Name: Tuan Pham
ID: 4652218

Math 8202: General Algebra
Homework #4

10/10

(1) Problem 1, Lang p. 320

In the following series of problems, the Galois groups are denoted by G.

(a) $X^3 - X - 1$ over $\mathbb{Q}$.

By the Integral Root test, the possible rational roots of this polynomial are ± 1. After checking, none of them are roots. Thus $X^3 - X - 1$ has no root in $\mathbb{Q}$. Hence, it is irreducible over $\mathbb{Q}$.

The discriminant is $\Delta = -4a^3 - 27b^2 = -4(-1)^3 - 27(-1)^2 = -23 < 0$.

Thus Δ is not the square of any element of $\mathbb{Q}$. Therefore $G \simeq S_3$.

(b) $X^3 - 10$ over $\mathbb{Q}$.

By the Integral Root test, the possible rational roots of this polynomial are $\pm 2, \pm 5, \pm 10, \pm 1$. After checking, we see that none of them are roots. Thus $X^3 - 10$ has no root in $\mathbb{Q}$. Hence, it is irreducible over $\mathbb{Q}$.

The discriminant is $\Delta = -4a^3 - 27b^2 = -4 \cdot 0^3 - 27(-10)^2 = -27 \cdot 10^2 < 0$.

Thus Δ is not the square of any element of $\mathbb{Q}$. Therefore $G \simeq S_3$.

(c) $X^3 - 10$ over $\mathbb{Q}(\sqrt{2})$.

By part (b), $X^3 - 10$ is the irreducible polynomial of $\sqrt[3]{10}$ over $\mathbb{Q}$.

Moreover, $\sqrt[3]{10}$ is the only root of X^3-10 in $\mathbb{R}$. Suppose by contradiction that X^3-10 has a root in $\mathbb{Q}(\sqrt{2})$. Then $\sqrt[3]{10} \in \mathbb{Q}(\sqrt{2})$. There there are $r,s \in \mathbb{Q}$ such that $\sqrt[3]{10} = r\sqrt{2}+s$. We have

$$\begin{cases} (r\sqrt{2}+s)+(-r\sqrt{2}+s) = 2s, \\ (r\sqrt{2}+s)(-r\sqrt{2}+s) = s^2-2r^2. \end{cases}$$

Thus $\sqrt[3]{10}$ is a root of $X^2-2sX+(s^2-2r^2) \in \mathbb{Q}[X]$. This is a contradiction because X^3-10 is ~~the~~ an irreducible of $\sqrt[3]{10}$ over $\mathbb{Q}$.

Therefore, X^3-10 has no root in $\mathbb{Q}(\sqrt{2})$. Thus, it is irreducible over $\mathbb{Q}(\sqrt{2})$. As we see in part (b), $\Delta < 0$. Thus Δ is not the square of any element of $\mathbb{Q}(\sqrt{2})$. Thus $G \simeq S_3$.

(d) X^3-10 over $\mathbb{Q}(\sqrt{-3})$.

By part (b), X^3-10 is the irreducible polynomial of $\sqrt[3]{10}$ over $\mathbb{Q}$. Thus X^3-10 is also the irreducible polynomial of every root of its over $\mathbb{Q}$. Suppose by contradiction that X^3-10 has a root $\alpha \in \mathbb{Q}(\sqrt{-3})$. Then there are $r,s \in \mathbb{Q}$ such that $\alpha = r\sqrt{-3}+s$. We see that

$$\begin{cases} (r\sqrt{-3}+s)+(-r\sqrt{-3}+s) = 2s, \\ (r\sqrt{-3}+s)(-r\sqrt{-3}+s) = s^2+3r^2. \end{cases}$$

Thus α is a root of $X^2-2sX+(s^2+3r^2) \in \mathbb{Q}[X]$. This is a

Contradiction because the irreducible polynomial of α has degree 3.

Therefore, X^3-10 has no root in $\mathbb{Q}(\sqrt{-3})$. Thus it is irreducible over $\mathbb{Q}(\sqrt{-3})$. As in part (b), $\Delta = -27\cdot 10^2 = +(3\sqrt{-3})^2 10^2 = (30\sqrt{-3})^2$, which is the square of $30\sqrt{-3} \in \mathbb{Q}(\sqrt{-3})$. Therefore, $G \simeq A_3$.

(e) X^3-X-1 over $\mathbb{Q}(\sqrt{-23})$.

By part (a), X^3-X-1 is irreducible over $\mathbb{Q}$. Thus it is the irreducible of every root of its. Suppose by contradiction that X^3-X-1 has a root $\alpha \in \mathbb{Q}(\sqrt{-23})$. Then there are $r, s \in \mathbb{Q}$ such that

$$\alpha = r\sqrt{-23} + s.$$

Because $(r\sqrt{-23}+s)(-r\sqrt{-23}+s) = s^2+23r^2$ and $(r\sqrt{-23}+s)+(-r\sqrt{-23}+s)=2s$, α is a root of $X^2-2sX+(s^2+23r^2) \in \mathbb{Q}[X]$. This is a contradiction because the irreducible polynomial of α over $\mathbb{Q}$ has degree 3

Therefore, X^3-X-1 has no root in $\mathbb{Q}(\sqrt{-23})$. Thus, it is irreducible over $\mathbb{Q}(\sqrt{-23})$. As in part (a), $\Delta = -23 = \sqrt{-23}^2$. Thus $G \simeq A_3$.

(f) X^4-5 over $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(i)$.

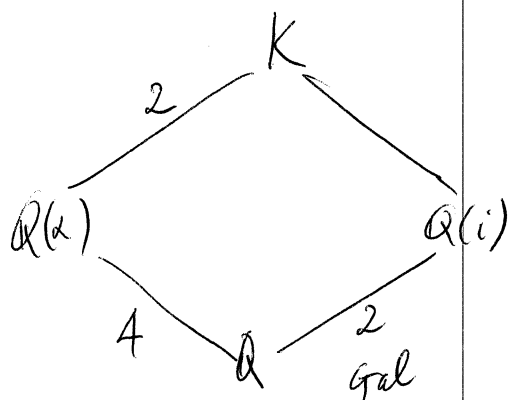
We have $X^4-5 = (X+\sqrt[4]{5})(X-\sqrt[4]{5})(X+i\sqrt[4]{5})(X-i\sqrt[4]{5})$. Put $\alpha = \sqrt[4]{5}$. Then the splitting field of X^4-5 is $K = \mathbb{Q}(\pm\alpha, \pm i\alpha) = \mathbb{Q}(\alpha, i)$.

4

By the Eisenstein's criterion with $p=5$, we know that X^4-5 is irreducible over $\mathbb{Q}$. Thus $[\mathbb{Q}(\alpha):\mathbb{Q}] = \deg(X^4-5) = 4$.

Since X^2+1 is irreducible over $\mathbb{Q}$, $[\mathbb{Q}(i):\mathbb{Q}] = \deg(X^2+1) = 2$. Moreover, $\mathbb{Q}(i) = \mathbb{Q}(i,-i)$ which is the spliting field of X^2+1. Thus $\mathbb{Q}(i)/\mathbb{Q}$ is a Galois extension. We have $\mathbb{Q} \subset \mathbb{Q}(i) \cap \mathbb{Q}(\alpha)$. Suppose $x \in \mathbb{Q}(i) \cap \mathbb{Q}(\alpha)$. Then there are $r, s \in \mathbb{Q}$ such that $x = r+is$. Since $x \in \mathbb{Q}(\alpha) \subset \mathbb{R}$, $s=0$. Thus $x = r \in \mathbb{Q}$. Thus $\mathbb{Q} = \mathbb{Q}(i) \cap \mathbb{Q}(\alpha)$.

We have the following diagram.



$$[K:\mathbb{Q}(\alpha)] = [\mathbb{Q}(i):\mathbb{Q}] = 2.$$

Thus, $[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = 4 \times 2 = 8$.

Then $$[K:\mathbb{Q}(i)] = \frac{[K:\mathbb{Q}]}{[\mathbb{Q}(i):\mathbb{Q}]} = \frac{8}{2} = 4.$$

We have $[\mathbb{Q}(i)(\alpha):\mathbb{Q}(i)] \leq \deg(X^4-5) = 4$. Thus the equality must happen. Thus X^4-5 is irreducible over $\mathbb{Q}(i)$. Thus there is a unique $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i))$ such that $\sigma(\alpha) = i\alpha$. Moreover,

$$\sigma^2(\alpha) = \sigma(i\alpha) = i^2\alpha = -\alpha,$$

$$\sigma^3(\alpha) = \sigma(\sigma^2(\alpha)) = \sigma(-\alpha) = -i\alpha,$$

$$\sigma^4(\alpha) = \sigma(\sigma^3(\alpha)) = \sigma(-i\alpha) = (-i)(i\alpha) = \alpha.$$

Thus $\mathrm{ord}(\sigma) = 4$.

We have $2 = [K : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)] \leq \deg(X^2+1)$. Thus the equality must hold. Thus X^2+1 is irreducible over $\mathbb{Q}(\alpha)$. Thus there is a unique $\tau \in \mathrm{Gal}(K/\mathbb{Q}(\alpha))$ such that $\tau(i) = -i$. Since $\tau^2(i) = \tau(-i) = i$, $\mathrm{ord}(\tau) = 2$. Moreover, $\tau \notin \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$ because it fixes α but not i.

Because $|G| = [K : \mathbb{Q}] = 8$, we have

$$G = \{\tau\sigma^k : 0 \leq k < 4\} \cup \{\sigma^k : 0 \leq k < 4\}.$$

We have $\tau\sigma, \sigma^3\tau \in \mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})$, such

$$\tau\sigma(i) = \tau(i) = -i, \qquad \tau\sigma(\alpha) = \tau(i\alpha) = \tau(i)\tau(\alpha) = -i\alpha,$$

$$\sigma^3\tau(i) = \sigma^3(-i) = -\sigma^3(i) = -i, \qquad \sigma^3\tau(\alpha) = \sigma^3(\alpha) = -i\alpha.$$

Thus $\tau\sigma = \sigma^3\tau$. This means $G = \langle \sigma, \tau \mid \sigma^4 = \mathrm{id}, \tau^2 = \mathrm{id}, \tau\sigma = \sigma^3\tau \rangle$.

Thus $G \simeq D_8$.

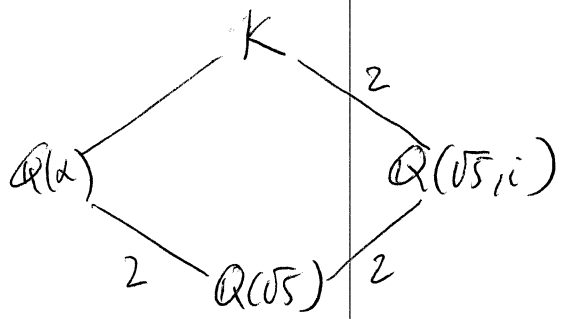
Put $G_1 = \mathrm{Gal}(K/\mathbb{Q}(\sqrt{5}))$. First we'll compute the degree of the extension $K/\mathbb{Q}(\sqrt{5})$. Because X^2+1 has no real root, it is ~~separable~~ irreducible over $\mathbb{Q}(\sqrt{5})$. Thus $[\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}(\sqrt{5})] = 2$.

Because $X^2 - \sqrt{5}$ has no root in $\mathbb{Q}(\sqrt{5})$, it is irreducible over $\mathbb{Q}(\sqrt{5})$.

~~...~~ $\sqrt{X}$ ~~...~~ ~~...~~ ~~...~~ Since $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, -\alpha)$, the extension $\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{5})$ is normal and thus Galois.

6

We have $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{5},i) \cap \mathbb{Q}(\alpha)$. Take any $x \in \mathbb{Q}(\sqrt{5},i) \cap \mathbb{Q}(\alpha)$. Then there are $u, v \in \mathbb{Q}(\sqrt{5})$ such that $x = u + iv$. Since $x \in \mathbb{Q}(\alpha) \subset \mathbb{R}$, $v = 0$. Then $x = u \in \mathbb{Q}(\sqrt{5})$. Hence, $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{5},i) \cap \mathbb{Q}(\alpha)$. Thus, $[K : \mathbb{Q}(\sqrt{5},i)] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5})] = 2$ and we have the following diagram.



Then $[K : \mathbb{Q}(\sqrt{5}] = [K : \mathbb{Q}(\sqrt{5},i)][\mathbb{Q}(\sqrt{5},i) : \mathbb{Q}(\sqrt{5})]$

$= 2 \times 2 = 4$.

Thus $|G_1| = 4$.

We have $\sigma^2(\sqrt{5}) = \sigma^2(\alpha^2) = \sigma^2(\alpha)^2 = (-\alpha)^2 = \sqrt{5}$, and $\tau(\sqrt{5}) = \tau(\alpha^2)$ $= \tau(\alpha)^2 = \alpha^2 = \sqrt{5}$. Thus $\sigma^2, \tau \in G_1$. As mentioned earlier, $\mathrm{ord}(\sigma^2) = \mathrm{ord}(\tau) = 2$ and $\sigma^2 \neq \tau$. Moreover,

$$\sigma^2\tau(\alpha) = \sigma^2(\alpha) = -\alpha, \qquad \sigma^2\tau(i) = \sigma^2(-i) = -\sigma^2(i) = -i,$$

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

Thus $\sigma^2\tau = \tau\sigma^2$. Thus $G_1 = \langle\sigma^2\rangle\langle\tau\rangle \simeq \langle\sigma^2\rangle \times \langle\tau\rangle \simeq (\mathbb{Z}/2) \times (\mathbb{Z}/2)$.

