the 12 $\mathbb{Q}$-automorphisms. Start by defining σ which fixes ζ and acts on α, sending it to another of the roots of the minimal polynomial of α over $\mathbb{Q}$, $f(t)$, choose $\alpha\zeta$.

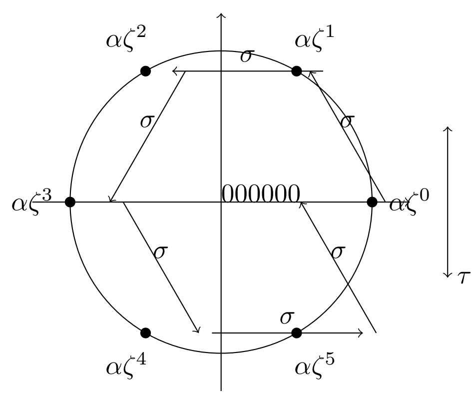
Now define τ which fixes α and acts on ζ, sending it into another root of the minimal polynomial of ζ over $\mathbb{Q}(\alpha)$, choose $-\zeta$.

$$\begin{aligned} \sigma &: \alpha \mapsto \alpha\zeta \qquad & \tau &: \alpha \mapsto \alpha \\ & \zeta \mapsto \zeta & & \zeta \mapsto -\zeta = \zeta^{-1} \end{aligned}$$

In other words, we have 12 $\mathbb{Q}$-automorphisms, which are the combination of σ and τ:

$$\begin{aligned} \sigma^k \tau^j : \ & \alpha \mapsto \alpha\zeta^k \\ & \zeta \mapsto \zeta^j \end{aligned}$$

for $0 \leq k \leq 5$ and $j = \pm 1$.



NOTE: WIP diagram.

Observe, that Γ is generated by the combination of σ and τ, and it is isomorphic to the group of symmetries of order 12, the dihedral group (2.6) of order 12, $\mathbb{D}_6$, ie. $\Gamma \cong \mathbb{D}_6$.

Let's find the subgroups of Γ, and the fixed fields of $\mathbb{Q}(\alpha, \zeta)$.

We know that $\Gamma \cong \mathbb{D}_6$, and we know from the properties of the dihedral group (2.6) that the number of subgroups of $\mathbb{D}_6$ will be $d(6) + s(6) = 4 + 12 = 16$ subgroups.

