# MTH-ALG, Algebra Problem Sets Solutions

Atonu Roy Chowdhury,
achowdhu@ictp.it, atonuroychowdhury@gmail.com

This is available in: https://atonurc.github.io/ICTP/MTH-ALG.pdf

No AI (or LLM) has been used to solve the exercises. All the errors are my own. Please send me an email if anything is wrong, or not clearly explained.

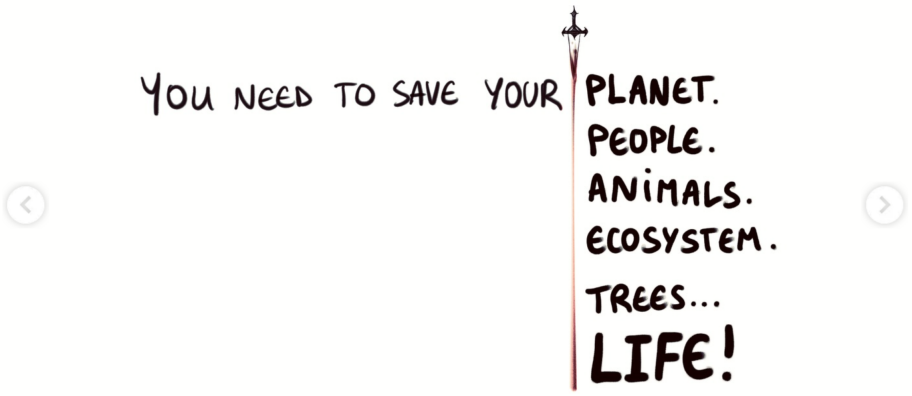



Figure 1: Source: https://www.instagram.com/p/DSi57dsij5h/?img_index=7

## Contents


1 Problem Set 1 3

2 Problem Set 2 12

3 Problems on Groups from Lothar Göttsche's Notes 23

4 Problems on Rings from Lothar Göttsche's Notes 36

5 Problem Set 3 65

6 Problem Set 4 71

7 Problems on Fields from Lothar Göttsche's Notes 82

8 Problem Set 5 128

# §1 Problem Set 1

**Exercise 1.1.** Let

$$G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}. \tag{1.1}$$

(a) How many elements of $G$ have order 60?

(b) How many cyclic subgroups of $G$ have order 30?

(c) How many injective homomorphisms

$$f : \mathbb{Z}/12\mathbb{Z} \longrightarrow G \tag{1.2}$$

are there?

*Solution.* (a) We shall prove something first:

> **Claim 1.1:** If $a \in G$ has order $n$, and $b \in H$ has order $m$, then $\operatorname{ord}((a,b)) = \operatorname{lcm}(n,m)$ in $G \times H$.
>
> *Proof.* Suppose $(a,b)^k = (e,e)$. Then $a^k = b^k = e$. This gives us that $n \mid k$ and $m \mid k$. Hence,
>
> $$\operatorname{lcm}(n,m) \mid k. \tag{1.3}$$
>
> Furthermore,
>
> $$(a,b)^{\operatorname{lcm}(n,m)} = \left(a^{\operatorname{lcm}(n,m)}, b^{\operatorname{lcm}(n,m)}\right) = (e,e)\,. \tag{1.4}$$
>
> Hence, $\operatorname{ord}((a,b)) = \operatorname{lcm}(n,m)$. □

Now, $(a,b)$ will have order 60 if $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) = 60$. Since $\operatorname{ord}(a) \in \{1,2,3,6\}$ and $\operatorname{ord}(b) \in \{1,2,4,5,10,20\}$, $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) = 60$ can only happen in the following cases:

- $\operatorname{ord}(a) = 3, \operatorname{ord}(b) = 20$. Then the choices for $b$ are all the numbers coprime to 20, so we have $\varphi(20) = 8$ choices. The choices for $a$ are $2, 4$. Hence there are $8 \times 2 = 16$ possibilities.
- $\operatorname{ord}(a) = 3, \operatorname{ord}(b) = 20$. Then the choices for $b$ are all the numbers coprime to 20, so we have $\varphi(20) = 8$ choices. The choices for $a$ are $1, 5$. Hence there are $8 \times 2 = 16$ possibilities.

Hence, there are $16 + 16 = 32$ elements of order 60.

(b) Let's first calculate how many elements $(a,b)$ are there of order 30. As before, the possibilities are:

- $\operatorname{ord}(a) = 3, \operatorname{ord}(b) = 10$. Then the choices for $b$ are multiples of 2 by all the numbers coprime to 10, so we have $\varphi(10) = 4$ choices. The choices for $a$ are $2, 4$. Hence there are $4 \times 2 = 8$ possibilities.

- $\bullet \operatorname{ord}(a) = 6, \operatorname{ord}(b) = 10$. Then the choices for $b$ are multiples of 2 by all the numbers coprime to 10, so we have $\varphi(10) = 4$ choices. There are $\varphi(6) = 2$ choices for $a$. Hence there are $4 \times 2 = 16$ possibilities.
- $\bullet \operatorname{ord}(a) = 6, \operatorname{ord}(b) = 5$. Then the choices for $b$ are multiples of 4 by all the numbers coprime to 5, so we have $\varphi(5) = 4$ choices. There are $\varphi(6) = 2$ choices for $a$. Hence there are $4 \times 2 = 16$ possibilities.

Hence, there are $8 + 8 + 8 = 24$ numbers of order 30. A subgroup of order 30 consists of $\varphi(30) = 8$ generators. Hence, the number of subgroups of order 30 is $24/8 = 3$.

(c) Note that $f$ is completely fixed by $f\left(\overline{1}\right)$. For $f$ to be injective, $f\left(\overline{1}\right)$ has to be an element of order 12. Let's now calculate how many elements $(a, b)$ are there of order 12. The possibilities are:

- $\bullet \operatorname{ord}(a) = 3, \operatorname{ord}(b) = 4$. Then the choices for $b$ are multiples of 5 by all the numbers coprime to 4, so we have $\varphi(4) = 2$ choices. The choices for $a$ are $2, 4$. Hence there are $2 \times 2 = 4$ possibilities.
- $\bullet \operatorname{ord}(a) = 6, \operatorname{ord}(b) = 4$. Then the choices for $b$ are multiples of 5 by all the numbers coprime to 4, so we have $\varphi(4) = 2$ choices. There are $\varphi(6) = 2$ choices for $a$. Hence there are $2 \times 2 = 4$ possibilities.

Hence, there are $4 + 4 = 8$ elements of order 12. As a result, there are 12 injective homomorphisms $f : \mathbb{Z}_{12} \to G$.

■

**Exercise 1.2.** Let $(G_i)_{i=1}^n$ be a family of normal subgroups of $G$ such that

$$G = \left\langle \bigcup_{i=1}^{n} G_i \right\rangle. \tag{1.5}$$

Show that $G$ is isomorphic to the direct product of the $G_i$ if and only if one of the following conditions holds:

1. For every $i$,
$$G_i \cap \left\langle \bigcup_{j \neq i} G_j \right\rangle = \{e\}. \tag{1.6}$$
2. Every element $g \in G$ can be written uniquely as a product
$$g = g_1 g_2 \cdots g_n, \qquad g_i \in G_i. \tag{1.7}$$

*Solution.* We will show the equivalence of the following 3 statements:

1. The map $f : G_1 \times \cdots \times G_n \to G$ defined by

$$f(g_1, g_2, \ldots, g_n) = g_1 g_2 \cdots g_n \tag{1.8}$$

is an isomorphism.