Put $G_2 = \mathrm{Gal}(K/\mathbb{Q}(\sqrt{-5}))$. ~~We have $\sqrt{-5} = i\sqrt{5}$. Put $k = \mathbb{Q}(i\sqrt{5})$.~~

~~Suppose by contradiction that $\alpha \in k$. Then there exist $r, s \in \mathbb{Q}$ such that $\alpha = ri\sqrt{5} + s$. Since $\alpha \in \mathbb{R}$, $r = 0$. Thus $\alpha = s \in \mathbb{Q}$. This is a contradiction.~~ Because $\sqrt{-5}$ is a root of $X^2 + 5$ and $X^2 + 5$ is irreducible over $\mathbb{Q}$, it is the irreducible polynomial of $\sqrt{-5}$ over $\mathbb{Q}$. Thus,

$[\mathbb{Q}(\sqrt{-5}:\mathbb{Q}] = \deg(X^2+5) = 2$. We have

$$8 = [K:\mathbb{Q}] = [K:\mathbb{Q}(\sqrt{-5})][\mathbb{Q}(\sqrt{-5}):\mathbb{Q}] = 2[K:\mathbb{Q}(\sqrt{-5})].$$

Thus, $|G_2| = [K:\mathbb{Q}(\sqrt{-5})] = 4$. Note that $\sqrt{-5} = i\sqrt{5} = i\alpha^2$. We have

$$\sigma^2(i\alpha^2) = i\sigma^2(\alpha^2) = i\sigma^2(\alpha)^2 = i(-\alpha)^2 = i\alpha^2,$$

$$\sigma\tau(i\alpha^2) = \sigma(-\tau\alpha^2) = -i\sigma(\alpha^2) = -i\sigma(\alpha)^2 = -i(i\alpha)^2 = i\alpha^2.$$

Thus, $\sigma^2, \sigma\tau \in G_2$. Moreover, $(\sigma^2)^2 = id$ and

$$(\sigma\tau)^2 = \sigma(\tau\sigma)\tau = \sigma(\sigma^3\tau)\tau = \sigma^4\tau^2 = id.$$

Thus, $ord(\sigma^2) = ord(\sigma\tau) = 2$. Also,

$$\sigma^2(\sigma\tau) = \sigma^3\tau = \tau\sigma = \sigma(\sigma^3\tau)\sigma = \sigma(\tau\sigma)\sigma = (\sigma\tau)\sigma^2.$$

Thus, $G_2 = \langle\sigma^2\rangle\langle\tau\rangle \simeq (\mathbb{Z}/2)\times(\mathbb{Z}/2)$.

Put $G_3 = Gal(K/\mathbb{Q}(i))$. When we determined G_1 we showed that $[K:\mathbb{Q}] = 8$ and $[\mathbb{Q}(i):\mathbb{Q}] = 2$. Thus $|G_3| = [K:\mathbb{Q}(i)] = \dfrac{[K:\mathbb{Q}]}{[\mathbb{Q}(i):\mathbb{Q}]} = 4$.

Also, we pointed out that $\sigma \in G_3$ and $ord(\sigma) = 4$. Therefore,

$$G_3 = \langle\sigma\rangle \simeq \mathbb{Z}/4.$$

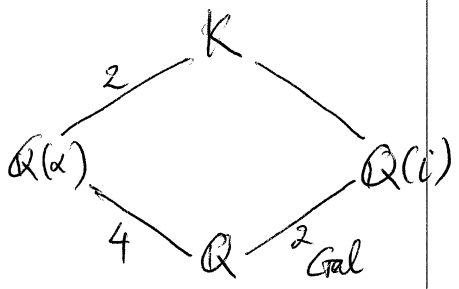
(g) $X^4 - a$ where a is any integer $\neq 0, \neq \pm 1$ and is square-free. Over $\mathbb{Q}$.

Because a is an integer which is not $0, -1, 1$, it has a prime divisor p. Since a is square free, $p^2 \nmid a$. By Eisenstein's criterion, $X^4 - a$ is irreducible over $\mathbb{Q}$. We considers two cases of a as follow.

• Case 1: $a > 0$

Then $X^4 - a$ has roots $\pm\sqrt[4]{a}, \pm i\sqrt[4]{a}$. Thus the splitting field is $K(\sqrt[4]{a}, i)$. Put $\alpha = \sqrt[4]{a}$. Since $X^4 - a$ is irreducible over $\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(X^4 - a) = 4$.

As mentioned in part (f), $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ and $\mathbb{Q}(i)/\mathbb{Q}$ is a Galois extension. We'll show that $\mathbb{Q} = \mathbb{Q}(\alpha) \cap \mathbb{Q}(i)$. Take $x \in \mathbb{Q}(\alpha) \cap \mathbb{Q}(i)$. Then there are $r, s \in \mathbb{Q}$ such that $x = r + si$. Since $x \in \mathbb{Q}(\alpha) \subset \mathbb{R}$, $s = 0$. Thus $x = r \in \mathbb{Q}$. Therefore $\mathbb{Q} = \mathbb{Q}(\alpha) \cap \mathbb{Q}(i)$. we have the following diagram.



$[K : \mathbb{Q}(\alpha)] = [\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Thus, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$.

From now, the arguments follow exactly the same as in part (f), from line 7th from the bottom of page 4 to line 7th from the bottom of page 5. Accordingly,

$$G = \langle \sigma, \tau \mid \sigma^4 = id, \tau^2 = id, \tau\sigma = \sigma^3\tau \rangle \simeq D_8$$

where $\sigma \in Gal(K/\mathbb{Q}(i))$ such that $\sigma(\alpha) = i\alpha$ and $\tau \in Gal(K/\mathbb{Q}(\alpha))$ such that $\tau(i) = -i$.

• Case 2: $a < 0$

Then $X^4 - a$ has roots $\pm\beta, \pm\bar{\beta}$ where $\beta = \sqrt{i}\sqrt[4]{-a} = \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)\sqrt[4]{-a}$.

Thus, $K = \mathbb{Q}(\beta, \bar{\beta}) = \mathbb{Q}\left(\beta+\bar{\beta}, \frac{\beta-\bar{\beta}}{\beta+\bar{\beta}}\right) = \mathbb{Q}(\sqrt{2}\sqrt[4]{-a}, i)$.

Put $\alpha = \sqrt{2}\sqrt[4]{-a}$. Then $K = \mathbb{Q}(\alpha, i)$. We have $\alpha^4 = -4a$. Thus α is a root of X^4+4a. Let p be a prime divisor of a. ~~Since $p^2 \nmid a$, by Eisenstein's criterion, we conclude that X^4+~~ If $p>2$ then $p^2 \nmid (4a)$. Thus, by Eisenstein's criterion, X^4+4a is irreducible over $\mathbb{Q}$. If a doesn't have any odd prime divisor, then all prime divisors of a must be 2. Since a is square-free, $4 \nmid a$. Since $a<0$, the only possible case is $a=-2$. Then $X^4+4a = X^4-8$. This polynomial doesn't have any rational root because $\pm\sqrt[4]{8} \notin \mathbb{Q}$. Suppose by contradiction that X^4-8 is reducible over $\mathbb{Q}$. Then there are $b,c,d,e \in \mathbb{Q}$ such that $X^4-8 = (X^2+bX+c)(X^2+dX+e)$. Then

$$\begin{cases} b+d=0 & (1) \\ bd+c+e=0 & (4) \\ be+cd=0 & (2) \\ ce=-8 & (3) \end{cases}$$

(1) gives $d=-b$. Then (2) becomes $b(e-c)=0$. By (3), $e \neq c$. Thus $b=0$. Then (4) gives $c+e=0$. Then (3) becomes $c^2=8$. This is impossible because $\pm\sqrt{8} \notin \mathbb{Q}$. Therefore, X^4+4a is irreducible over $\mathbb{Q}$.

Thus, $[\mathbb{Q}(\alpha):\mathbb{Q}] = \deg(X^4+4a) = 4$.

From now, we follow the same arguments as in Case 1, from the 4th line till the end. We get the same conclusion (with $\alpha = \sqrt[4]{2}\sqrt[4]{-a}$) that $G = \langle \sigma, \tau \mid \sigma^4 = id,\ \tau^2 = id,\ \tau\sigma = \sigma^3\tau \rangle \simeq D_8$

where $\sigma \in Gal(K/\mathbb{Q}(i))$ such that $\sigma(\alpha) = i\alpha$ and $\tau \in Gal(K/\mathbb{Q}(\alpha))$ such that $\tau(i) = -i$.

(b) $X^3 - a$ where a is any square-free integer ≥ 2. Over $\mathbb{Q}$.

We consider two cases.

- $a = \ell^3$ for some $\ell \in \mathbb{Z}$, $\ell \geq 2$

Then $X^3 - a = X^3 - \ell^3 = (X-\ell)(X^2+\ell X+\ell^2)$. The quadratic polynomial has roots α and $\bar{\alpha}$ with $\alpha = \ell\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \notin \mathbb{Q}$. Thus, it is irreducible over $\mathbb{Q}$. We have

$$K = \mathbb{Q}(\alpha, \bar{\alpha}) = \mathbb{Q}\left(\alpha, \frac{\alpha+\bar{\alpha}}{\ell}\right) = \mathbb{Q}(\alpha, 1) = \mathbb{Q}(\alpha).$$

Thus, $|G| = [K:\mathbb{Q}] = \deg(X^2+\ell X+\ell^2) = 2$. Because α and $\bar{\alpha}$ are roots of $X^2+\ell X+\ell^2$, there exists $\tau \in G$ such that $\tau(\alpha) = \bar{\alpha}$. Note that $\tau \neq id$ because $\alpha \neq \bar{\alpha}$. Therefore,

$$G = \langle \tau \rangle = \{id, \tau\} \simeq \mathbb{Z}/2.$$

- a is not a third power of any integer

Then $\sqrt[3]{a} \notin \mathbb{Q}$. Thus $X^3 - a$ has no root in $\mathbb{Q}$. Hence, it is

irreducible over $\mathbb{Q}$. The determinant is $\Delta = -4.0^3 - 27(a)^2 < 0$.

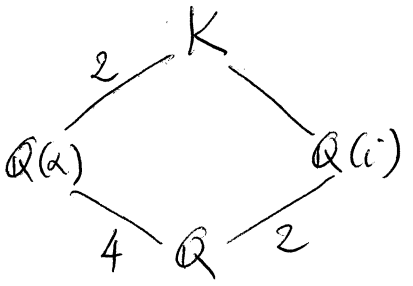
Thus, Δ is not the square of any element in $\mathbb{Q}$. Therefore, $G \simeq S_3$.

(i) X^4+2 over $\mathbb{Q}$, $\mathbb{Q}(i)$.

Put $G = Gal(K/\mathbb{Q})$. Now we are dealing with a special case of part (g) where $a = -2$. Accordingly, $\alpha = \sqrt{2}\sqrt[4]{2}$ and

$$G = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = id,\ \tau\sigma = \sigma^3\tau \rangle \simeq D_8$$

where $\sigma \in Gal(K/\mathbb{Q}(i))$ such that $\sigma(\alpha) = i\alpha$ and τ is the complex conjugation. Also, as in Part (g), we have the diagram:



Thus $[K : \mathbb{Q}(i)] = \dfrac{[K:\mathbb{Q}]}{[\mathbb{Q}(i):\mathbb{Q}]} = \dfrac{8}{2} = 4.$

Because $\sigma \in Gal(K/\mathbb{Q}(i))$ and $ord(\sigma) = 4$,

$$Gal(K/\mathbb{Q}(i)) = \langle \sigma \rangle \simeq \mathbb{Z}/4.$$

(j) $(X^2-2)(X^2-3)(X^2-5)(X^2-7)$ over $\mathbb{Q}$.

This is a special case of part (k) below. The answer is that G is isomorphic to the subgroup of S_8 generated by 4 transpositions (1 5), (2 6), (3 7) and (4 8). Also, $G \simeq (\mathbb{Z}/2) \times (\mathbb{Z}/2) \times (\mathbb{Z}/2) \times (\mathbb{Z}/2)$.

(k) $f(X) = (X^2-p_1)(X^2-p_2)\cdots(X^2-p_n)$ over $\mathbb{Q}$, where $p_1, p_2, \ldots, p_n$ are distinct prime numbers.

12

First, we have a general property as follow: let $p_1, \dots, p_n$ be n distinct prime numbers. Then any $\sqrt{p_i}$ is not in the field $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{i-1}}, \sqrt{p_{i+1}}, \dots, \sqrt{p_n})$ generated by ~~all~~ other the square roots of all other primes.