generators	order	group	fixed field	notes (check fixed field)
$\langle\rangle = \langle\sigma^6\rangle = \langle\tau^2\rangle$	1	id	$\mathbb{Q}(\alpha, \zeta)$	
$\langle\sigma\rangle = \langle\sigma^5\rangle$	6	$\mathbb{Z}_6$	$\mathbb{Q}(\zeta)$	
$\langle\sigma^2\rangle = \langle\sigma^4\rangle$	3	$\mathbb{Z}_3$	$\mathbb{Q}(\alpha^3, \zeta)$	$\sigma^2(\alpha^3) = \alpha^3\zeta^{3\cdot 2} = \alpha^3\zeta^6 = \alpha^3 \cdot 1 = \alpha^3$
$\langle\sigma^3\rangle$	2	$\mathbb{Z}_2$	$\mathbb{Q}(\alpha^2, \zeta)$	$\sigma^3(\alpha^2) = (\alpha\zeta^3)^2 = \alpha^2\zeta^6 = \alpha^2$
$\langle\tau\rangle$	2	$\mathbb{Z}_2$	$\mathbb{Q}(\alpha)$	
$\langle\sigma\tau\rangle$	2	$\mathbb{Z}_2$	$\mathbb{Q}(\alpha + \alpha\zeta)$	$\sigma\zeta(\alpha+\alpha\zeta) = \sigma(\alpha+\alpha\zeta^{-1}) = \alpha\zeta+\alpha\zeta^{-1}\zeta = \alpha\zeta+\alpha$
$\langle\sigma^2\tau\rangle$	2	$\mathbb{Z}_2$	$\mathbb{Q}(\alpha + \alpha\zeta^2), \mathbb{Q}(\alpha\zeta)$	$\sigma^2\tau(\alpha + \alpha\zeta^2) = \sigma(\alpha + \alpha\zeta^{-2}) = \alpha\zeta^2 + \alpha\zeta^{-2}\zeta^2 = \alpha\zeta^2 + \alpha$
$\langle\sigma^3\tau\rangle$	2	$\mathbb{Z}_2$	$\mathbb{Q}(\alpha + \alpha\zeta^3)$	$\sigma^3\tau(\alpha + \alpha\zeta^3) = \sigma(\alpha + \alpha\zeta^{-3}) = \alpha\zeta^3 + \alpha\zeta^{-3}\zeta^3 = \alpha\zeta^3 + \alpha$
$\langle\sigma^4\tau\rangle$	2	$\mathbb{Z}_2$	$\mathbb{Q}(\alpha + \alpha\zeta^4), \mathbb{Q}(\alpha\zeta^2)$	$\sigma^4\tau(\alpha + \alpha\zeta^4) = \sigma(\alpha + \alpha\zeta^{-4}) = \alpha\zeta^4 + \alpha\zeta^{-4}\zeta^4 = \alpha\zeta^4 + \alpha$
$\langle\sigma^5\tau\rangle$	2	$\mathbb{Z}_2$	$\mathbb{Q}(\alpha + \alpha\zeta^5)$	$\sigma^5\tau(\alpha + \alpha\zeta^5) = \sigma(\alpha + \alpha\zeta^{-5}) = \alpha\zeta^5 + \alpha\zeta^{-5}\zeta^5 = \alpha\zeta^5 + \alpha$
$\langle\sigma, \tau\rangle = \langle\sigma^5, \tau\rangle$	$6 \cdot 2 = 12$	$\mathbb{D}_6$	$\mathbb{Q}$	
$\langle\sigma^2, \tau\rangle = \langle\sigma^4, \tau\rangle$	$3 \cdot 2 = 6$	$\mathbb{D}_3$	$\mathbb{Q}(\alpha^3)$	$\sigma^2(\alpha^3) = \alpha^3\zeta^{3\cdot 2} = \alpha^3$ and $\tau(\alpha^3) = \alpha^3$
$\langle\sigma^3, \tau\rangle$	$2 \cdot 2 = 4$	$\mathbb{D}_2$	$\mathbb{Q}(\alpha^2)$	$\sigma^3(\alpha^2) = \alpha^2\zeta^{2\cdot 2} = \alpha^2$ and $\tau(\alpha^2) = \alpha^2$
$\langle\sigma^2, \sigma\tau\rangle$	$3 \cdot 2 = 6$	$\mathbb{D}_3$	$\mathbb{Q}(\alpha^3 + \alpha^3\zeta^3)$	$\sigma^2(\alpha^3 + \alpha^3\zeta^3) = \alpha^3\zeta^3 + \alpha^3\zeta^3\zeta^3 = \alpha^3\zeta^3 + \alpha^3\zeta^6 = \alpha^3\zeta^3 + \alpha^3$
$\langle\sigma^3, \sigma\tau\rangle$	$2 \cdot 2 = 4$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Q}(\alpha^2\zeta^2), \mathbb{Q}(\alpha^2 + \alpha^2\zeta^2)$	$\sigma^3(\alpha^2 + \alpha^2\zeta^2) = \alpha^2\zeta^{2\cdot 3} + \alpha^2\zeta^{2\cdot 3}\zeta^2 = \alpha^2 + \alpha^2\zeta^2$ and $\sigma\tau(\alpha^2+\alpha^2\zeta^2) = \alpha^2\zeta^2+\alpha^2\zeta^{-2}\zeta^2 = \alpha^2\zeta^2+\alpha^2$
$\langle\sigma^3, \sigma^2\tau\rangle$	$2 \cdot 2 = 4$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Q}(\alpha^2\zeta^4), \mathbb{Q}(\alpha^2 + \alpha^2\zeta^4)$	$\sigma^2\zeta(\alpha^2\zeta^4) = \alpha^2\zeta^2\zeta^{-4} = \alpha^2\zeta^{-2} = \alpha^2\zeta^4$ and $\sigma^3(\alpha^2\zeta^4) = \alpha^2\zeta^{2\cdot 3}\zeta^4 = \alpha^2\zeta^4$

References

[1] Ian Stewart. Galois Theory, Third Edition, 2004.

[2] James S. Milne. Fields and galois theory (v5.10), 2022. Available at `https://jmilne.org/math/`.

[3] Elmyn Berlekamp. Algebraic coding theory, 1984. Revised Edition from 1984.

[4] Gaurab Bardhan, Palash Nath, and Himangshu Chakraborty. Subgroups and normal subgroups of dihedral group up to isomorphism, 2010. `https://scipp.ucsc.edu/~haber/ph251/Dn_subgroups.pdf`.

[5] Thomas W. Judson. Abstract algebra: theory and applications, 1994. Available at `http://abstract.ups.edu/download.html`.

[6] David S. Dummit and Richard M. Foote. Abstract algebra (third edition), 2004.