2. Every element $g \in G$ can be written uniquely as a product

$$g = g_1 g_2 \cdots g_n, \qquad g_i \in G_i. \tag{1.9}$$

3. For every $i$,

$$G_i \cap \left\langle \bigcup_{j \neq i} G_j \right\rangle = \{e\}. \tag{1.10}$$

**Claim 1.2:** Assuming 2, if $g_i \in G_i$ and $g_j \in G_j$ for $i \neq j$, then $g_i g_j = g_j g_i$.

*Proof.* WLOG, assume $i < j$. Since $G_i$ is normal, $g_j g_i g_j^{-1} \in G_i$, so let's call this element $g_i'$. Therefore,

$$g_j g_i = g_i' g_j. \tag{1.11}$$

Similarly, since $G_j$ is normal, $g_i^{-1} g_j g_i \in G_j$, so let's call this element $g_j'$. Therefore,

$$g_j g_i = g_i g_j'. \tag{1.12}$$

But this gives two different representations of the element $g_j g_i$:

$$g_j g_i = e \cdots e \underbrace{g_i'}_{i\text{-th slot}} e \cdots e \underbrace{g_j}_{j\text{-th slot}} e \cdots e = e \cdots e \underbrace{g_i}_{i\text{-th slot}} e \cdots e \underbrace{g_j'}_{j\text{-th slot}} e \cdots e. \tag{1.13}$$

By the uniqueness, we have $g_i = g_i'$ and $g_j = g_j'$, proving that $g_j g_i = g_i g_j$. □

**Claim 1.3:** Assuming 3, if $g_i \in G_i$ and $g_j \in G_j$ for $i \neq j$, then $g_i g_j = g_j g_i$.

*Proof.* Consider the element $x := g_i g_j g_i^{-1} g_j^{-1}$. By the normality of $G_j$, $g_i g_j g_i^{-1} \in G_j$, so that $x \in G_j$. Similarly, by the normality of $G_i$, $g_j g_i^{-1} g_j^{-1} \in G_i$, so that $x \in G_i$. Since the intersection $G_i \cap G_j = \{e\}$, we can conclude that $x = e$, i.e. $g_i g_j = g_j g_i$. □

**(1⇒2)** Trivial.

**(2⇒3)** Let $x \in G_i \cap \left\langle \bigcup_{j \neq i} G_j \right\rangle$. Since $x \in G_i$, it can be uniquely represented as

$$x = e \cdots e \underbrace{x}_{i\text{-th slot}} e \cdots e. \tag{1.14}$$

Since $x \in \left\langle \bigcup_{j\neq i} G_j \right\rangle$, $x$ can be written as a string of elements of $G_j$. Since elements from different $G_j$'s commute, we can group the elements from the same $G_j$'s and then form

$$x = g_1 g_2 \cdots g_{i-1} e g_{i+1} \cdots g_n. \tag{1.15}$$

by uniqueness, we must have that all $g_j$'s must be $e$, and also $x = e$. Hence, $G_i \cap \left\langle \bigcup_{j\neq i} G_j \right\rangle = \{e\}$.

**(3⇒1)** First, we'll show that $f$ is a homomorphism.

$$f(g_1, \ldots, g_n) f\left(g_1', \ldots, g_n'\right) = (g_1 \cdots g_n)\left(g_1' \cdots g_n'\right). \tag{1.16}$$

Since elements from different $G_i$'s commute, this can be rewritten as

$$(g_1 \cdots g_n)\left(g_1' \cdots g_n'\right) = \left(g_1 g_1'\right)\left(g_2 g_2'\right) \cdots \left(g_n g n'\right) = f\left(g_1 g_1', \ldots, g_n g_n'\right), \tag{1.17}$$

i.e. $f$ is a homomorphism. $f$ is surjective indeed: since $G = \langle \bigcup_{i=1}^n G_i \rangle$, every element $g \in G$ can be written as a string of elements of $G_i$'s. Since elements from different $G_i$'s commute, we can group the elements from the same $G_i$'s and then form

$$g = g_1 g_2 \cdots g_n, \quad \text{where } g_i \in G_i \text{ for each } i. \tag{1.18}$$

Now, suppose $(g_1, \ldots, g_n) \in \operatorname{Ker} f$. Then

$$e = g_1 g_2 \cdots g_n. \tag{1.19}$$

From this, we can write

$$\begin{aligned} g_i^{-1} &= g_i^{-1}\ g_1 g_2 \cdots g_n = g_1 g_2 \cdots g_{i-1}\left(g_i^{-1} g_i\right) g_{i+1} \cdots g_n \\ &= g_1 g_2 \cdots g_{i-1} g_{i+1} \cdots g_n \in \left\langle \bigcup_{j\neq i} G_j \right\rangle. \end{aligned} \tag{1.20}$$

(Here the reordering is possible because $g_i^{-1}$ commutes with the other $g_j$'s.) Since $G_i \cap \left\langle \bigcup_{j\neq i} G_j \right\rangle = \{e\}$, this forces that $g_i = e$. This is true for each $i$. Hence, $\operatorname{Ker} f$ is trivial, and hence it's injective. This completes the proof. ■

**Exercise 1.3.** Let $G$ be a group, and define

$$\Delta = \{(x, x) \mid x \in G\}. \tag{1.21}$$

(a) Show that $\Delta$ is a subgroup of $G \times G$.

(b) Prove that $\Delta$ is a normal subgroup of $G \times G$ if and only if $G$ is abelian. Moreover, in this case, show that the quotient group $(G \times G)/\Delta$ is isomorphic to $G$.

*Solution.* (a) Take $(x,x),(y,y) \in \Delta$. Then

$$(x,x) * (y,y)^{-1} = (x,x) * \left(y^{-1}, y^{-1}\right) = \left(xy^{-1}, xy^{-1}\right) \in \Delta. \tag{1.22}$$

Therefore, $\Delta$ is a subgroup of $G \times G$.

(b) All subgroups of an abelian group are normal. So if $G$ is abelian, so is $G \times G$, and hence $\Delta$ is a normal subgroup.

Suppose $\Delta$ is a normal subgroup. Then given any $(g,h) \in G \times G$,

$$(g,h) * (x,x) * (g,h)^{-1} = (g,h) * (x,x) * \left(g^{-1}, h^{-1}\right) = \left(gxg^{-1}, hxh^{-1}\right). \tag{1.23}$$

This is in $\Delta$, by hypothesis that $\Delta$ is normal. Therefore,

$$gxg^{-1} = hxh^{-1} \tag{1.24}$$

Since this holds for every $g, x, h \in G$, we choose $h = e$, so we have

$$gxg^{-1} = x \implies gx = xg, \tag{1.25}$$

proving that $G$ is abelian. Suppose $G$ is abelian, then we define

$$\begin{aligned} f : G \times G &\to G \\ (x,y) &\mapsto xy^{-1}. \end{aligned} \tag{1.26}$$

This is a homomorphism, because

$$f\left((g,h) * (x,y)\right) = f\left(gx, hy\right) = (gx)\left(hy\right)^{-1} = gxy^{-1}h^{-1} \tag{1.27}$$

$$= \left(gh^{-1}\right)\left(xy^{-1}\right) = f\left(g,h\right) f\left(x,y\right). \tag{1.28}$$

Therefore, $f$ is a homomorphism. Now,

$$(x,y) \in \operatorname{Ker} f \iff xy^{-1} = e \iff x = y. \tag{1.29}$$

Therefore, $\operatorname{Ker} f = \Delta$. $f$ is surjective, since any $g \in G$ is $f(g,e) = g$. Hence, by the first isomorphism theorem,

$$\operatorname{im} f \cong \frac{\operatorname{dom} f}{\operatorname{Ker} f} \implies G \cong \frac{G \times G}{\Delta}. \tag{1.30}$$

■

**Exercise 1.4.** A subgroup $M$ of a group $G$ is called *maximal* if $M \neq G$ and for every subgroup $L$ of $G$,

$$M \subsetneq L \subseteq G \implies L = G. \tag{1.31}$$

(a) Let $K, M$ be subgroups of a group $G$ such that $K \trianglelefteq G$ and $K \subseteq M$. Prove that $M$ is a maximal subgroup of $G$ if and only if $M/K$ is a maximal subgroup of $G/K$.

(b) Prove that in a finite group $G$, every proper subgroup $H \neq G$ is contained in some maximal subgroup of $G$.

(c) Prove that in a finite abelian group different from the trivial group, the maximal subgroups are precisely those of prime index.

(d) Is the previous point true if we remove the assumption that the group is abelian?