The proof involves the use of quadratic reciprocity, which can be found in the course note of Abstract Algebra of Professor Paul Garrett, page 256. Accepting this property, we put for every $i = 1, \dots, n$,

$$K_i = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{i-1}}, \sqrt{p_{i+1}}, \dots, \sqrt{p_n}).$$

Then $\pm\sqrt{p_i} \notin K_i$. Thus the polynomial $X^2 - p_i$ is irreducible over K_i. We have $K = K_i(\sqrt{p_i})$. Because $\sqrt{p_i}$ and $-\sqrt{p_i}$ are roots of $X^2 - p_i$, there exists $\sigma_i \in Gal(K/K_i)$ such that $\sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$. In other words, $\sigma_i \in G$ which fixes $\sqrt{p_1}, \dots, \sqrt{p_{i-1}}, \sqrt{p_{i+1}}, \dots, \sqrt{p_n}$ and switches the sign of $\sqrt{p_i}$. Because $\sigma_i^2(\sqrt{p_i}) = \sigma_i(\sigma_i(\sqrt{p_i})) = \sigma_i(-\sqrt{p_i}) = -\sigma_i(\sqrt{p_i}) = \sqrt{p_i}$, $\sigma_i^2 = id_K$. Thus $\sigma_i \in G$ has order 2.

Each $\sigma \in G$ permutes the roots of $f(X)$. In other words, σ reduces to a permutation of $\{\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}, -\sqrt{p_1}, -\sqrt{p_2}, \dots, -\sqrt{p_n}\}$. Label the elements $\sqrt{p_1}, \dots, \sqrt{p_n}, -\sqrt{p_1}, \dots, -\sqrt{p_n}$ by $1, 2, \dots, n, n+1, \dots, 2n$ in this order. Then we get an injective group morphism $\phi: G \to S_{2n}$ by which each σ_i is viewed as a transposition; $\phi(\sigma_i) = (i \; n+i)$.

Since the transpositions $(1\ n+1), (2, n+2), \dots, (n\ 2n)$ commute with one another, $\sigma_1, \dots, \sigma_n$ also commute. For each $\sigma \in G$, we have

$$\sigma(\sqrt{p_i})^2 = \sigma(\sqrt{p_i}^2) = \sigma(p_i) = p_i.$$

Thus, $\sigma(\sqrt{p_i}) = \pm\sqrt{p_i}$. Hence, σ reduces to identity on $\{\sqrt{p_i}, -\sqrt{p_i}\}$ or it permutes these numbers. Thus, σ is a product (composition) of some of $\sigma_1, \sigma_2, \dots, \sigma_n$. Thus $\sigma = \sigma_1^{r_1} \cdots \sigma_n^{r_n}$ where each $r_i \in \{0,1\}$. Therefore, $G = \langle \sigma_1, \dots, \sigma_n \rangle$ is an abelian group. G is isomorphic to the subgroup of S_{2n} generated by $(1\ n+1), (2\ n+2), \dots, (n\ n+n)$.

In another aspect, because G is abelian,

$$G \simeq \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle \times \cdots \times \langle \sigma_n \rangle \simeq (\mathbb{Z}/2) \times (\mathbb{Z}/2) \times \cdots \times (\mathbb{Z}/2) \quad (n \text{ times}).$$

(l) $f(X) = (X^3-3)(X^3-2)(X^2-2)$ over $F = \mathbb{Q}(\sqrt{-3})$.

In the following, we will always think of $\sqrt{-3}$ as $i\sqrt{3}$.

First, we'll show that X^3-3, X^3-2 and X^2-2 are irreducible over F. By Eisenstein's Criterion with $p=3$ or $p=2$, these polynomials are irreducible over $\mathbb{Q}$. Let α be a root of X^3-3. Suppose by contradiction that $\alpha \in F$. Then there are $r, s \in \mathbb{Q}$ such that $\alpha = r + s\sqrt{3}$. Then α is a root of $X^2 - 2rX + (r^2+3r^2) \in \mathbb{Q}[X]$. This is a

contradiction because the irreducible polynomial of α over $\mathbb{Q}$ has degree 3. Thus X^3-3 has no root in F. Thus it is irreducible over F. By exactly the same argument, we can conclude that X^3-2 is also irreducible over F. The polynomial X^2-2 has roots $\pm\sqrt{2}$. Suppose by contradiction that $\sqrt{2} \in F$. Then there are $r, s \in \mathbb{Q}$ such that $\sqrt{2} = r+s\sqrt{-3} = r+is\sqrt{3}$. Thus the immaginary part is zero. Thus $r = \sqrt{2} \notin \mathbb{Q}$. This is a contradiction. Therefore, X^2-2 is irreducible over F.

Let ζ be a third root of 1. Then $\zeta^2+\zeta+1=0$. We can choose $\zeta = \frac{-1+\sqrt{-3}}{2}$. Thus $\zeta \in F$. The splitting field of X^2-2 is

$$K_1 = F(\sqrt{2}, -\sqrt{2}) = F(\sqrt{2}).$$

The splitting field of X^3-2 is

$$K_2 = F(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2) = F(\sqrt[3]{2}).$$

The splitting field of X^3-3 is

$$K_3 = F(\sqrt[3]{3}, \sqrt[3]{3}\zeta, \sqrt[3]{3}\zeta^2) = F(\sqrt[3]{3}).$$

Put $G_i = Gal(K_i/F)$. We'll find G_1, G_2, G_3.

Since $F \subset K_1$ is a quadratic extension, $G_1 \simeq S_2$. Since $F \subset K_2$ is a cubic extension with $\Delta = -4\cdot 0^2 - 27(-2)^2 = (6\sqrt{-3})^2$, which is a

Square in F, $G_2 \simeq A_3$. Since $F \subset K_3$ is a cubic extension with $\Delta = -4 \cdot 0^2 - 27(-3)^2 = (9\sqrt{-3})^2$, $G_3 \simeq A_3$.

Put $G = Gal(K/F)$. Each $\sigma \in G$ permutes the roots of X^2-2, permutes the roots of X^3-2 and permutes the roots of X^3-3. Therefore we get an injective group homomorphism $\phi : G \longrightarrow S_2 \times A_3 \times A_3$ given by

$$\phi(\sigma) = \big(\sigma(\sqrt{2}), \sigma(-\sqrt{2})\big) \times \big(\sigma(\sqrt[3]{2}), \sigma(\sqrt[3]{2}5), \sigma(\sqrt[3]{2}5^2)\big) \times \big(\sigma(\sqrt[3]{3}), \sigma(\sqrt[3]{3}5), \sigma(\sqrt[3]{3}5^2)\big).$$

We have $F \subset K_2 \subset K_2K_3 \subset K_1K_2K_3 = K$. Thus, to show that ϕ is an isomorphism, we have to show $K_2 \cap K_3 = F$ and $K_1 \cap K_2K_3 = F$.

① Show that $K_2 \cap K_3 = F$:

Suppose by contradiction that $F \subsetneq K_2 \cap K_3$. Then $[K_2 \cap K_3 : F] > 1$. We have $F \subset K_2 \cap K_3 \subset K_2$ and $[K_2 : F] = 3$. Thus we must have $[K_2 : K_2 \cap K_3] = \frac{3}{3} = 1$. Thus $K_2 \cap K_3 = K_2$. This means $K_2 \subset K_3$. With the same argument, replacing K_2 by K_3, we get $K_3 \subset K_2$. Thus $K_2 = K_3 = F(\sqrt[3]{2}) = F(\sqrt[3]{3})$.

Since $\sqrt[3]{3} \in F(\sqrt[3]{2})$, there exists $h \in F[X]$ such that $h(\sqrt[3]{2}) = \sqrt[3]{3}$. Because the irreducible polynomial of $\sqrt[3]{2}$ over F has degree 3, we can assume $\deg h \leq 2$. Thus $h(X) = aX^2 + bX + c$ with $a, b, c \in F$.

16

Because $F = \mathbb{Q}(\sqrt{-3})$, there are $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Q}$ such that

$$a = a_1 + a_2\sqrt{-3} = a_1 + a_2 i\sqrt{3},$$

$$b = b_1 + b_2 i\sqrt{3},$$

$$c = c_1 + c_2 i\sqrt{3}.$$

We have $\sqrt[3]{3} = h(\sqrt[3]{2}) = a\sqrt[3]{4} + b\sqrt[3]{2} + c$ and

$$\sqrt[3]{3} = \overline{h(\sqrt[3]{2})} = \bar{a}\sqrt[3]{4} + \bar{b}\sqrt[3]{2} + \bar{c}. \quad (*)$$

Thus $(a-\bar{a})\sqrt[3]{4} + (b-\bar{b})\sqrt[3]{2} + (c-\bar{c}) = 0$. Thus $\sqrt[3]{2}$ is a root of $(a-\bar{a})X^2 + (b-\bar{b})X + (c-\bar{c}) \in F[X]$. Since the irreducible polynomial of $\sqrt[3]{2}$ has degree 3, we have $a = \bar{a}$, $b = \bar{b}$ and $c = \bar{c}$. Thus $a, b, c \in \mathbb{Q}$.

Because $G_2 = \mathrm{Gal}(F(\sqrt[3]{2})/F) \simeq A_3$, there is $\sigma \in G_2$ such that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\zeta$. Since $G_2 = F(\sqrt[3]{3})$, σ permutes the roots of $X^3 - 3$. Thus $\sigma(\sqrt[3]{3}) \in \{\sqrt[3]{3}, \sqrt[3]{3}\zeta, \sqrt[3]{3}\zeta^2\}$. Because σ is not the identity, it must not fix $\sqrt[3]{3}$. We consider two cases:

- $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}\zeta$:

Then $\sqrt[3]{3}\zeta = \sigma(\sqrt[3]{3}) = \sigma h(\sqrt[3]{2}) = h\sigma(\sqrt[3]{2}) = h(\sqrt[3]{2}\zeta)$

$$= a\sqrt[3]{4}\zeta^2 + b\sqrt[3]{2}\zeta + c.$$

Replacing $\sqrt[3]{3}$ by the right hand side of $(*)$, we get

$$(a\sqrt[3]{4} + b\sqrt[3]{2} + c)\zeta = a\sqrt[3]{4}\zeta^2 + b\sqrt[3]{2}\zeta + c.$$

$$\Leftrightarrow a\sqrt[3]{4}\zeta + c\zeta = a\sqrt[3]{4}\zeta^2 + c$$

$$\Leftrightarrow (a\sqrt[3]{4}\zeta - c)(1-\zeta) = 0$$

$$\Leftrightarrow a\sqrt[3]{4}\zeta = c$$

Taking both sides to the power 3, we get $4a^3 = c^3$. Since 4 is not a cubic in $\mathbb{Q}$, we must have $a = c = 0$. Then (*) gives $b = \sqrt[3]{\frac{2}{3}}$.

This is not a rational ~~functo~~ number, so $b \notin \mathbb{Q}$. This is a contradiction.

- $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}\zeta^2$:

Then $\sqrt[3]{3}\zeta^2 = \sigma(\sqrt[3]{3}) = a\sqrt[3]{4}\zeta^2 + b\sqrt[3]{2}\zeta + c$.

Replacing $\sqrt[3]{3}$ by the right hand side of (*), we get

$$(a\sqrt[3]{4} + b\sqrt[3]{2} + c)\zeta^2 = a\sqrt[3]{4}\zeta^2 + b\sqrt[3]{2}\zeta + c$$

$$\Leftrightarrow b\sqrt[3]{2}\zeta^2 + c\zeta^2 = b\sqrt[3]{2}\zeta + c$$

$$\Leftrightarrow [b\sqrt[3]{2}\zeta + c(\zeta+1)](\zeta-1) = 0$$

$$\Leftarrow b\sqrt[3]{2}\zeta + c(\zeta+1) = 0 \quad (**)$$

Since $\zeta^2 + \zeta + 1 = 0$, we have $\zeta + 1 = -\zeta^2$. Thus,

$$(**) \Leftrightarrow b\sqrt[3]{2}\zeta - c\zeta^2 = 0$$

$$\Leftrightarrow b\sqrt[3]{2}\zeta^2 - c\zeta^3 = 0$$

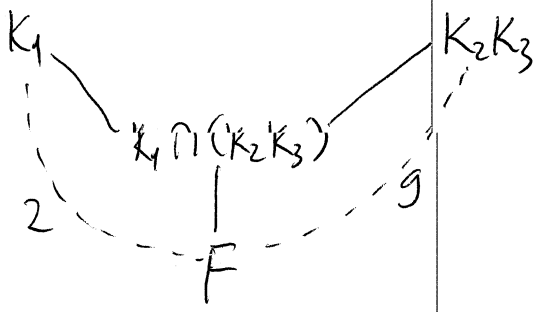
$$\Leftrightarrow b\sqrt[3]{2}\zeta^2 = c$$

Taking both sides ~~by~~ the power 3, we get $2b^3 = c^3$. Since 2 is not a cubic in $\mathbb{Q}$, we get $b = c = 0$. Thus, (*) gives $a = \sqrt[3]{\frac{3}{4}}$. This

is not a rational number. Thus we get a contradiction.

※ Show that $K_1 \cap (K_2K_3) = F$.

Because $K_2 \cap K_3 = F$, $Gal(K_2K_3/F) \simeq Gal(K_2/F) \times Gal(K_3/F)$, which has order $3 \times 3 = 9$. Thus $[K_2K_3 : F] = 9$. By the beside diagram, we see that $[K_1 \cap (K_2K_3) : F]$ divides 2 and 9. Thus it must be 1.