*Solution.* (a) Let $\pi : G \to G/K$ denote the projection map. Suppose $M$ is a maximal subgroup of $G$. Assume for the sake of contradiction that $M/K$ is **NOT** maximal. Then there exists another subgroup

$$\frac{M}{K} \subsetneq X \subsetneq \frac{G}{K}. \tag{1.32}$$

Now consider $\pi^{-1}(X)$.

**Claim 1.4:** If $f : G_1 \to G_2$ is a homomorphism, and $H_2 \subseteq G_2$ is a subgroup, then $f^{-1}(H_2) \subseteq G_1$ is a subgroup.

*Proof.* Take $x, y \in f^{-1}(H_2)$. Then $f(x), f(y) \in H_2$. Since $H_2 \subseteq G_2$ is a subgroup,

$$f\left(xy^{-1}\right) = f(x) f(y)^{-1} \in H_2, \tag{1.33}$$

proving that $xy^{-1} \in f^{-1}(H_2)$. So $f^{-1}(H_2) \subseteq G_1$ is a subgroup. □

Now, $\pi^{-1}(X)$ is a subgroup of $G$, that contains $\pi^{-1}(M/K) = M$. Hence, either $\pi^{-1}(X) = M$ or $\pi^{-1}(X) = G$.

$$\pi^{-1}(X) = \{g \in G \mid gK \in X\}. \tag{1.34}$$

If $\pi^{-1}(X) = G$, then $X = G/K$; and if $\pi^{-1}(X) = M$, then $X = M/K$; both of which contradict (1.32).

Conversely, suppose $M/K$ is a maximal subgroup in $G/K$. Assume for the sake of contradiction that $M$ is **NOT** maximal. Then there exists another subgroup

$$M \subsetneq H \subsetneq G. \tag{1.35}$$

Since image of a subgroup is also a subgroup, we have $\frac{M}{K} \subset \frac{H}{K} \subset \frac{G}{K}$. By the maximality of $M/K$, either $H/K = M/K$ or $H/K = G/K$.

**Claim 1.5:** For any subgroup $L \supseteq K$, $\pi^{-1}(L/K) = L$.

*Proof.* It's clear that $L \subseteq \pi^{-1}(L/K)$. Now take any $g \in \pi^{-1}(L/K)$. Then $gK \in L/K$.

$$gK = lK \text{ for some } l \in L. \tag{1.36}$$

Therefore, $l^{-1}g \in K \subseteq L$. Hence, $g = l\left(l^{-1}g\right) \in L$. As a result, $L \supseteq \pi^{-1}(L/K)$. □

If $H/K = M/K$, by taking $\pi^{-1}$, we get $H = K$; and if $H/K = G/K$, then $H = G$; both of which contradict (1.35).

(b) Let $H$ be a proper subgroup of a finite group $G$. We construct a sequence of subgroups

$$H =: H_0 \subsetneq H_1 \subsetneq H_2 \subsetneq \cdots \tag{1.37}$$

If $H_i$ is maximal, then we are done, since $H$ is contained in a maximal subgroup! Otherwise, there exists some $g_{i+1} \in G - H_i$ such that

$$H_i \subsetneq H_{i+1} := \langle H_i, g_{i+1} \rangle \subsetneq G. \tag{1.38}$$

If there is no such $g_{i+1}$, then $H_i$ is indeed maximal, because adding one element to $H_i$ and making a group with it makes it the whole $G$.

Now, since $G$ is a finite group, this sequence can't go on forever. Therefore, it has to stop somewhere, and thus we find a maximal subgroup that contains $H$.

(c) Let $M$ be a subgroup of prime index, i.e. $[G : M] = p$. Let's pick a subgroup $L$ with

$$M \subseteq L \subseteq G. \tag{1.39}$$

Then

$$[G : M] = [G : L]\,[L : M]\,. \tag{1.40}$$

(This follows from the fact that for finite groups $[G : H] = \frac{|G|}{|H|}$.) Since $[G : M]$ is a prime, it forces either $[G : L] = 1$, or $[L : M] = 1$; consequently $G = L$ or $L = M$. Therefore, $M$ is maximal.

Now suppose $M$ is a maximal subgroup in a finite abelian group $G$. Since $G$ is abelian, $M$ is normal, so we can form the quotient group $G/M$. By part (a), since $M$ is maximal, we can conclude that $\{\overline{e}\} = M/M$ is a maximal subgroup of $G/M$.

**Claim 1.6:** If $\{e\}$ is a maximal subgroup of $G \neq \{e\}$, then $G \cong \mathbb{Z}_p$ for some prime $p$.

*Proof.* Adding one single non-identity element makes it the whole group, so for every $a \in G$ with $a \neq e$,

$$\langle a \rangle = G. \tag{1.41}$$

Hence, $G$ is cyclic. If $|G|$ was infinite, then it would have subgroups other than the trivial one. But as $\{e\}$ is a maximal subgroup, it's the only subgroup. Therefore, $|G|$ can't be infinite.

Now, if $|G|$ was composite, say $|G| = mn$, then $a^{mn} = e$, proving $a^m$ has order $n$. This gives rise to a subgroup of size $n$, namely $\langle a^m \rangle$, which is a contradiction! Therefore, $|G|$ is prime. □

Now, $\{\overline{e}\} = M/M$ is a maximal subgroup of $G/M$, proves that $|G/M| = p$. Therefore,

$$M \subsetneq G \text{ is maximal } \iff [G : M] \text{ is prime.} \tag{1.42}$$

(d) No. We can consider the group $G = A_4$ of alternating group of degree 4, which contains all even permutations of $\{1, 2, 3, 4\}$. The subgroup

$$H = \langle (1\ 2\ 3) \rangle \tag{1.43}$$

has size 3, so that $[G : H] = 2^2$ is not a prime. However, $H$ is maximal. Indeed, if there exists another subgroup

$$H \subsetneq K \subsetneq G, \tag{1.44}$$

then $|K|$ divides $|G| = 12$, and $|H| = 3$ divides $|K|$, forces $|K| = 6$. If $K$ contains a product of two 2-cycles, e.g. $(1\ 2)\,(3\ 4)$, then

$$(1\ 2\ 3)\,(1\ 2)\,(3\ 4) = (1\ 3\ 4) \in K \tag{1.45}$$

Since $K$ is a group, it contains the inverse $(1\ 4\ 3)$ as well. These are all the 6 elements of $K$. But then

$$(1\ 2)\,(3\ 4)\,(1\ 2\ 3) = (2\ 4\ 3) \tag{1.46}$$

that gives one more element in $K$, which is a contradiction!

Therefore, $K$ doesn't contain any product of two 2-cycles, i.e. the only non-identity elements in $K$ are 3-cycles. But every 3-cycle comes with its inverse as well, and no 3-cycle is its own inverse. Therefore, $|K|$ can't be even! Thus we arrive at a contradiction. Hence, $H$ is maximal.

■

**Exercise 1.5.** Let $p$ be a prime number.

(a) Determine all elements of order dividing $p$ in $S_n$. Denote by $a_n$ the number of such elements and derive a formula for $a_n$.

(b) Prove the identity

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = e^{x + \frac{x^p}{p}}. \tag{1.47}$$

*Solution.* (a) Every element $\sigma \in S_n$ can be decomposed into disjoint cycles. The disjoint cycles commute. Now, if $\operatorname{ord} \sigma \mid p$, then we must have $\sigma^p = e$. This will happen if and only if $c_i^p = e$ for each disjoint cycle $c_i$ in $\sigma$.

Now, for a cycle $c_i$, $c_i^p = e$ happens if the length of the cycle is either 1 or $p$. Therefore, $a_n$ will be the number of ways we can decompose $\{1, 2, \ldots, n\}$ into cycles of length 1 or $p$.