Thus $K_1 \cap (K_2K_3) = F$.

Up to now, we proved that $K_2 \cap K_3 = F$ and $K_1 \cap (K_2K_3) = F$. Note that $K = K_1K_2K_3$. Thus the morphism ϕ is isomorphic. Therefore,

$$G \simeq S_2 \times A_3 \times A_3 \simeq (\mathbb{Z}/2) \times (\mathbb{Z}/3) \times (\mathbb{Z}/3).$$

(m) $X^n - t$ over $\mathbb{C}(t)$, where t is transcendental over $\mathbb{C}$ and n is a positive integer.

First we will show that $X^n - t$ is irreducible over $\mathbb{C}(t)$. Put $A = \mathbb{C}[t]$ and $F = \mathbb{C}(t)$. Then A is a factoral ring and F is a field of fractions of A. Because t is a polynomial of degree 1 in A, it is irreducible. Thus it is a prime of A. By Eisenstein's criterion, $X^n - t$ is irreducible over F.

Let $\alpha = \sqrt[n]{t}$ be a root of $X^n - t$ in $\overline{F}$ and $\zeta = \exp\left(\frac{2\pi i}{n}\right)$

be a primitive n^{th} root of unity. Note that $\zeta \in \mathbb{C} \subset F$.

Then all roots of $X^n - t$ are $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$. Thus, the splitting field of $X^n - t$ is $K = F(\alpha, \alpha\zeta, \ldots, \alpha\zeta^{n-1}) = F(\alpha)$.

Put $G = Gal(K/F)$. Each $\sigma \in G$ permutes the roots of $X^n - t$. Thus, there is a unique $\omega_\sigma \in \mu_n = \{1, \zeta, \ldots, \zeta^{n-1}\}$ such that $\sigma(\alpha) = \alpha\omega_\sigma$. Then we get a map $\phi : G \longrightarrow \mu_n$, $\phi(\sigma) = \omega_\sigma$. We'll show that ϕ is a group isomorphism.

For $\sigma, \tau \in G$, $\sigma\tau(\alpha) = \sigma(\alpha\omega_\tau) = \sigma(\alpha)\sigma(\omega_\tau) = (\alpha\omega_\sigma)\omega_\tau$

($\omega_\tau \in \mathbb{C}$, so it's fixed by σ)

$= \alpha(\omega_\sigma\omega_\tau)$.

Thus, $\phi(\sigma\tau) = \omega_\sigma\omega_\tau = \phi(\sigma)\phi(\tau)$. Thus ϕ is a group homomorphism.

Suppose that $\phi(\sigma) = 1$. Then $\sigma(\alpha) = \alpha$. Thus σ fixes every element of $F(\alpha)$. Thus, $\sigma = id_K$. Hence, ϕ is injective. Now take $\lambda \in \mu_n$ arbitrarily. Then α and $\alpha\lambda$ are roots of $X^n - t$, which is an irreducible polynomial in $F[X]$. Thus there exists $\sigma \in G$ such that $\sigma(\alpha) = \lambda\alpha$. Thus $\phi(\sigma) = \lambda$. Hence, ϕ is surjective. We have proved that ϕ is an isomorphism. Therefore, $G \overset{\phi}{\simeq} \mu_n \simeq \mathbb{Z}/n$.

(4) $X^4 - t$ over $\mathbb{R}(t)$, where t is transcendental over $\mathbb{R}$.

Put $A = \mathbb{R}[t]$ and $F = \mathbb{R}(t)$. Then F is a field of fractions of A. Since t is an irreducible polynomial in $\mathbb{R}[t] = A$, it is a prime of A. By Eisenstein's criterion, $X^4 - t$ is irreducible over F.

Let $\alpha = \sqrt[4]{t}$ be a root of $X^4 - t$ in $\bar{F}$. Then all roots of $X^4 - t$ are $\pm\alpha$ and $\pm i\alpha$. Thus, the splitting field of $X^4 - t$ is

$$K = F(\pm\alpha, \pm i\alpha) = F(\alpha, i).$$

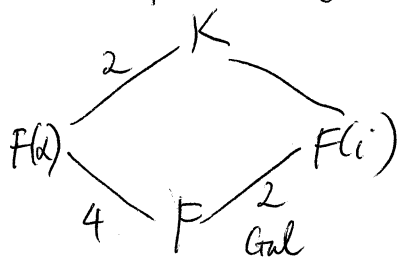
Since α has irreducible polynomial $X^4 - t$, $[F(\alpha) : F] = 4$. Next, suppose by contradiction that $i \in F = \mathbb{R}(t)$. Then there are polynomials $f, g \in \mathbb{R}[t]$, $g \neq 0$ such that $i = \frac{f(t)}{g(t)}$. Then $f(t) - ig(t) = 0$. Thus $f(t)^2 + g(t)^2 = (f(t) - ig(t))(f(t) + ig(t)) = 0$. For each $r \in \mathbb{R}$, we have $f(r)^2 + g(r)^2 = 0$ with $f(r), g(r) \in \mathbb{R}$. Thus $g(r) = 0$. Since g has infinitely many roots in $\mathbb{R}$, $g(t) \equiv 0$. This is a contradiction.

Therefore, $X^2 + 1$ has no root in F. Thus $X^2 + 1$ is the irreducible polynomial of i over F. Thus $[F(i) : F] = 2$. Next, we'll show that $F(i) \cap F(\alpha) = F$. Suppose by contradiction that $F \subsetneq F(i) \cap F(\alpha)$. Then the degree of extension is at least 2. Moreover, $F \subset F(i) \cap F(\alpha) \subset F(i)$

and $[F(i):F]=2$, we must have $F(i)\cap F(\alpha)=F(i)$. Thus $F(i)\subset F(\alpha)$. Thus $i\in F(\alpha)$, which means $i=h(\alpha)$ for some polynomial $h\in F[X]$. Because $h\in \mathbb{R}(t)[X]$, each coefficient of h is a rational function in t. Thus, there are $f\in\mathbb{R}[t,X]$ and $g\in\mathbb{R}[t]\setminus\{0\}$ such that

$$h(X)=\frac{f(t,X)}{g(t)}$$

Therefore, $i=f(t,\alpha)/g(t)$, or equivalently, $f(t,\alpha)-ig(t)=0$. Thus $f(t,\alpha)^2+g(t)^2=\big(f(t,\alpha)-ig(t)\big)\big(f(t,\alpha)+ig(t)\big)=0$. For each $r\in\mathbb{R}$, we have $f(r,\alpha(r))^2+g(r)^2=0$ where $\alpha(r)$ is some element in $\bar{F}$ such that $\alpha(r)^4-r=0$. Since $f(r,\alpha(r)), g(r)\in\mathbb{R}$, we get $g(r)=0$. Thus $g(t)$ has infinitely many roots in $\mathbb{R}$. Thus $g(t)\equiv 0$, which is a contradiction. Therefore, $F(i)\cap F(\alpha)=F$. We get the following diagram.



$$[K:F(\alpha)]=[F(i):F]=2.$$

$$[K:F]=[K:F(\alpha)][F(\alpha):F]=8.$$

Then $[K:F(i)]=\dfrac{[K:F]}{[F(i):F]}=\dfrac{8}{2}=4$.

Because $[K:F(\alpha)]\le \deg(X^4-t)=4$ and $[K:F(\alpha)]\in\deg(X^2+1)=2$, the equalities must happen. Thus X^4-t is irreducible over $F(\alpha)$,

and X^2+1 is irreducible over $F(\alpha)$. Thus there is $\sigma \in Gal(K/F(i))$ such that $\sigma(\alpha) = i\alpha$, and there is $\tau \in Gal(K/F(\alpha))$ such that $\tau(i) = -i$. We have $ord(\sigma) = 4$ and $ord(\tau) = 2$ by the same computation as in part (g), at the bottom of page 4. Also, $\tau \in \langle \sigma \rangle$ because it fixes α but not i. Thus $|G| = [K:F] = 8$ and

$$G = \{\tau\sigma^k : 0 \le k < 4\} \cup \{\sigma^k : 0 \le k < 4\}.$$

By the same computation as in page 5, we have $\tau\sigma = \sigma^3\tau$. Thus,

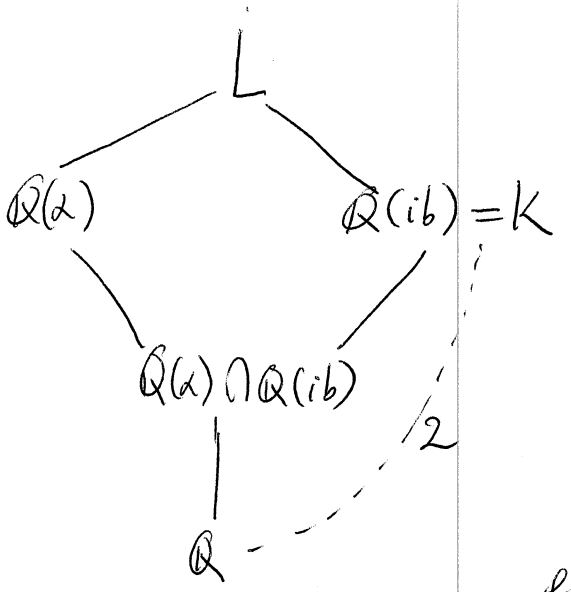
$$G = \langle \sigma, \tau \mid \sigma^4 = id, \tau^2 = id, \tau\sigma = \sigma^3\tau \rangle \simeq D_8.$$

(7) Problem 7, Lang p. 322

(a) Let $a \in \mathbb{Z}$, $a < 0$ and $\mathbb{Q} K = \mathbb{Q}(\sqrt{a})$.

Suppose by contradiction that there is an extension $K \subset L$ such that $\mathbb{Q} \subset L$ is cyclic and $[L:\mathbb{Q}] = 4n$ for some $n \in \mathbb{N}$.

Put $b = \sqrt{-a} > 0$. Then $K = \mathbb{Q}(ib)$. The polynomial $X^2 - a$ has no root in $\mathbb{R}$, so it has no root in $\mathbb{Q}$. Thus $X^2 - a$ is irreducible over $\mathbb{Q}$. It has roots $\pm ib$. Thus $[K:\mathbb{Q}] = \deg(X^2 - a) = 2$. By the Primitive Element theorem, there is $\alpha \in \overline{\mathbb{Q}}$ such that $L = K(\alpha)$. Put $G = Gal(L/\mathbb{Q})$. Then G is cyclic of order $4n$. Let σ be a generator of G.



Since $\mathbb{Q} \subset L$ is an abelian extension, $Gal(L/K)$ is a subgroup of G with index equal to $[K:\mathbb{Q}]=2$. Thus, $Gal(L/K) = \langle \sigma^2 \rangle$.

Thus $\sigma^{2n} \in Gal(L/K)$, which means σ^{2n} fixes everything in K. (*)

Because $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(ib) : \mathbb{Q}]$ divides $[K:\mathbb{Q}]=2$, it can be 1 or 2.

Case 1 $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(ib) : \mathbb{Q}] = 2$

Then $\mathbb{Q}(\alpha) \cap \mathbb{Q}(ib) = K$, which means $K \subset \mathbb{Q}(\alpha)$. Thus $L = \mathbb{Q}(\alpha)$.

We have an automorphism $\tau : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}$, $\tau(z) = \bar{z}$. This is the complex conjugation restricted on $\bar{\mathbb{Q}}$. Note that $\tau^2 = id$. Because $\mathbb{Q} \subset L$ is a normal extension, τ reduces to an automorphism of L over $\mathbb{Q}$. Thus, $\tau|_L$ ~~is a~~ because $\tau(ib) = -ib$, it is not the identity. Since $\tau^2 = id$, it is an element of G of order 2. Thus $\tau|_L = \sigma^{2n}$. Then $\sigma^{2n}(ib) = -ib$.

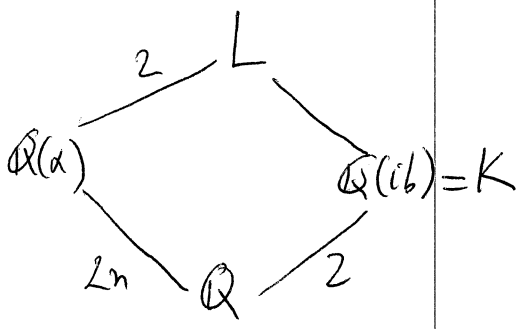
This contradicts (*).

Case 2 $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(ib) : \mathbb{Q}] = 1$

Then $\mathbb{Q}(\alpha) \cap \mathbb{Q}(ib) = \mathbb{Q}$. Because $\mathbb{Q} \subset K$ is Galois, we get the

24

following diagram.



$$[\mathbb{Q}(\alpha):\mathbb{Q}] = \frac{[L:\mathbb{Q}]}{[L:\mathbb{Q}(\alpha)]} = \frac{[L:\mathbb{Q}]}{[K:\mathbb{Q}]} = 2n.$$

Thus, $Gal(L/\mathbb{Q}(\alpha))$ is a subgroup of G with index $2n$. Thus $Gal(L/\mathbb{Q}(\alpha)) = \langle \sigma^{2n} \rangle$.

Thus, $\sigma^{2n} \in Gal(L/\mathbb{Q}(\alpha))$, which mean σ^{2n} fixes everything in $\mathbb{Q}(\alpha)$. Together with (*), we say σ^{2n} fixes everything in $\mathbb{Q}(\alpha, i\sqrt{6}) = L$.

Thus $\sigma^{2n} = id$. This is a contradiction because $ord(\sigma) = 4n$.

(6) $f(X) = X^4 + 30X^2 + 45$.

α is a root of $f(X)$.

$\mathbb{Q}(\alpha)/\mathbb{Q}$ cyclic?

First, we'll show that $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ is Galois. We have $f(X) \in \mathbb{Q}[X]$.

By Eisenstein's criterion with $p = 5$, $f(X)$ is irreducible over $\mathbb{Q}$. The roots of $f(X)$ are $\pm i\sqrt{15+6\sqrt{5}}$ and $\pm i\sqrt{15-6\sqrt{5}}$.

Put $r_1 = i\sqrt{15+6\sqrt{5}}$ and $r_2 = i\sqrt{15-6\sqrt{5}}$. we have

$$\frac{r_1}{r_2} = \frac{\sqrt{15+6\sqrt{5}}}{\sqrt{15-6\sqrt{5}}} = \frac{15+6\sqrt{5}}{\sqrt{15^2-(6\sqrt{5})^2}} = \frac{3\sqrt{5}(\sqrt{5}+2)}{3\sqrt{5}} = \sqrt{5}+2, \quad (*)$$

$$r_1^2 = -15-6\sqrt{5}, \qquad r_2^2 = -15+6\sqrt{5}.$$

Thus $\sqrt{5}+2 = -\frac{3+r_1^2}{6}$ and $\sqrt{5}+2 = \frac{27+r_2^2}{6}$ (**)

From (*) and (**), we get

$$\frac{r_1}{r_2} = -\frac{3+r_1^2}{6} \quad \text{and} \quad \frac{r_1}{r_2} = \frac{27+r_2^2}{6}.$$

Thus $r_2 = -\frac{6r_1}{3+r_1^2}$ and $r_1 = \frac{1}{6} r_2 (27+r_2^2)$.

Therefore, $\mathbb{Q}(r_1) = \mathbb{Q}(r_1, r_2) = \mathbb{Q}(\pm r_1, \pm r_2)$, and similarly

$$\mathbb{Q}(r_2) = \mathbb{Q}(r_1, r_2) = \mathbb{Q}(\pm r_1, \pm r_2).$$

Thus, with any choice of α as a root of $f(X)$, $\mathbb{Q}(\alpha)$ is always the splitting field of $f(X)$. Thus $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ is a normal extension. Moreover, because $\mathrm{char}(\mathbb{Q}) = 0$, it is separable. Thus $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ is Galois.

Put $G = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Then $|G| = \deg f(X) = 4$. We'll show that G is cyclic. WLOG, we can assume $\alpha = r_2$. Put $\omega = \sqrt{5}+2$. By (*), $r_1 = \omega\alpha$. Since $f(X)$ is irreducible, there exists $\sigma \in G$ such that $\sigma(\alpha) = \omega\alpha$. We have $\sigma(r_2) = r_1$. Since σ is a field-isomorphism, $\sigma(-r_2^2) = -r_1^2$.

Thus, $\sigma(15-6\sqrt{5}) = 15+6\sqrt{5}$. Thus, $\sigma(\sqrt{5}) = -\sqrt{5}$. Then

$$\sigma(\omega) = \sigma(\sqrt{5}+2) = -\sqrt{5}+2 = \frac{-1}{\sqrt{5}+2} = \frac{-1}{\omega}.$$

We have $\sigma(\alpha) = \omega\alpha$,

$$\sigma^2(\alpha) = \sigma(\omega\alpha) = \sigma(\omega)\,\sigma(\alpha) = -\frac{1}{\omega}\,\omega\alpha = -\alpha,$$

$$\sigma^3(\alpha) = \sigma(-\alpha) = -\sigma(\alpha) = -\omega\alpha,$$

$$\sigma^4(\alpha) = \sigma(-\omega\alpha) = -\sigma(\omega)\sigma(\alpha) = -\left(-\frac{1}{\omega}\right)\omega\alpha = \alpha.$$

Thus $\sigma^4 = id$. Since $|G| = 4$, we get $G = \{id, \sigma, \sigma^2, \sigma^3\} = \langle\sigma\rangle$.

(c) $f(X) = X^4 + 4X^2 + 2 \in \mathbb{Z}[X]$. By Eisenstein's criterion with $p=2$, $f(X)$ is irreducible over $\mathbb{Q}$. The roots of $f(X)$ are $\pm\alpha, \pm\beta$ where $\alpha = i\sqrt{2-\sqrt{2}}$, $\beta = i\sqrt{2+\sqrt{2}}$. We have

$$\frac{\beta}{\alpha} = \frac{\sqrt{2+\sqrt{2}}}{\sqrt{2-\sqrt{2}}} = \frac{\sqrt{2+\sqrt{2}}^2}{\sqrt{2^2-(\sqrt{2})^2}} = \frac{2+\sqrt{2}}{\sqrt{2}} = 1+\sqrt{2}. \quad (*)$$

Also, $\alpha^2 = -2+\sqrt{2}$. Thus $1+\sqrt{2} = 3+\alpha^2$. Together with $(*)$, we get

$$\beta = (1+\sqrt{2})\alpha = (3+\alpha^2)\alpha.$$

The splitting field of $f(X)$ is $\mathbb{Q}(\pm\alpha, \pm\beta) = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$. Put $G = Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$. Then $|G| = \deg f(X) = 4$. We'll show that G is cyclic. Put $\omega = 1+\sqrt{2}$. By $(*)$, $\beta = \omega\alpha$. Since $f(X)$ is irreducible, there exists $\sigma \in G$ such that $\sigma(\alpha) = \beta = \omega\alpha$. We have

$$\sigma(\alpha^2) = \sigma(\alpha)^2 = \beta^2 \iff \sigma(\sqrt{2}-2) = -\sqrt{2}-2 \iff \sigma(\sqrt{2}) = -\sqrt{2}.$$

Thus $\sigma(\omega) = \sigma(1+\sqrt{2}) = 1-\sqrt{2} = -1/\omega$. Then

$$\sigma(\alpha) = \omega\alpha,$$

$$\sigma^2(\alpha) = \sigma(\omega\alpha) = \sigma(\omega)\sigma(\alpha) = -\frac{1}{\omega}\omega\alpha = -\alpha,$$

$$\sigma^3(\alpha) = \sigma(-\alpha) = -\sigma(\alpha) = -\omega\alpha,$$

$$\sigma^4(\alpha) = \sigma(-\omega\alpha) = -\sigma(\omega)\sigma(\alpha) = -\left(-\frac{1}{\omega}\right)\omega\alpha = \alpha.$$

Thus $\sigma^4 = id$. Since $|G| = 4$, we obtain $G = \{id, \sigma, \sigma^2, \sigma^3\} = \langle\sigma\rangle$.

③ Problem 8, Lang p. 322

Let $f(X) = X^4 + aX^2 + b$ with $a, b \in \mathbb{Q}$ be an irreducible polynomial over $\mathbb{Q}$. Let $\pm\alpha, \pm\beta$ be the roots of $f(X)$. Put $K = \mathbb{Q}(\pm\alpha, \pm\beta)$ and $G = \mathrm{Gal}(K/\mathbb{Q})$.

(a) We'll show that G is isomorphic to a subgroup of D_8.

Because $\mathrm{char}\,\mathbb{Q} = 0$ and $f(X)$ is irreducible over $\mathbb{Q}$, it is a separable polynomial. Thus $\alpha, \beta, -\alpha, -\beta$ are distinct. Let us label $\alpha, \beta, -\alpha, -\beta$ by $1, 2, 3, 4$ in this order and denote by S_4 the group of permutations of these numbers. Each $\sigma \in G$ permutes the roots of $f(X)$. Moreover, σ is uniquely determined by its values on $(\alpha, \beta, -\alpha, -\beta)$. Thus there is an injective group homomorphism $\phi: G \to S_4$ which maps σ to the 4-tuple of labels in $\{1,2,3,4\}$ of $(\sigma(\alpha), \sigma(\beta), \sigma(-\alpha), \sigma(-\beta))$.

Put $\lambda = (1\,2)(3\,4)$ and $\rho = (1\,2\,3\,4)$. These elements of S_4 satisfy

$$\lambda^2 = \mathrm{id}, \quad \rho^4 = \mathrm{id},$$

$$\lambda\rho = (12)(34)(1234) = (24),$$

$$\rho^3\lambda = (4321)(12)(34) = (24).$$

Thus $\lambda\rho = \rho^3\lambda$. This means $\langle \lambda, \rho \rangle$ is a subgroup of S_4 that is isomorphic to D_8. Our goal is to show that $\phi(G) \subset \langle \lambda, \rho \rangle$.

28

Take $\sigma \in G$ arbitrarily. We'll show that $\phi(\sigma) \in \langle \lambda, \rho \rangle$. We know that $\sigma(\alpha) \in \{\pm\alpha, \pm\beta\}$. Also, since $\beta \neq \pm\alpha$, $\sigma(\beta) \neq \pm\sigma(\alpha)$. There are 4 cases as follow.

- $\underline{\sigma(\alpha) = \alpha}$ Then $\sigma(\beta) \neq \pm\alpha$, so $\sigma(\beta) = \pm\beta$.

  If $\sigma(\beta) = \beta$ then $\sigma = id$. If $\sigma(\beta) = -\beta$ then

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

  Then $\phi(\sigma) = (2\ 4) = \lambda\rho$.

- $\underline{\sigma(\alpha) = -\alpha}$ Then $\sigma(\beta) \neq \pm\alpha$, so $\sigma(\beta) = \pm\beta$.

  If $\sigma(\beta) = -\beta$ then $(\sigma(\alpha), \sigma(\beta), \sigma(-\alpha), \sigma(-\beta)) = (-\alpha, -\beta, \alpha, \beta)$.

  Then $\phi(\sigma) = (1\ 3)(2\ 4) = \rho^2$.

  If $\sigma(\beta) = \beta$ then $(\sigma(\alpha), \sigma(\beta), \sigma(-\alpha), \sigma(-\beta)) = (-\alpha, \beta, \alpha, -\beta)$. #

  Then $\phi(\sigma) = (1\ 3) = \lambda\rho^3$.

- $\underline{\sigma(\alpha) = \beta}$ Then $\sigma(\beta) \neq \pm\beta$, so $\sigma(\beta) = \pm\alpha$.

  If $\sigma(\beta) = \alpha$ then $(\sigma(\alpha), \sigma(\beta), \sigma(-\alpha), \sigma(-\beta)) = (\beta, \alpha, -\beta, -\alpha)$.

  Then $\phi(\sigma) = (1\ 2)(3\ 4) = \lambda$.

  If $\sigma(\beta) = -\alpha$ then $(\sigma(\alpha), \sigma(\beta), \sigma(-\alpha), \sigma(-\beta)) = (\beta, -\alpha, -\beta, \alpha)$.

  Then $\phi(\sigma) = (1\ 2\ 3\ 4) = \rho$.

- $\underline{\sigma(\alpha) = -\beta}$ Then $\sigma(\beta) \neq \pm\beta$, so $\sigma(\beta) = \pm\alpha$.

  If $\sigma(\beta) = \alpha$ then $(\sigma(\alpha), \sigma(\beta), \sigma(-\alpha), \sigma(-\beta)) = (-\beta, \alpha, \beta, -\alpha)$.

  Then $\phi(\sigma) = (1\ 4\ 3\ 2) = \rho^3$.

If $\sigma(\beta) = -\alpha$ then $(\sigma(\alpha), \sigma(\beta), \sigma(-\alpha), \sigma(-\beta)) = (-\beta, -\alpha, \beta, \alpha)$.

Then $\phi(\sigma) = (1\,4)(2\,3) = \lambda\rho^2$. Therefore, we proved that $\phi(\sigma) \in \langle \lambda, \rho \rangle$.

We have $\langle \lambda, \rho \rangle = \{id, \rho, \rho^2, \rho^3, \lambda, \lambda\rho, \lambda\rho^2, \lambda\rho^3\}$. We can enumerate all subgroups of $\langle \lambda, \rho \rangle$ as follow.

- Subgroup of order 1 is $\{id\}$.
- Subgroups of order 2 are $\{id, \lambda\}$, $\{id, \rho^2\lambda\}$, $\{id, \rho^2\}$, $\{id, \rho\lambda\}$, $\{id, \rho^3\lambda\}$.
- Subgroups of order 4 are

$H_1 = \{id, \rho^2, \lambda, \rho^2\lambda\} \simeq (\mathbb{Z}/2) \times (\mathbb{Z}/2)$,

(because all elements bgt id have order 2)

$H_2 = \{id, \rho, \rho^2, \rho^3\} \simeq \mathbb{Z}/4$,

(because this is a cyclic group)

$H_3 = \{id, \rho^2, \rho\lambda, \rho^3\lambda\} \simeq (\mathbb{Z}/2) \times (\mathbb{Z}/2)$,

(because all elements but id have order 2).