Now, suppose $\sigma \in S_n$ consists of $m$ disjoint cycles of length $p$, and the other $n - mp$ elements are fixed points (i.e. cycles of length 1). Here, $m$ ranges from 0 to $\left\lfloor \frac{n}{p} \right\rfloor$. Therefore,

$$a_n = \sum_{m=0}^{\left\lfloor \frac{n}{p} \right\rfloor} \text{number of } \sigma\text{'s with } m \text{ disjoint cycles of length } p. \tag{1.48}$$

First, we can choose the numbers involved in the $p$-cycles in $\binom{n}{mp}$ ways. Now, we can partition them into $m$ sets of size $p$, which can be done in

$$\binom{mp}{p} \cdot \binom{mp-p}{p} \cdot \cdots \cdot \binom{p}{p} = \frac{(mp)!}{(p!)^m} \tag{1.49}$$

many ways. Now, each cycles can be permuted in $(p-1)!$ different ways. Finally, the cycles themselves can permute in $m!$ ways among themselves. So we need to divide by that. Therefore, the number of $\sigma$'s with $m$ disjoint cycles of length $p$ is

$$\binom{n}{mp} \cdot \frac{(mp)!}{(p!)^m} \cdot ((p-1)!)^m \cdot \frac{1}{m!} = \frac{n!}{p^m m!\,(n-mp)!}. \tag{1.50}$$

Hence,

$$a_n = \sum_{m=0}^{\left\lfloor \frac{n}{p} \right\rfloor} \frac{n!}{p^m m!\,(n-mp)!}. \tag{1.51}$$

(b) Using (1.51), we have

$$f(x) := \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = \sum_{n=0}^{\infty} \sum_{m=0}^{\left\lfloor \frac{n}{p} \right\rfloor} \frac{x^n}{p^m m!\,(n-mp)!}. \tag{1.52}$$

We can swap the sum into

$$f(x) = \sum_{m=0}^{\infty} \sum_{n=mp}^{\infty} \frac{x^n}{p^m m!\,(n-mp)!}. \tag{1.53}$$

Suppose $k = n - mp$, so that $n = k + mp$. Then the sum can be rewritten as

$$f(x) = \sum_{m=0}^{\infty} \sum_{k=0}^{\infty} \frac{x^{k+mp}}{p^m m! k!} = \sum_{m=0}^{\infty} \frac{1}{m!} \left( \frac{x^p}{p} \right)^m \sum_{k=0}^{\infty} \frac{x^k}{k!} = e^{\frac{x^p}{p}} e^x = e^{\frac{x^p}{p} + x}. \tag{1.54}$$

■

## §2 Problem Set 2

**Exercise 2.1.** Find all $p$-Sylow subgroups of the following groups:

(a) $\mathbb{Z}/n\mathbb{Z}$;

(b) $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$;

(c) the dihedral group $D_n$ (the group of symmetries of a regular $n$-polygon).

*Solution.* Before proceeding, we claim that for abelian groups, the $p$-Sylow subgroup is unique! Indeed, if $H_1$ and $H_2$ are two $p$-Sylow subgroups of $G$, then by Sylow's Second Theorem, they are related by a conjugation, i.e.

$$H_2 = gH_1g^{-1} \text{ for some } g \in G. \tag{2.1}$$

But if $G$ is abelian, we have

$$H_2 = gH_1g^{-1} = H_1. \tag{2.2}$$

Furthermore, notice that if $G$ is not necessarily abelian, but a $p$-Sylow subgroup happens to be normal, then also the $p$-Sylow subgroup is unique. Because if $H_1$ is a $p$-Sylow subgroup which happens to be normal, and $H_2$ is another $p$-Sylow subgroup, then

$$H_2 = gH_1g^{-1} = H_1. \tag{2.3}$$

We shall use these two properties below.

(a) Let $n = p^k m$, where $p \nmid m$. Since the group is abelian, there is exactly one $p$-Sylow subgroup, i.e. subgroup of order $p^m$. That's precisely the subgroup generated by $m$, since it has order $p^k$, i.e.

$$H = \langle m \rangle = \left\{0, m, 2m, 3m, \ldots, \left(p^k - 1\right) m\right\}. \tag{2.4}$$

(b) $|G| = 6 \cdot 12 = 2^3 \cdot 3^2$. Since the group is abelian, there is exactly one $p$-Sylow subgroup. For $p = 2$, we can choose a copy of $\mathbb{Z}_2$ inside $\mathbb{Z}_6$, and a copy of $\mathbb{Z}_4$ inside $\mathbb{Z}_{12}$, and take their direct product, and that will be the subgroup of order $2^3$.

$$H = \{0, 3\} \times \{0, 3, 6, 9\} \subset \mathbb{Z}_6 \times \mathbb{Z}_{12}. \tag{2.5}$$

For $p = 3$, we can choose a copy of $\mathbb{Z}_3$ inside $\mathbb{Z}_6$, and a copy of $\mathbb{Z}_3$ inside $\mathbb{Z}_{12}$, and take their direct product, and that will be the subgroup of order $3^2$.

$$H' = \{0, 2, 4\} \times \{0, 4, 8\} \subset \mathbb{Z}_6 \times \mathbb{Z}_{12}. \tag{2.6}$$

(c) $|D_n| = 2n$. Suppose $p \neq 2$. Then $p \mid 2n$ if and only if $p \mid n$. We write

$$2n = 2 \cdot p^k \cdot m, \tag{2.7}$$

where $p \nmid m$. Let $a$ be rotation by $\frac{2\pi}{n}$. Then $\langle a \rangle$ is an order-$n$ subgroup of $D_n$. We take

$$H = \langle a^m \rangle = \left\{ e, a^m, a^{2m}, \ldots, a^{\left(p^k-1\right)m} \right\}, \tag{2.8}$$

which is a subgroup of order $p^k$, i.e. a $p$-Sylow subgroup. Now, we claim that $H$ is normal in $D_n$. Indeed, all the rotations commute with all the elements of $H$. If $b$ is a reflection, then we have

$$ba^ib^{-1} = a^{-i}, \tag{2.9}$$

(this can be proven by induction on $i$), and hence

$$\left(a^j b\right)\ a^i\ \left(a^j b\right)^{-1} = a^j b a^i b a^{-j} = a^j a^{-i} a^{-j} = a^{-i}. \tag{2.10}$$

Therefore, $H$ is normal, and hence there is only one $p$-Sylow subgroup for $p \neq 2$.

Now suppose $p = 2$. If $2 \nmid n$, then

$$n_2 \mid n \implies n_2 \leq n. \tag{2.11}$$

We can then exhibit $n$ subgroups of order 2, namely the ones containing one reflection and the identity:

$$H_i = \left\{ e, a^i b \right\}, \quad \text{for } i = 0, 1, 2, \ldots, n-1. \tag{2.12}$$

Now consider the case $2 \mid n$. Suppose $n = 2^k m$, where $m$ is odd. Then

$$|D_n| = 2n = 2^{k+1} m. \tag{2.13}$$

Then

$$n_2 \mid m \implies n_2 \leq m. \tag{2.14}$$

We now exhibit $m$ subgroups of order $2^{k+1}$. These will be isomorphic to $D_{2^k}$. We define

$$H_i = \left\langle a^m, a^i b \right\rangle, \quad \text{for } i = 0, 1, 2, \ldots, m-1 \tag{2.15}$$

Here, $a' := a^m$ is a rotation of order $2^k$ (since $a^{2^k m} = a^n = e$), and $b' := a^i b$ is a reflection of degree 2, and

$$b'a'b' = \left(a^i b\right)\left(a^m\right)\left(a^i b\right) = a^i \left(b a^{i+m} b\right) = a^i a^{-i-m} = a^{-m} = \left(a'\right)^{-1}, \tag{2.16}$$

and therefore,

$$H_i = \left\langle a', b' \mid \left(a'\right)^{2^k} = \left(b'\right)^2 = e,\ b'a'b' = \left(a'\right)^{-1} \right\rangle \cong D_{2^k}, \tag{2.17}$$

so each $H_i$ is a subgroup of size $2^{k+1}$, i.e. a 2-Sylow subgroup. Since $n_2 \leq m$, and we have exhibited $m$ subgroups, these are the all of them!

■

**Exercise 2.2.** Find all 2-Sylow subgroups of the following groups:

(a) the symmetric group $S_4$;

(b) the symmetric group $S_5$.

*Solution.* (a) $|S_4| = 24 = 2^3 \cdot 3$. So we need to find all subgroups of size 8. By Sylow's theorems, if $n_2$ is the number of 2-Sylow subgroups,

$$n_2 \mid 3 \implies n_2 \in \{1, 3\}\,. \tag{2.18}$$

We claim that there are 3 of them, by finding 3 subgroups of order 8. First, note that there's a subgroup isomorphic to $D_4$.

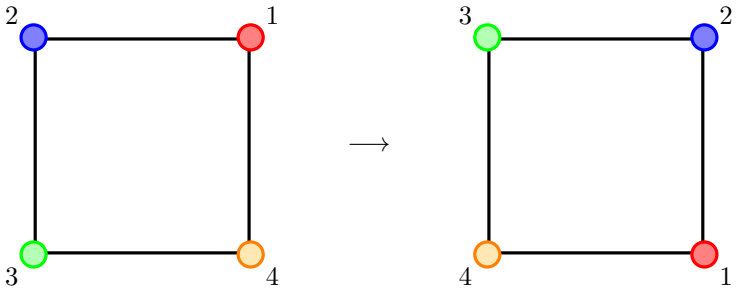



Figure 2: Rotation in $D_4$, which can be realized as the element (1 2 3 4). To see the resemblence, in the left figure, 1 is in the top-right position, which is occupied by 2 in the right figure, so $\sigma(1) = 2$, etc.

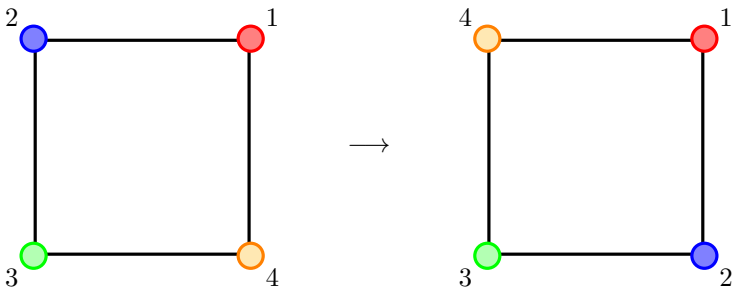



Figure 3: Reflection in $D_4$, which can be realized as the element (2 4). To see the resemblence, in the left figure, 2 is in the top-left position, which is occupied by 4 in the right figure, so $\sigma(2) = 4$, etc.

These two generate $D_4$, so we can take the corresponding subgroup in $S_4$

$$G_1 = \langle (1\ 2\ 3\ 4)\,, (2\ 4) \rangle\,, \tag{2.19}$$

which is isomorphic to $D_4$, and hence a subgroup of order 8, i.e. a 2-Sylow subgroup. To find the others, it's sufficient to change the labels in the vertices of the square. There are

3-possible ways we can cyclically rename the vertices, which gives the other two subgroups:

$$G_2 = \langle (1\ 3\ 2\ 4), (1\ 2) \rangle , \tag{2.20}$$

$$G_3 = \langle (1\ 2\ 4\ 3), (1\ 4) \rangle . \tag{2.21}$$

These are all the 2-Sylow subgroups of size 8.

(b) $|S_5| = 120 = 2^3 \cdot 15$. So we need to find all subgroups of size 8. By Sylow's theorems, if $n_2$ is the number of 2-Sylow subgroups,

$$n_2 \mid 15 \implies n_2 \in \{1, 3, 5, 15\} . \tag{2.22}$$

Note that, given any 4-element subset of $\{1, 2, 3, 4, 5\}$, we can find 3 subgroups of size 8, as per part (a). The total number of 4-element subsets of $\{1, 2, 3, 4, 5\}$ is $\binom{5}{4} = 5$. Hence, this already gives us a recipe to build $5 \times 3 = 15$ subgroups of order 8. Since $n_2 \leq 15$, these are all of them!

■

**Exercise 2.3.** (a) Show that there are no simple groups of order 30, 42 or 105.

(b) More generally, show that there are no simple groups of order $pqr$, where $p$, $q$, $r$ are distinct prime numbers.

*Solution.* We'll just solve (b). Assume for the sake of contradiction that ther exists a simple group $G$ with $|G| = pqr$. WLOG, $p < q < r$.

Note that, we must have $n_r > 1$, because if $n_r = 1$, then the $r$-Sylow subgroup would've been normal, contradicting the simplicity of $G$. Also, $n_r \equiv 1 \pmod{r}$ forces that $n_r > r > q > p$. Now, since

$$n_r \mid pq, \tag{2.23}$$

the only possibility is $n_r = pq$. In other words, there are $pq$ subgroups of order $r$, which gives

$$(\text{number of elements of order } r) = n_r (r-1) = pq (r-1) = |G| - pq. \tag{2.24}$$

Similarly, we must have $n_q > 1$, because if $n_q = 1$, then the $q$-Sylow subgroup would've been normal, contradicting the simplicity of $G$. Also, $n_q \equiv 1 \pmod{q}$ forces that $n_q > q > p$. Therefore,

$$(\text{number of elements of order } q) = n_q (q-1) > pq - p. \tag{2.25}$$

Therefore,

$$(\text{number of elements of order } p) = n_p (p-1) < p. \tag{2.26}$$

But this forces $n_p = 1$, which implies the $p$-Sylow subgroup is normal, contradicting the simplicity of $G$. Therefore, there is no simple group of order $pqr$. ■

**Exercise 2.4.** Consider the action of a finite group $G$ on a finite set $X$, with $N$ orbits. For every $g \in G$, consider the set

$$\mathrm{Fix}(g) := \{x \in X \mid g \cdot x = x\}. \tag{2.27}$$

(a) Derive Burnside's formula:

$$N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| \,. \tag{2.28}$$

(b) Apply the previous formula to solve the following problem: count the numbers of bracelets made of 3 red beads and 7 blue beads. *Hint:* Two bracelets are indistinguishable if one is obtained by the other with a rotation or a reflection.

*Solution.* (a) Consider the set

$$S = \{(g, x) \mid g \cdot x = x\} \,. \tag{2.29}$$

We can count $|S|$ in two different ways. For every $g \in G$, we count the number of $x \in S$ fixed by $g$. Then for every $x \in X$, we count the number of $g \in G$ that fixes $x$. Therefore,

$$|S| = \sum_{g \in G} |\mathrm{Fix}(g)| = \sum_{x \in X} |G_x| \,, \tag{2.30}$$

where $G_x$ is the stabilizer of $x$. Since $X$ is the disjoint union of $G$-orbits,

$$\sum_{x \in X} |G_x| = \sum_{\text{orbits } Gx} \sum_{y \in Gx} |G_y| \,. \tag{2.31}$$

Now, for $y \in Gx$, $Gx = Gy$, so their stabilizers have the same size, i.e. $|G_x| = |G_y|$.

> **Claim 2.1:** For $y \in Gx$, $|G_x| = |G_y|$
>
> *Proof.* Since $y \in Gx$, $y = g \cdot x$ for some $g \in G$. If $g_0 \in G_x$ is in the stabilizer of $x$, then $g_0 \cdot x = x$. Now,
>
> $$\left(gg_0g^{-1}\right) \cdot y = \left(gg_0g^{-1}\right) \cdot (g \cdot x) = \left(gg_0g^{-1}g\right) \cdot x = g \cdot (g_0 \cdot x) = g \cdot x = y. \tag{2.32}$$
>
> Therefore, $gg_0g^{-1} \in G_y$, i.e. $G_y = gG_xg^{-1}$. Since conjugation preserves size, $|G_x| = |G_y|$. □

With this, we rewrite (2.31),

$$\sum_{x \in X} |G_x| = \sum_{\text{orbits } Gx} |Gx| \, |G_x| \tag{2.33}$$

By Orbit-Stabilizer theorem, $|G| = |Gx| \, |G_x|$. Hence,

$$\sum_{x \in X} |G_x| = \sum_{\text{orbits } Gx} |Gx| \, |G_x| = N \, |G| \,, \tag{2.34}$$

where $N$ is the number of orbits. Hence,

$$N = \frac{1}{|G|} \sum_{x \in X} |G_x| = \frac{1}{G} \sum_{g \in G} |\mathrm{Fix}(g)| \,. \tag{2.35}$$

(b) Let $G = D_{10}$, the dihedral group on a regular 10-gon. Then $|G| = 20$. Let $X$ be the set of all bracelets made of 3 red beads and 7 blue beads (without accounting for indistinguishability). Then

$$|X| = \binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{3!} = 120. \tag{2.36}$$

Consider $D_{10}$'s action on $X$. Then the number of indistinguishable bracelets will be the number of orbits in this action. By Burnside's lemma, if $N$ is the number of orbits,

$$N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| \,. \tag{2.37}$$

For each $g \in G$, let's now compute the size of $\mathrm{Fix}(g)$.