- Subgroup of order 8 is $H = \langle \lambda, \rho \rangle \simeq D_8$.

Because $f(X)$ is irreducible over $\mathbb{Q}$, $|G|$ is divisible by $\deg f(X) = 4$.

Thus $\phi(G)$ can be H_1, H_2, H_3 or H. Therefore, $G \simeq \mathbb{Z}/4$ or $(\mathbb{Z}/2)\times(\mathbb{Z}/2)$ or D_8.

(b) Put $r = \frac{\alpha}{\beta} - \frac{\beta}{\alpha}$ (note that $\alpha, \beta \neq 0$ because $\alpha \neq -\alpha$, $\beta \neq -\beta$).

30

We'll show that $G \simeq \mathbb{Z}/4$ if and only if $r \in \mathbb{Q}$. It is true that

$$G \simeq \mathbb{Z}/4 \iff \phi(G) = H_2$$

Suppose that $\phi(G) = H_2$. We'll show $r \in \mathbb{Q}$. Put $\sigma = \phi^{-1}(\beta)$. Then $\sigma(\alpha) = \beta$ and $\sigma(\beta) = -\alpha$. Then $G = \langle \phi^{-1}(\beta) \rangle = \langle \sigma \rangle$.

$$\sigma\left(\frac{\alpha}{\beta}\right) = \frac{\sigma(\alpha)}{\sigma(\beta)} = \frac{-\beta}{\alpha}, \qquad \sigma\left(\frac{\beta}{\alpha}\right) = \sigma\left(\frac{\alpha}{\beta}\right)^{-1} = -\frac{\alpha}{\beta}$$

Thus, $\sigma(r) = \sigma\left(\frac{\alpha}{\beta}\right) - \sigma\left(\frac{\beta}{\alpha}\right) = \left(-\frac{\beta}{\alpha}\right) - \left(-\frac{\alpha}{\beta}\right) = r$. Thus r is fixed by σ. Thus r is fixed by every automorphism in G. Thus $r \in \mathbb{Q}$.

Conversely, suppose that $r \in \mathbb{Q}$. We'll show $\phi(G) = H_2$. Since α and β are roots of an irreducible polynomial $f(X)$ over $\mathbb{Q}$, there exists $\sigma \in G$ such that $\sigma(\alpha) = \beta$. Because $\sigma(\beta) \neq \pm\sigma(\alpha)$, $\sigma(\beta) = \pm\alpha$. If $\sigma(\beta) = \alpha$ then $r = \sigma(r) = \frac{\sigma(\alpha)}{\sigma(\beta)} - \frac{\sigma(\beta)}{\sigma(\alpha)} = \frac{\beta}{\alpha} - \frac{\alpha}{\beta} = -r$; then $r = 0$, which means $(\alpha^2 - \beta^2)/(\alpha\beta) = 0$, which means $\alpha = \pm\beta$. This is impossible. Thus, $\sigma(\beta) = -\alpha$. Then by definition of ϕ, $\phi(\sigma) = (1\,2\,3\,4) = \rho$. Thus, $\rho \in \phi(G)$. Thus $H_2 = \langle \rho \rangle \subset \phi(G)$. Suppose by contradiction that $\phi(G) = H$. Put $\tau = \phi^{-1}(\lambda)$. Then $\tau(\alpha) = \beta$ and $\tau(\beta) = \alpha$. We have

$$r = \tau(r) = \frac{\tau(\alpha)}{\tau(\beta)} - \frac{\tau(\beta)}{\tau(\alpha)} = \frac{\beta}{\alpha} - \frac{\alpha}{\beta} = -r$$

This is a contradiction. Thus, $H_2 \subset \phi(G) \subsetneq H$. Thus $\phi(G) = H_2$.

Next, we'll show that $\phi(G) = H_1 \Leftrightarrow \alpha\beta \in \mathbb{Q}$.

Suppose that $\phi(G) = H_1 = \{id, \rho^2, \lambda, \rho^2\lambda\}$. Put $\sigma = \phi^{-1}(\rho^2)$ and $\tau = \phi^{-1}(\lambda)$. Then $G = \{id, \sigma, \tau, \sigma\tau\}$. We have

$$\sigma = \phi^{-1}((13)(24)), \text{ so } \sigma(\alpha) = -\alpha, \ \sigma(\beta) = -\beta,$$

$$\tau = \phi^{-1}((12)(34)), \text{ so } \tau(\alpha) = \beta, \ \tau(\beta) = \alpha.$$

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

$\tau(\alpha\beta) = \tau(\alpha)\tau(\beta) = \beta\alpha = \alpha\beta$,

$\sigma\tau(\alpha\beta) = \sigma(\alpha\beta) = \alpha\beta$.

Thus, $\alpha\beta$ is fixed by everything in G. Thus, $\alpha\beta \in \mathbb{Q}$.

Conversely, suppose that $\alpha\beta \in \mathbb{Q}$. Since α and β are two roots of an irreducible polynomial $f(X)$ in $\mathbb{Q}[X]$, there exists $\tau \in G$ such that $\tau(\alpha) = \beta$. Then $\tau(\beta) = \dfrac{\tau(\alpha\beta)}{\tau(\alpha)} = \dfrac{\alpha\beta}{\beta} = \alpha$.

Now that $\tau(\alpha) = \beta$ and $\tau(\beta) = \alpha$, $\phi(\tau) = \lambda$. Thus $\lambda \in \phi(G)$. Thus, there are only two possibilities: $\phi(G) = H_1$ or $\phi(G) = H$. Suppose by contradiction that $\phi(G) = H$. Put $\tau' = \phi^{-1}(\rho) = \phi^{-1}((1\,2\,3\,4))$. Then $\tau'(\alpha) = \beta$ and $\tau'(\beta) = -\alpha$. Then $\tau'(\beta) = \dfrac{\tau'(\alpha\beta)}{\tau'(\alpha)} = \dfrac{\alpha\beta}{\beta} = \alpha$,

which is a contradiction. Thus, $\phi(G) = H_1$.

Next, we'll show that $\alpha^2 - \beta^2 \notin \mathbb{Q}$. Suppose by contradiction that

$\alpha^2-\beta^2 \in \mathbb{Q}$. Since α and β are two roots of an irreducible $f(X)$ in $\mathbb{Q}[X]$, there is $\tau \in G$ such that $\tau(\alpha)=\beta$. Because $\tau(\beta) \neq \pm\tau(\alpha)$, $\tau(\beta)=\pm\alpha$. Then $\tau(\alpha^2-\beta^2)=\tau(\alpha)^2-\tau(\beta)^2=\beta^2-\alpha^2=-(\alpha^2-\beta^2) \neq \alpha^2-\beta^2$. This contradicts the assumption $\alpha^2-\beta^2 \in \mathbb{Q}$.

Next, we will show that $\phi(G)$ is never equal to H_3. Suppose by contradiction that $\phi(G)=H_3=\{id, \rho^2, \rho\lambda, \rho^3\lambda\}$. Put $\sigma=\phi^{-1}(\rho^2)$ and $\tau=\phi^{-1}(\rho\lambda)$. Then $G=\{id, \sigma, \tau, \sigma\tau\}$, we have

$$\sigma=\phi^{-1}((13)(24)), \text{ so } \sigma(\alpha)=-\alpha \text{ and } \sigma(\beta)=-\beta,$$

$$\tau=\phi^{-1}((13)), \text{ so } \tau(\alpha)=-\alpha \text{ and } \tau(\beta)=\beta.$$

Then $\sigma(\alpha^2-\beta^2)=\sigma(\alpha)^2-\sigma(\beta)^2=\alpha^2-\beta^2$,

$\tau(\alpha^2-\beta^2)=\tau(\alpha)^2-\tau(\beta)^2=\alpha^2-\beta^2$,

$\sigma\tau(\alpha^2-\beta^2)=\sigma(\alpha^2-\beta^2)=\alpha^2-\beta^2$.

Thus $\alpha^2-\beta^2$ is fixed by everything in G. Thus $\alpha^2-\beta^2 \in \mathbb{Q}$. This contradicts a fact we have just proved.

In conclusion, there are only 3 possibilities:

(i) $G \simeq \mathbb{Z}/4 \Leftrightarrow \phi(G)=H_2 \Leftrightarrow \frac{\alpha}{\beta}-\frac{\beta}{\alpha} \in \mathbb{Q}$,

(ii) $G \simeq (\mathbb{Z}/2)\times(\mathbb{Z}/2) \Leftrightarrow \phi(G)=$ "H_1 or "$H_3 \Leftrightarrow$ "$\phi(G)=$"$H_1 \Leftrightarrow \alpha\beta \in \mathbb{Q}$,

(iii) $G \simeq D_8 \Leftrightarrow \frac{\alpha}{\beta}-\frac{\beta}{\alpha} \notin \mathbb{Q}$ and $\alpha\beta \notin \mathbb{Q}$.

(c) $f(X) = X^4 - 4X^2 - 1$.

Let K be the splitting field of $f(X)$ over $\mathbb{Q}$ and G be the Galois group. First, we'll describe G and all of its subgroups.

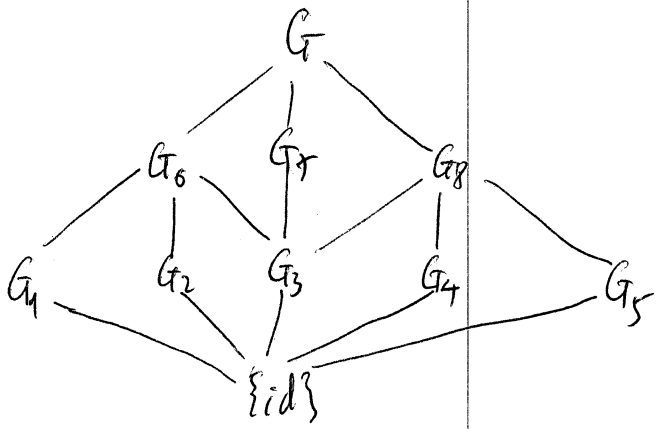
We'll show that $f(X)$ is irreducible over $\mathbb{Q}$. Because $f(\pm 1) \neq 0$, f has no root in $\mathbb{Q}$. Suppose that $f(X)$ is reducible over $\mathbb{Q}$. Since $f \in \mathbb{Z}[X]$ and monic, it is reducible in $\mathbb{Z}[X]$. Then there are a, b, c, d in $\mathbb{Z}$ such that $f(X) = (X^2 + aX + b)(X^2 + cX + d)$. Then

$$\begin{cases} a + c = 0 \\ b + d + ac = -4 \\ ad + bc = 0 \\ bd = -1 \end{cases} \qquad \text{Therefore,} \qquad \begin{cases} a = -c \\ b + d - a^2 = -4 \\ a(b - d) = 0 \\ bd = -1 \end{cases}$$

Since $bd = -1 < 0$, $b \neq d$. Then the third equation implies $a = 0$. Then $b + d = -4$ and $bd = -1$. Then we try $b, d = \pm 1$ into the equation $b + d = -4$. None of these cases work. Thus $f(X)$ is irreducible in $\mathbb{Q}[X]$.

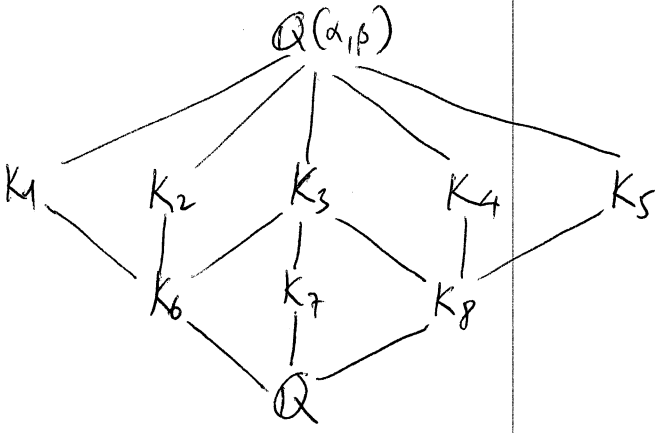
$f(X)$ has four roots $\pm\alpha, \pm\beta$ with $\alpha = \sqrt{\sqrt{5} - 2}$ and $\beta = i\sqrt{\sqrt{5} + 2}$. By simple computation, we have $\alpha\beta = i \notin \mathbb{Q}$, $\alpha/\beta - \beta/\alpha = -2i\sqrt{5} \notin \mathbb{Q}$. Thus, by part (b), $\phi(G) = H = \langle \lambda, \rho \rangle$. Put $\sigma = \phi^{-1}(\rho)$ and $\tau = \phi^{-1}(\lambda)$. Then $G = \{ id, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau \}$. Because we enumerated all subgroups of H, we have the list of subgroups of G as follow.

- Order 1: $\{id\}$.
- Order 2: $G_1=\{id,\tau\}$, $G_2=\{id,\sigma^2\tau\}$, $G_3=\{id,\sigma^2\}$, $G_4=\{id,\sigma\tau\}$, $G_5=\{id,\sigma^3\tau\}$.
- Order 4: $G_6=\{id,\sigma^2,\tau,\sigma^2\tau\}$,
  $G_7=\{id,\sigma,\sigma^2,\sigma^3\}$,
  $G_8=\{id,\sigma^2,\sigma\tau,\sigma^3\tau\}$.
- Order 8: G.