- If $g = e$, $|\mathrm{Fix}(e)| = |X| = 120$.
- If $g$ is a rotation by $\frac{2\pi}{10}k$ for $k = 1, \ldots, 9$, then we claim that $\mathrm{Fix}(g) = \varnothing$.

  If we consider the positions (in modulo 10), then a rotation is just adding a constant with the positions. If $r_1, r_2, r_3$ are the position of the red beads in a configuration, if $g$ fixes that configuration, then we must have

  $$\{r_1, r_2, r_3\} = \{r_1 + a, r_2 + a, r_3 + a\} \pmod{10}. \tag{2.38}$$

  After adding, we have

  $$r_1 + r_2 + r_3 \equiv r_1 + r_2 + r_3 + 3a \pmod{10}. \tag{2.39}$$

  In other words, $10 \mid 3a$. But since 10 and 3 are coprime, this means $a = 0 \pmod 1)0$, i.e. the rotation is the trivial one. Therefore, for nontrivial rotations, $|\mathrm{Fix}(g)| = 0$.
- If $g$ is reflection in a line $\ell$ through the midpoints of opposite edges, then there are the same number of beads on both sides of $\ell$, and we can't arrange the beads of the same color evenly, because there are an odd number of red beads and an odd number of blue beads. So in this case, $|\mathrm{Fix}(g)| = 0$. There are 5 such reflections.
- If $g$ is reflection in a line $\ell$ through two opposite vertices, then we can choose one of them to be red, and we can choose the other to be blue. This can be done in $\binom{2}{1} = 2$ ways.

  Then if we color one side of $\ell$, the other side becomes fixed. On each side of $\ell$, we have 4 points, and we can choose one of them to be red, which can be done in $\binom{4}{1} = 4$ ways. Therefore, $|\mathrm{Fix}(g)| = 2 \times 4 = 8$. There are 5 such reflections.

Now,

$$N = \frac{1}{20}\left(120 + 0 \times 9 + 0 \times 5 + 8 \times 5\right) = \frac{160}{20} = 8. \tag{2.40}$$

■

**Exercise 2.5** (Frattini's Lemma)**.** Let $H \trianglelefteq G$ be a normal subgroup of a finite group. Let $S$ be a $p$-Sylow of $H$. Show that the conjugates of $S$ in $G$ are in $H$ as well and deduce the following:

$$G = HN_G(S), \tag{2.41}$$

where $N_G(S)$ denotes the normalizer of $S$ in $G$.

*Solution.* For every $g \in G$, since $S \leq H$,

$$gSg^{-1} \subseteq gHg^{-1} = H, \tag{2.42}$$

so conjugates of $S$ in $G$ are in $H$ as well! Now we shall prove that any $g \in G$ can be written as $g = hn$ for some $h \in H, n \in N_G(S)$.

Note that since $gSg^{-1} \subseteq H$, $gSg^{-1}$ is also a $p$-Sylow subgroup of $H$, because conjugation preserves cardinality. Since both $S$ and $gSg^{-1}$ are $p$-Sylow subgroups of $H$, by the Second Sylow Theorem, they are related by a conjugation in $H$, i.e.

$$gSg^{-1} = hSh^{-1} \tag{2.43}$$

for some $h \in H$. This gives

$$h^{-1}gSg^{-1}h = S. \tag{2.44}$$

Since $N_G(S) = \left\{g \mid gSg^{-1} = S\right\}$, by (2.44), $h^{-1}g \in N_G(S)$.

$$h^{-1}g = n \text{ for some } N_G(S), \text{ for some } h \in H \tag{2.45}$$

$$\implies g = hn \text{ for some } N_G(S), \text{ for some } h \in H. \tag{2.46}$$

Therefore, $G = HN_G(S)$. ■

**Exercise 2.6** (Short exact sequences)**.** Given a sequence of morphisms

$$N \xrightarrow{a} G \xrightarrow{b} K \tag{2.47}$$

we say that it is exact in $G$ if

$$\operatorname{Ker} b = \operatorname{im} a. \tag{2.48}$$

A sequence of the form

$$e \longrightarrow N \xrightarrow{a} G \xrightarrow{b} K \longrightarrow e \tag{2.49}$$

which is exact in $N$, $G$, $K$ is called a short exact sequence (where we denote with $e$ the group with one element).

(a) Show that in the short exact sequence above $a$ is injective and $b$ surjective.

(b) Show that $a(N) \trianglelefteq G$ and

$$K \simeq G/a(N).$$

(c) Let $N$ and $K$ be groups. Show that you can define a short exact sequence:

$$e \longrightarrow N \xrightarrow{\ i\ } N \times K \xrightarrow{\ p\ } K \longrightarrow e \tag{2.50}$$

*Solution.* (a) Exactness at $N$ gives

$$\operatorname{Ker} a = \operatorname{im} (e \to N) = \{e\}, \tag{2.51}$$

so $a$ is injective. Exactness at $K$ gives

$$\operatorname{im} b = \operatorname{Ker} (K \to e) = K, \tag{2.52}$$

so $b$ is surjective.

(b) Exactness at $G$ gives $a(N) = \operatorname{im} a = \operatorname{Ker} b$. Kernel is always normal, because for $h \in \operatorname{Ker} b$ and $g \in G$,

$$b\left(ghg^{-1}\right) = b(g)\, b(h)\, b(g)^{-1} = b(g)\, b(g)^{-1} = e, \tag{2.53}$$

so $ghg^{-1} \in \operatorname{Ker} b$, proving $\operatorname{Ker} b$ is normal. Now, since $b$ is surjective,

$$\operatorname{im} b \cong \frac{\operatorname{dom} b}{\operatorname{Ker} b} \implies K \cong \frac{G}{\operatorname{Ker} b} = \frac{G}{a(N)}. \tag{2.54}$$

(c) We define

$$i(n) = (n, e_K) \text{ and } p(n, k) = k. \tag{2.55}$$

Then clearly $i$ is injective and $p$ is surjective. Also,

$$\operatorname{im} i = N \times \{e_K\} = \operatorname{Ker} p. \tag{2.56}$$

Hence, the sequence $e \to N \to N \times K \to K \to e$ is exact.

■

**Exercise 2.7** (Semidirect products)**.** Let $N$ and $K$ be groups, and let

$$\varphi : K \longrightarrow \operatorname{Aut}(N) \tag{2.57}$$

be a group homomorphism. For each $k \in K$ and $n \in N$, we denote by $\varphi(k)(n)$ the image of $n$ under the automorphism of $N$ corresponding to $k$ via $\varphi$.

(a) Define a binary operation on the set-theoretic product $N \times K$ by

$$(n,k) * \left(n',k'\right) = \left(n\ \varphi(k)\left(n'\right), kk'\right). \tag{2.58}$$

Show that this operation defines a group. We denote this group by $N \rtimes_\varphi K$ and call it the semidirect product of $N$ by $K$ with respect to $\varphi$.

(b) Show that there is a short exact sequence

$$e \longrightarrow N \xrightarrow{\ i\ } N \rtimes_\varphi K \xrightarrow{\ p\ } K \longrightarrow e \tag{2.59}$$

where

$$i(n) = (n,e) \qquad \text{and} \qquad p(n,k) = k. \tag{2.60}$$

(c) Show that if

$$\varphi : K \longrightarrow \mathrm{Aut}(N) \tag{2.61}$$

is the trivial homomorphism, then $N \rtimes_\varphi K$ is the usual direct product of groups $N \times K$.

(d) Conversely, let $G$ be a group with subgroups $N, K \leq G$ such that

$$N \trianglelefteq G, \qquad N \cap K = \{e\}, \qquad G = NK. \tag{2.62}$$

Show that $G$ is isomorphic to the semidirect product $N \rtimes_\varphi K$, where

$$\varphi(k)(n) = knk^{-1} \tag{2.63}$$

for $n \in N$ and $k \in K$.

*Solution.* (a) For simplicity of notations, I'll write $\varphi_k = \varphi(k)$. Since $\varphi$ is a homomorphism, this will give us

$$\varphi_{kk'} = \varphi\left(kk'\right) = \varphi\left(k\right) \circ \varphi\left(k'\right) = \varphi_k \circ \varphi k'. \tag{2.64}$$

Associativity:

$$\begin{aligned}
\left[(n,k) * \left(n',k'\right)\right] * \left(n'',k''\right) &= \left(n\ \varphi_k\left(n'\right), kk'\right) * \left(n'',k''\right) \\
&= \left(n\ \varphi_k\left(n'\right)\ \ \varphi_{kk'}\left(n''\right), (kk')k''\right) \\
&= \left(n\ \varphi_k\left(n'\right)\ \ \left(\varphi_k\varphi_{k'}\left(n''\right)\right), (kk')k''\right) \\
&= \left(n\ \varphi_k\left(n'\varphi_{k'}\left(n''\right)\right), k\left(k'k''\right)\right). \qquad (2.65) \\
(n,k) * \left[\left(n',k'\right) * \left(n'',k''\right)\right] &= (n,k) * \left(n'\varphi_{k'}\left(n''\right), k'k''\right) \\
&= \left(n\ \varphi_k\left(n'\varphi_{k'}\left(n''\right)\right), k\left(k'k''\right)\right). \qquad (2.66)
\end{aligned}$$

We claim that $(e_N, e_K)$ is the identity.

$$(e_N, e_K) * (n, k) = (e_N \varphi_{e_K}(n), e_K k) \tag{2.67}$$
$$(n, k) * (e_N, e_K) = (n\varphi_k(e_N), k e_K) = (n, k). \tag{2.68}$$

We claim that $(n,k)^{-1} = \left(\varphi_{k^{-1}}\left(n^{-1}\right), k^{-1}\right)$.

$$\begin{aligned}(n,k) * \left(\varphi_{k^{-1}}\left(n^{-1}\right), k^{-1}\right) &= \left(n\varphi_k\left(\varphi_{k^{-1}}\left(n^{-1}\right)\right), kk^{-1}\right) \\ &= \left(nn^{-1}, kk^{-1}\right) = (e_N, e_K) \qquad (2.69)\\ \left(\varphi_{k^{-1}}\left(n^{-1}\right), k^{-1}\right) * (n,k) &= \left(\varphi_{k^{-1}}\left(n^{-1}\right)\varphi_{k^{-1}}(n), k^{-1}k\right) \\ &= \left(\varphi_{k^{-1}}\left(n^{-1}n\right), k^{-1}k\right) = (e_N, e_K). \qquad (2.70)\end{aligned}$$

Therefore, $N \rtimes_\varphi K$ is a group.

(b) Let's first verify that $i$ and $p$ are group homomorphisms:

$$\begin{aligned}i(n_1) * i(n_2) = (n_1, e_K) * (n_2, e_K) &= (n_1 \varphi_{e_K}(n_2), e_K e_K) \qquad (2.71)\\ &= (n_1 n_2, e_K) = i(n_1 n_2). \qquad (2.72)\\ p\left((n,k) * \left(n', k'\right)\right) = p\left(n\ \varphi_k\left(n'\right), kk'\right) &= kk' = p(n,k)\, p\left(n', k'\right). \qquad (2.73)\end{aligned}$$

Clearly $i$ is injective and $p$ is surjective. Also,

$$\operatorname{im} i = N \times \{e_K\} = \operatorname{Ker} p. \tag{2.74}$$

Hence, the sequence $e \to N \to N \rtimes_\varphi K \to K \to e$ is exact.

(c) If $\varphi$ is the trivial homomorphism, then $\varphi_k = \mathrm{id}_N$ for every $k$. Then

$$(n,k) * \left(n', k'\right) = \left(n\ \varphi_k\left(n'\right), kk'\right) = \left(n\ \mathrm{id}_N\left(n'\right), kk'\right) = \left(nn', kk'\right), \tag{2.75}$$

which is exactly the same as the group operation on the direct product $N \times K$.

(d) We define the map

$$\begin{aligned}f : N \rtimes_\varphi K &\to G \\ (n,k) &\mapsto nk.\end{aligned} \tag{2.76}$$

Let's first check that it's a homomorphism:

$$\begin{aligned}f\left((n,k) * \left(n', k'\right)\right) = f\left(\left(n\ \varphi_k\left(n'\right), kk'\right)\right) &= f\left(n\ kn'k^{-1}, kk'\right) \qquad (2.77)\\ &= nkn'k^{-1}\ kk' = nk\ n'k' \qquad (2.78)\\ &= f(n,k)\, f\left(n', k'\right). \qquad (2.79)\end{aligned}$$

It's injective because if $f(n,k) = e$, then

$$e = f(n,k) = nk \implies n = k^{-1} \in N \cap K = \{e\}, \tag{2.80}$$

so $\operatorname{Ker} f = \{(e,e)\}$. Also, $f$ is surjective since $G = NK$, so every element $g \in G$ can be written as $g = nk$ for some $n \in N$ and $k \in K$. Therefore, $f$ is an isomorphism.

■

## §3 Problems on Groups from Lothar Göttsche's Notes

**Exercise 3.1.** Find a subgroup $H$ of $S_3$ of order 3, i.e. with $|H| = 3$.

*Solution.* Consider

$$H = \langle (1\ 2\ 3) \rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}. \tag{3.1}$$

Then $|H| = 3$, and $H$ is a subgroup of $S_3$. In fact, $H$ is isomorphic to $\mathbb{Z}_3$. ■

**Exercise 3.2.** Let $G$ be a group. The center $C(G)$ of $G$ is

$$C(G) := \{g \in G \mid ga = ag,\ \forall a \in G\}. \tag{3.2}$$

(a) Show $C(G)$ is a subgroup of $G$.

(b) Show $C(G)$ is commutative.

(c) What is the center of $S_3$?

*Solution.* (a) First, $C(G) \neq \varnothing$, since $e \in C(G)$. Now, given any $x, y \in C(G)$, we'll show that $xy \in C(G)$ and $x^{-1} \in C(G)$. First notice that

$$(xy)\, a = x\,(ya) = x\,(ay) = (xa)\, y = (ax)\, y = a\,(xy), \tag{3.3}$$

for every $a \in G$; and hence, $xy \in C(G)$. Now,

$$xa = ax \implies x^{-1}(xa)\, x^{-1} = x^{-1}(ax)\, x^{-1} \implies ax^{-1} = x^{-1}a, \tag{3.4}$$

for every $a \in G$; and hence, $x^{-1} \in C(G)$. Therefore, $C(G) \leq G$.

(b) The elements of $C(G)$ commute with **every** element of $G$. So, in particular, they commute among themselves. Therefore, $C(G)$ is abelian.

(c) We claim that $C(S_3) = \{e\}$.

$$(1\ 2)(1\ 2\ 3) = (2\ 3), \quad (1\ 2\ 3)(1\ 2) = (1\ 3). \tag{3.5}$$

Hence, neither (1 2), nor (1 2 3) belong in the center. Since center is a subgroup, $(1\ 2\ 3)^{-1} = (1\ 3\ 2)$ is also not in the center. We can rule out (2 3) and (1 3) similarly:

$$(2\ 3)(1\ 2\ 3) = (1\ 3), \quad (1\ 2\ 3)(2\ 3) = (1\ 2); \tag{3.6}$$

$$(1\ 3)(1\ 2\ 3) = (1\ 2), \quad (1\ 2\ 3)(1\ 3) = (2\ 3). \tag{3.7}$$

Therefore, $C(S_3) = \{e\}$.