The index of a layer in the immediate upper layer is 2.

Put $K_i = K^{G_i}$ - the intermediate field that is fixed by G_i. Then we get an upside down diagram;



The degree of extension between two consecutive layers is 2.

By definition, $\sigma(\alpha)=\beta$, $\sigma(\beta)=-\alpha$ and $\tau(\alpha)=\beta$, $\tau(\beta)=\alpha$.

Then we obtain a chart of images of automorphisms in G at special values as follow.

	α	β	$\alpha\beta$	$\alpha^2-\beta^2$	$\alpha/\beta-\beta/\alpha$
id	α	β	$\alpha\beta$	$\alpha^2-\beta^2$	$\alpha/\beta-\beta/\alpha$
σ	β	$-\alpha$	$-\alpha\beta$	$\beta^2-\alpha^2$	$-\beta/\alpha+\alpha/\beta$
σ^2	$-\alpha$	$-\beta$	$\alpha\beta$	$\alpha^2-\beta^2$	$\alpha/\beta-\beta/\alpha$
σ^3	$-\beta$	α	$-\alpha\beta$	$\beta^2-\alpha^2$	$-\beta/\alpha+\alpha/\beta$
τ	β	α	$\alpha\beta$	$\beta^2-\alpha^2$	$\beta/\alpha-\alpha/\beta$
$\sigma\tau$	$-\alpha$	β	$-\alpha\beta$	$\alpha^2-\beta^2$	$-\alpha/\beta+\beta/\alpha$
$\sigma^2\tau$	$-\beta$	$-\alpha$	$\alpha\beta$	$\beta^2-\alpha^2$	$\beta/\alpha-\alpha/\beta$
$\sigma^3\tau$	α	$-\beta$	$-\alpha\beta$	$\alpha^2-\beta^2$	$-\alpha/\beta+\beta/\alpha$

From the chart, we see that α is fixed by $G_5=\{id, \sigma^3\tau\}$. Thus $\mathbb{Q}(\alpha)\subset K_5$. Since $[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg f(X)=4$, $\mathbb{Q}(\alpha)=K_5$.

Similarly, β is fixed by $G_4=\{id, \sigma\tau\}$. Thus $\mathbb{Q}(\beta)\subset K_4$. Since $[\mathbb{Q}(\beta):\mathbb{Q}]=\deg f(X)=4$, $\mathbb{Q}(\beta)=K_4$.

From the chart, we see that $\alpha+\beta$ is fixed by $G_1=\{id, \tau\}$. Thus $\mathbb{Q}(\alpha+\beta)\subset K_1$. Since $\alpha+\beta$ is not fixed by σ^2, $\alpha+\beta\notin K_6$. Thus $[\mathbb{Q}(\alpha+\beta):\mathbb{Q}]>[K_6:\mathbb{Q}]=2$. Thus $[\mathbb{Q}(\alpha+\beta):\mathbb{Q}]=4$ and hence $\mathbb{Q}(\alpha+\beta)=K_1$.

From the chart, $\alpha-\beta$ is fixed by $G_2=\{id, \sigma^2\tau\}$. Thus, $\mathbb{Q}(\alpha-\beta)\subset K_2$. Since $\alpha-\beta$ is not fixed by σ^2, $\alpha-\beta\notin K_6$. Thus, $[\mathbb{Q}(\alpha-\beta):\mathbb{Q}]>[K_6:\mathbb{Q}]=2$. Thus $[\mathbb{Q}(\alpha-\beta):\mathbb{Q}]=4$ and hence $\mathbb{Q}(\alpha-\beta)=K_2$.

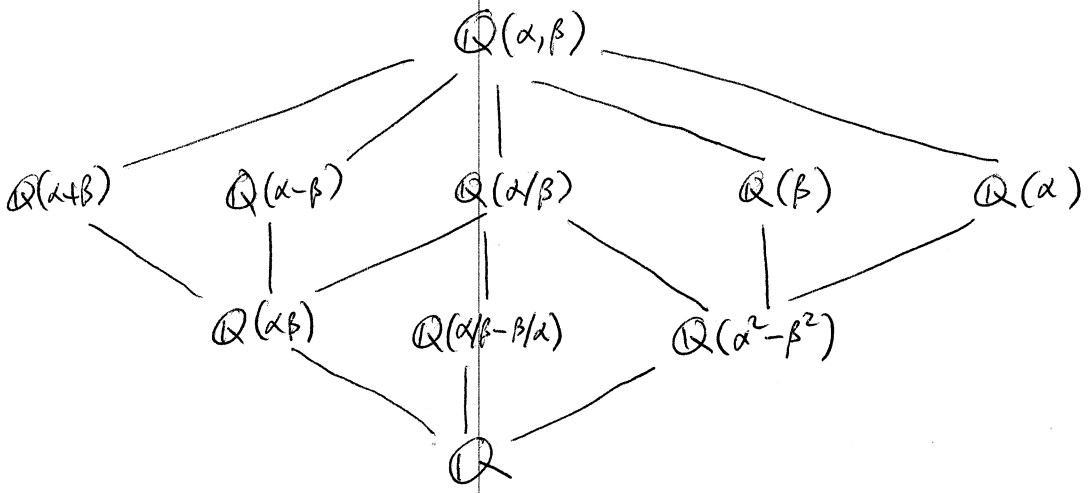
From the chart, α/β is fixed by $G_5 = \{id, \sigma^2\}$. Thus $\mathbb{Q}(\alpha/\beta) \subset K_5$. Since α/β is not fixed by $\sigma^2\tau$, $\alpha/\beta \notin K_6$. Thus $[\mathbb{Q}(\alpha/\beta) : \mathbb{Q}] > [K_6 : \mathbb{Q}] = 2$. Thus $[\mathbb{Q}(\alpha/\beta) : \mathbb{Q}] = 4$. Thus $\mathbb{Q}(\alpha/\beta) = K_6$.

From the chart, $\alpha\beta$ is fixed by $G_6 = \{id, \sigma^2, \tau, \sigma^2\tau\}$. Thus $\mathbb{Q}(\alpha\beta) \subset K_6$. Since $\alpha\beta \notin \mathbb{Q}$, $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] \geq 2$. Thus the equality must happen and $\mathbb{Q}(\alpha\beta) = K_6$.

From the chart, $\alpha^2 - \beta^2$ is fixed by $G_8 = \{id, \sigma^2, \sigma\tau, \sigma^3\tau\}$. Thus, $\mathbb{Q}(\alpha^2 - \beta^2) \subset K_8$. Since $\alpha^2 - \beta^2 = 2\sqrt{5} \notin \mathbb{Q}$, $[\mathbb{Q}(\alpha^2 - \beta^2) : \mathbb{Q}] \geq 2$. Thus, the equality must happen and $\mathbb{Q}(\alpha^2 - \beta^2) = K_8$.

From the chart, $\alpha/\beta - \beta/\alpha$ is fixed by $G_7 = \{id, \sigma, \sigma^2, \sigma^3\}$. Thus, $\mathbb{Q}(\alpha/\beta - \beta/\alpha) \subset K_7$. Since $\alpha/\beta - \beta/\alpha \notin \mathbb{Q}$, $[\mathbb{Q}(\alpha/\beta - \beta/\alpha) : \mathbb{Q}] \geq 2$. Thus, the equality must happen and $\mathbb{Q}(\alpha/\beta - \beta/\alpha) = K_7$.

Therefore, there are 10 intermediate fields between $\mathbb{Q}$ and $K = \mathbb{Q}(\alpha, \beta)$.



(4) Problem 9, Lang p. 322

Let p be a prime number, $f(X) \in k[X]$ be an irreducible polynomial over k with degree p. Let $\theta_1, \theta_2, \dots, \theta_p \in \bar{k}$ be the roots of $f(X)$ and $K = k(\theta_1)$. Suppose that $k \subset K$ is separable and $\theta_2 \in K$. We'll show that $k \subset K$ is normal.

Since θ_1 is separable over k, its irreducible polynomial is sparable. Thus, $f(X)$ is separable. Put $L = k(\theta_1, \theta_2, \dots, \theta_p)$ - the splitting field of $f(X)$. Then $k \subset L$ is Galois. Put $G = Gal(L/k)$.

Each $\sigma \in G$ permutes the roots of $f(X)$. Thus, if we label $\theta_1, \theta_2, \dots, \theta_p$ by $1, 2, \dots, p$ in this order, we will get an injective group homomorphism $\phi : G \to S_p$. Since $f(X)$ is irreducible, $|G|$ is divisible by $\deg f = p$. By Cauchy's theorem, G has an element of order p, say σ. Then $\phi(\sigma)$ is a p-cycle, say $s = [1\ i_2\ i_3 \dots i_p] = [1\ s(1)\ s^2(1) \dots s^{p-1}(1)]$. Equivalently, $(\theta_1, \theta_{i_2}, \dots, \theta_{i_p}) = (\theta_1, \sigma(\theta_1), \dots, \sigma^{p-1}(\theta_1))$.

By ~~considering~~ replacing σ by another power of σ if necessary, we can assume $\sigma(\theta_1) = \theta_2$. Then $\sigma(\theta_1) \in K$. Since $K = k(\theta_1)$, $\sigma(K) \subset K$. Thus, $\{\theta_1, \theta_2, \dots, \theta_p\} = \{\theta_1, \sigma(\theta_1), \dots, \sigma^{p-1}(\theta_1)\} \subset K$.

BP

Therefore $L = K$, and K is normal over k. The Galois group $G = Gal(K/k) = Gal(k(\theta_1)/k)$ has order equal to $\deg f(X) = p$. Thus, G is a cyclic group.

(5) Problem 10, Lang p 322.

Let $f(X) \in \mathbb{Q}[X]$ with degree $= n > 2$. Let K be the splitting field of $f(X)$ over $\mathbb{Q}$. Suppose that $G = Gal(K/\mathbb{Q}) \simeq S_n$.

(a) We'll show that $f(X)$ is irreducible over $\mathbb{Q}$.

Suppose by contradiction that $f(X)$ is reducible over $\mathbb{Q}$. Then there are $g, h \in \mathbb{Q}[X]$ with $1 \leq \deg g, \deg h \leq n-1$ and $f(X) = g(X)h(X)$. Let $\alpha_1, \dots, \alpha_\ell \in \bar{\mathbb{Q}}$ be the distinct roots of $g(X)$ and $\beta_1, \dots, \beta_s \in \bar{\mathbb{Q}}$ be the distinct roots of $h(X)$. Then $\ell, s \geq 1$ and $\ell + s \leq n$.

Because $K = \mathbb{Q}(\alpha_1, \dots, \alpha_\ell, \beta_1, \dots, \beta_s)$, each $\sigma \in G$ is uniquely determined by its values on $(\alpha_1, \dots, \alpha_\ell, \beta_1, \dots, \beta_s)$. Because $g, h \in \mathbb{Q}[X]$, σ permutes the roots of $g(X)$, and permutes the roots of $h(X)$ as well. Thus σ permutes $(\alpha_1, \dots, \alpha_\ell)$ and permutes $(\beta_1, \dots, \beta_s)$. The maximum possible number of such σ's is $\ell!\, s!$ We have

$$\ell!\, s! \leq \ell!(n-\ell)! = \frac{n!}{\binom{n}{\ell}} < n! \qquad (\text{since } 1 \leq \ell \leq n-1)$$

Thus $|G| < n!$ which is a contradiction.

(b) Let α be a root of $f(X)$ and τ be an automorphism of $\mathbb{Q}(\alpha)$. We'll show that $\tau = id$.

First, because $\tau(1) = 1$, $\tau(m) = m$ for all $m \in \mathbb{Z}$. Thus, $\tau\left(\frac{m}{n}\right) = \frac{m}{n}$ for all $m, n \in \mathbb{Z}$, $n \neq 0$. Thus τ fixes everything in $\mathbb{Q}$. Since $f(X) \in \mathbb{Q}[X]$, $\tau(\alpha) = \beta$ is also a root of $f(X)$. If $\beta = \alpha$ then $\tau = id$. Suppose by contradictim that $\beta \neq \alpha$. Let $c_1, c_2, \dots, c_{n-2}$ be the other roots of $f(X)$. WLOG, we can assume that $f(X)$ is a monic polynomial. Then

$$f(X) = \underbrace{(X-\alpha)(X-\beta)}_{g(X)} \underbrace{(X-c_1)\cdots(X-c_{n-2})}_{h(X)}.$$

Since $\beta \in \mathbb{Q}(\alpha)$, both $f(X)$ and $g(X)$ are in $\mathbb{Q}(\alpha)[X]$. Thus $h(X)$ is the quotient of $f(X)$ by $g(X)$ of a division in $\mathbb{Q}(\alpha)[X]$. Then $K = \mathbb{Q}(\alpha, \beta, c_1, \dots, c_{n-2}) = \mathbb{Q}(\alpha)(c_1, \dots, c_{n-2})$ is the splitting field of $h(X)$ over $\mathbb{Q}(\alpha)$. Put $G' = Gal(K/\mathbb{Q}(\alpha))$. Each $\sigma \in G'$ permutes the roots of $h(X)$ and is uniquely determined by its values on $(c_1, \dots, c_{n-2})$. Thus $|G'| \leq (n-2)!$ Then

$$[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = |G'| \deg f(X) \leq (n-2)!\, n = \frac{n!}{n-1}.$$

Since $n > 2$, $[K:\mathbb{Q}] < n!$ This is a contradiction.

(c) Let α be a root of $f(X)$. Suppose that $n \geq 4$. We'll show $\alpha^n \notin \mathbb{Q}$.

Suppose by contradiction that $\alpha^n = a \in \mathbb{Q}$. Then α is a root of $X^n - a \in \mathbb{Q}[X]$. Thus $f(X) \mid (X^n - a)$. Since $f(X)$ has degree n and can be assumed to be monic, $f(X) = X^n - a$.

Let $\zeta \in \bar{\mathbb{Q}}$ be a primitive n'th root of unity. Then all roots of $f(X)$ are $\alpha, \alpha\zeta, \dots, \alpha\zeta^{n-1}$. Put $F = \mathbb{Q}(\zeta)$. Then

$$K = \mathbb{Q}(\alpha, \alpha\zeta, \dots, \alpha\zeta^{n-1}) = \mathbb{Q}(\alpha, \zeta) = F(\alpha)$$

Thus, $[K : \mathbb{Q}] = [F(\alpha) : F][\mathbb{Q}(\zeta) : \mathbb{Q}]$ (*).

Since $f(X) \in F[X]$ and $f(\alpha) = 0$, the irreducible polynomial of α over F divides $f(X)$. Thus $[F(\alpha) : F] \leq \deg f(X) = n$. Since ζ is a root of $X^n - 1 \in \mathbb{Q}[X]$, the irreducible polynomial of ζ over $\mathbb{Q}$ divides $X^n - 1$. Thus $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq n$. Therefore, from (*) we get $[K : \mathbb{Q}] \leq n^2$.

Because $n \geq 4$, $n! = 1.2 \cdots (n-1)n \geqslant 2(n-1)n = [n + (n-2)]n > n^2 \geqslant [K : \mathbb{Q}]$

This is a contradiction.

⑥ Problem 15, Lang p. 323.

Let $k \subset K$ be a Galois extension and F be an intermediate field. Put

$$G = \mathrm{Gal}(K/k),$$

$$H = \{\sigma \in G : \sigma(F) = F\},$$

$$L = \mathrm{Gal}(K/F)$$

We'll show that $H = N_L$ - the normalizer of L in G.

First, we show that H is a subgroup of G. Since $id_K \in H$, $H \neq \emptyset$. For $\sigma, \tau \in H$, $\sigma\tau(F) \subseteq \sigma(F) = F$. Thus $\sigma\tau \in H$. Also, $\sigma(F) = F$ implies $F = \sigma^{-1}(F)$. Thus $\sigma^{-1} \in H$. Thus $H < G$.

Show $H \subset N_L$: let $\sigma \in H$. We need to show $\sigma L \sigma^{-1} = L$. First, we will show $\sigma L \sigma^{-1} \subset L$. Take $\tau \in L$ arbitrarily. For each $x \in F$, $\sigma^{-1}(x)$ is in F. Thus $\sigma^{-1}(x)$ is fixed by τ. Thus $\sigma\tau\sigma^{-1}(x) = \sigma\sigma^{-1}(x) = x$. Thus $\sigma\tau\sigma^{-1}$ fixes everything in F. Thus $\sigma\tau\sigma^{-1} \in L$. Next, we'll show that $L \subset \sigma L \sigma^{-1}$. Because we proved that $\lambda L \lambda^{-1} \subset L$ for all $\lambda \in H$, we can take $\lambda = \sigma^{-1} \in H$ and get $\sigma^{-1} L \sigma \subset L$. Then $L \subset \sigma L \sigma^{-1}$.

Show $N_L \subset H$ let $\sigma \in N_L$, which means $\sigma L \sigma^{-1} = L$. We'll show that $\sigma \in H$, which means $\sigma(F) = F$. First, we'll show that $\sigma^{-1}(F) \subset F$. Take $x \in F$ arbitrarily. ~~To show that $\sigma(x) \in F$ is equivalent to show that $\sigma(x)$ is fixed by everything in L.~~ Take $\tau \in L$ arbitrarily. Then $\sigma\tau\sigma^{-1} \in L$. Thus it fixes x, which means $\sigma\tau\sigma^{-1}(x) = x$. Thus $\tau\sigma^{-1}(x) = \sigma^{-1}(x)$. Thus $\sigma^{-1}(x)$ is fixed by everything in L. Thus $\sigma^{-1}(x) \in F$. Thus $\sigma^{-1}(F) \subset F$. So far, we proved that $\lambda^{-1}(F) \subset F$ for all $\lambda \in N_L$. Take $\lambda = \sigma$, we get $\sigma(F) \subset F$. Therefore, $\sigma(F) = F$.

⑦ Problem 18, Lang p. 323.

(a) Let a be a square-free integer. We want to determine all roots of unity in $\mathbb{Q}(\sqrt{a})$. First, because $\sqrt{a} \notin \mathbb{Q}$ and $\pm\sqrt{a}$ are roots of $X^2 - a$, this polynomial is irreducible over $\mathbb{Q}$. Thus,

$$[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = \deg(X^2 - a) = 2.$$

Suppose that ζ be a root of unity that lies in $\mathbb{Q}(\sqrt{a})$. Let $n \in \mathbb{N}$ be the smallest number such that $\zeta^n = 1$. Then $1, \zeta, \ldots, \zeta^{n-1}$ are pairwise distinct. Thus they are all n'th roots of unity. Thus ζ is a primitive n'th root of unity. Its irreducible polynomial is the n'th cyclotomic polynomial $\phi_n(X)$. Then

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \phi_n(X) = \varphi(n).$$

Since $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\alpha)$, $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Thus $\varphi(n) \leq 2$.

- If $n = 1$, $\phi_1(X) = X - 1$. Thus $\zeta = 1$.
- If $n = 2$, $\phi_2(X) = X + 1$. Thus $\zeta = -1$.
- If $n \geq 3$, then 1 and $n-1$ are two numbers in $\{1, \ldots, n-1\}$ that are prime to n. Because $\varphi(n) \leq 2$, there is no other element in $\{1, \ldots, n-1\}$ that ~~are~~ is prime to n, and $\varphi(n) = 2$. Let p be any prime divisor of n and p^α be the highest power of p dividing n. Then $\varphi(n) \geq \varphi(p^\alpha) = p^{\alpha-1}(p-1) \geq p - 1$. Thus $p \leq 3$.

Thus, $p=2$ or $p=3$. This means n can be one of the form 2^r, 3^s, $2^r 3^s$ where $r, s \geq 1$.

If $n = 2^r$ then $\varphi(n) = 2^{r-1}$. Then $2 = 2^{r-1}$, so $r=2$. Then $n=4$.

If $n = 3^s$ then $\varphi(n) = 2 \cdot 3^{s-1}$. Then $2 = 2 \cdot 3^{s-1}$, so $s=1$. Then $n=3$.

If $n = 2^r 3^s$ then $\varphi(n) = \varphi(2^r)\varphi(3^s) = 2^{r-1} \cdot 2 \cdot 3^{s-1} = 2^r \cdot 3^{s-1}$.

Then $2 = 2^r \cdot 3^{s-1}$, so $r = 1$ and $s = 1$. Thus $n = 6$.

We have $\phi_3(X) = X^2 + X + 1$,

$$\phi_4(X) = \frac{X^4 - 1}{\phi_1(X)\phi_2(X)} = \frac{X^4 - 1}{(X-1)(X+1)} = X^2 + 1,$$

$$\phi_6(X) = \frac{X^6 - 1}{\phi_1(X)\phi_2(X)\phi_3(X)} = \frac{X^6 - 1}{(X^2-1)(X^2+X+1)} = X^2 - X + 1.$$

In brief, there are only 4 kinds of values for ζ.

- $\zeta = \pm 1$,
- $\zeta = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, (the primitive 3^{rd} roots)
- $\zeta = \pm i$, (the primitive 4^{th} roots)
- $\zeta = \frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, (the primitive 6^{th} roots)

For any number $a \in \mathbb{Z}$, ± 1 always lie in $\mathbb{Q}(\sqrt{a})$. ~~Thus, for each~~

~~Specific value of a, all we have to do is to figure out if $i\sqrt{3}$~~

Moreover, $\pm\frac{1}{2} \pm i\frac{\sqrt{3}}{2} \in \mathbb{Q}(\sqrt{a}) \iff i\sqrt{3} \in \mathbb{Q}(\sqrt{a})$,

$\pm i \in \mathbb{Q}(\sqrt{a}) \iff i \in \mathbb{Q}(\sqrt{a})$.

Thus, for each specific value of a, all we have to do is to figure out if $i\sqrt{3}$ or i belongs to $\mathbb{Q}(\sqrt{a})$. The irreducible polynomials of them over $\mathbb{Q}$ are respectively x^2+3 and x^2+1. Let A be the set of all roots of unity contained in $\mathbb{Q}(\sqrt{a})$.

* $a=-1$ $\quad \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(i)$

Then $\pm i \in \mathbb{Q}(i)$. Suppose by contradiction that $i\sqrt{3} \in \mathbb{Q}(i)$. Then $\sqrt{3} \in \mathbb{Q}(i)$. Then there are $r, s \in \mathbb{Q}$ such that $\sqrt{3} = r + is$. Thus the imaginary part is zero and $\sqrt{3} = r \in \mathbb{Q}$. This is a contradiction. Therefore, $A = \{\pm 1, \pm i\}$, i.e. all 4^{th} roots of unity.

* $a=-2$ $\quad \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(i\sqrt{2})$

Suppose by contradiction that $i \in \mathbb{Q}(i\sqrt{2})$. Then $\sqrt{2} \in \mathbb{Q}(i\sqrt{2})$. Then there are $r, s \in \mathbb{Q}$ such that $\sqrt{2} = r + is\sqrt{2}$. The imaginary part must be zero and $\sqrt{2} = r \in \mathbb{Q}$. This is a contradiction.

Suppose by contradiction that $i\sqrt{3} \in \mathbb{Q}(i\sqrt{2})$. Then there are $r, s \in \mathbb{Q}$ such that $i\sqrt{3} = r + is\sqrt{2}$. Then $i\sqrt{3}$ is a root of $X^2 - 2rX + (r^2+2s^2)$.

Since X^2+3 is the irreducible polynomial of $i\sqrt{3}$, these two polynomials must be the same. Thus $r=0$ and $r^2+2s^2=3$. Thus $s=\pm\sqrt{3/2} \notin \mathbb{Q}$. This is a contradiction. Therefore, $A=\{\pm 1\}$.

* $a=2$ $\quad \mathbb{Q}(\sqrt{a})=\mathbb{Q}(\sqrt{2})$

Since $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, it doesn't contain i or $i\sqrt{3}$. Thus, $A=\{\pm 1\}$.

* $a=-3$ $\quad \mathbb{Q}(\sqrt{a})=\mathbb{Q}(i\sqrt{3})$

Then $i\sqrt{3} \in \mathbb{Q}(i\sqrt{3})$. Suppose by contradiction that $i \in \mathbb{Q}(i\sqrt{3})$. Then there are $r, s \in \mathbb{Q}$ such that $i=r+si\sqrt{3}$. The real part must be zero and $i=si\sqrt{3}$. Thus $s=1/\sqrt{3} \notin \mathbb{Q}$. This is a contradiction. Therefore, $A=\{\pm 1, \pm\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\}$, i.e. all 6^{th} roots of unity.

* $a=3$ $\quad \mathbb{Q}(\sqrt{a})=\mathbb{Q}(\sqrt{3})$

Since $\mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$, it doesn't contain i or $i\sqrt{3}$. Thus, $A=\{\pm 1\}$.

* $a=-5$ $\quad \mathbb{Q}(\sqrt{a})=\mathbb{Q}(\sqrt{-5})=\mathbb{Q}(i\sqrt{5})$

Suppose by contradiction that $i \in \mathbb{Q}(i\sqrt{5})$. Then there are $r, s \in \mathbb{Q}$ such that $i=r+si\sqrt{5}$. The real part must be zero and $i=si\sqrt{5}$. Thus $s=1/\sqrt{5} \notin \mathbb{Q}$, which is a contradiction.

Suppose by contradiction that $i\sqrt{3} \in \mathbb{Q}(i\sqrt{5})$. Then there are $r, s \in \mathbb{Q}$

46

such that $i\sqrt{3} = r + si\sqrt{5}$. Thus $i\sqrt{3}$ is a root of $X^2 - 2rX + (r^2 + 5s^2)$. Since $X^2 + 3$ is the irreducible polynomial of $i\sqrt{3}$ over $\mathbb{Q}$, these polynomials must be the same. Thus $r = 0$ and $r^2 + 5s^2 = 3$. Thus $s = \pm\sqrt{15}/5 \notin \mathbb{Q}$. Thus is a contradiction.

Therefore, $A = \{\pm 1\}$.

(b) Let ζ be a primitive m'th root of unity. Then

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \phi_m(X) = \varphi(m).$$

Thus $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2 \iff \varphi(m) = 2$. As proved in part (b), there are only three numbers satisfying this condition, namely 3, 4, 6.