■

**Exercise 3.3.** Prove that every subgroup of a cyclic group is cyclic.

*Solution.* Let $G = \langle a \rangle$ be a cyclic group and $H \leq G$. Then every element of $H$ is of the form $a^i$ for some $i \in \mathbb{Z}$. Let

$$m = \min \left\{ i \in \mathbb{Z}_{>0} \mid a^i \in H \right\}. \tag{3.8}$$

We claim that $H = \langle a^m \rangle$. Since $a^m \in H$, it's clear that $\langle a^m \rangle \subset H$. Assume for the sake of contradiction that there exists some $b \in H$ and $b \notin \langle a^m \rangle$. Since $b \in G = \langle a \rangle$,

$$b = a^n, \quad \text{for some } n \in \mathbb{Z}. \tag{3.9}$$

Now, by performing division algorithm on $n$, we can write

$$n = mq + r, \quad \text{for } 0 \leq r < m. \tag{3.10}$$

Since $b \notin \langle a^m \rangle$, $r > 0$. Now, since $b = a^{mq+r}, a^m \in H$, $a^r \in H$. But $m$ is the minimal positive integer such that $a^m \in H$, and now we have found an even smaller positive integer. Contradiction! ■

**Exercise 3.4.** Let $G$ be a finite group. Let $K \subset H$ and $H \subset G$ be subgroups. Show that

$$[G : K] = [G : H][H : K]. \tag{3.11}$$

*Solution.* We shall use the fact that for finite groups, $[G : H] = \frac{|G|}{|H|}$.

$$[G : H][H : K] = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = [G : K]. \tag{3.12}$$

■

**Exercise 3.5.** Let $G$ be a group and $H, K$ normal subgroups. Then $H \cap K$ is a normal subgroup of $G$.

*Solution.* It's easy to see that $N := H \cap K$ is a subgroup of $G$. Indeed, $N \neq \varnothing$ as $e \in N$. For $x, y \in N$,

$$x, y \in H \text{ implies } xy^{-1} \in H; \text{ and } x, y \in K \text{ implies } xy^{-1} \in K. \tag{3.13}$$

Therefore, $xy^{-1} \in H \cap K = N$. Hence, $N \leq G$. Now, for any $g \in G$,

$$N \subseteq H \implies gNg^{-1} \subseteq gHg^{-1} = H, \quad \text{and } N \subseteq K \implies gNg^{-1} \subseteq gKg^{-1} = K. \tag{3.14}$$

Hence, $gNg^{-1} \subseteq H \cap K = N$, proving that $N \trianglelefteq G$. ■

**Exercise 3.6.** Let $G$ be a group and $H$ a subgroup of index 2. Show $H$ is a normal subgroup of $G$.

*Solution.* We shall prove a more general statement:

Suppose $G$ is a finite group, and let $p$ be the smallest prime divisor of $|G|$. If $H$ is a subgroup with $[G : H] = p$, then $H \trianglelefteq G$.

Consider the action of $G$ on the left coset space of $H$, by left multiplication:

$$g \cdot (aH) := (ga) H. \tag{3.15}$$

This gives a group homomorphism

$$f : G \to \mathrm{Sym}\,(G/H) \cong S_p. \tag{3.16}$$

Then $\mathrm{Ker}\, f \trianglelefteq G$. Furthermore, if $k \in \mathrm{Ker}\, f$, then for all $aH \in G/H$,

$$k \cdot (aH) := (ka) H = aH. \tag{3.17}$$

In particular, choosing $a = e$ gives us $kH = H$, i.e. $k \in H$. Hence,

$$\mathrm{Ker}\, f \leq H \leq G. \tag{3.18}$$

By the first isomorphism theorem, $\mathrm{im}\, f \cong \frac{G}{\mathrm{Ker}\, f}$, and hence $|\mathrm{im}\, f|$ divides $|G|$. But since $\mathrm{im}\, f$ is (isomorphic to) a subgroup of $S_p$, it divides $|S_p| = p!$ as well. Therefore,

$$|\mathrm{im}\, f| \,\Big|\, \gcd\left(|G|, p!\right) = p, \tag{3.19}$$

since $p$ is the smallest prime factor of $|G|$. Therefore, $|\mathrm{im}\, f| = |G/\mathrm{Ker}\, f| = [G : \mathrm{Ker}\, f]$ divides $p$. From (3.18), we have

$$[G : \mathrm{Ker}\, f] = [G : H]\,[H : \mathrm{Ker}\, f] = p\,[H : \mathrm{Ker}\, f]\,, \tag{3.20}$$

which divides $p$. Hence, we must have $[H : \mathrm{Ker}\, f] = 1$, i.e. $H = \mathrm{Ker}\, f$. Since kernels are always normal, $H \trianglelefteq G$. ■

**Exercise 3.7.** Let $G$ be a group. Let $G'$ be the subgroup of $G$ generated by

$$U = \{xyx^{-1}y^{-1} \mid x, y \in G\}. \tag{3.21}$$

(a) Show $G'$ is a normal subgroup of $G$.

(b) Show $G/G'$ is abelian.

*Solution.* (a) We denote $[x, y] := xyx^{-1}y^{-1}$. If $f : G \to G$ is a homomorphism, then

$$f\left([x, y]\right) = f\left(xyx^{-1}y^{-1}\right) = f(x)\, f(y)\, f(x)^{-1}\, f(y)^{-1} = \left[f(x), f(y)\right]. \tag{3.22}$$

Therefore, $f(U) \subseteq U$. As a result,

$$f\left(G'\right) = f\left(\langle U \rangle\right) \subseteq \langle U \rangle = G'. \tag{3.23}$$

For any $g \in G$, $x \mapsto gxg^{-1}$ is a homomorphism, so $gG'g^{-1} \subseteq G'$ for any $g \in G$. Hence, $G' \trianglelefteq G$.

(b)

$$\begin{aligned} \left(xG'\right)\left(yG'\right) = \left(yG'\right)\left(xG'\right) &\iff (xy)\,G' = (yx)\,G' \\ &\iff (yx)^{-1}\,(xy) \in G' \\ &\iff x^{-1}y^{-1}xy \in G', \end{aligned} \tag{3.24}$$

which is true! Hence, $G/G'$ is abelian.

■

**Exercise 3.8.** Let $G$ be a group. Show that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

*Solution.* First, we'll show that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. Let $\tau_g, \tau_h \in \mathrm{Inn}(G)$, where

$$\tau_g\,(x) = gxg^{-1}, \quad \tau_h\,(x) = hxh^{-1}. \tag{3.25}$$

Then

$$(\tau_g \circ \tau_h)\,(x) = \tau_g\left(hxh^{-1}\right) = g\left(hxh^{-1}\right)g^{-1} = (gh)\,x\,(gh)^{-1} = \tau_{gh}(x). \tag{3.26}$$

Hence, $\tau_g \circ \tau_h = \tau_{gh} \in \mathrm{Inn}(G)$. Furthermore, we claim that $\tau_g^{-1} = \tau_{g^{-1}}$.

$$\tau_g \circ \tau_{g^{-1}} = \tau_{gg^{-1}} = \tau_e = \mathrm{id}_G, \quad \tau_{g^{-1}} \circ \tau_g = \tau_{g^{-1}g} = \tau_e = \mathrm{id}_G\,. \tag{3.27}$$

Hence, $\tau_g^{-1} = \tau_{g^{-1}} \in \mathrm{Inn}(G)$.

Now we show $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Let $\varphi \in \mathrm{Aut}(G)$, and $\tau_g \in \mathrm{Inn}(G)$.

$$\left(\varphi \circ \tau_g \varphi^{-1}\right)(x) = \varphi\left(g \cdot \varphi^{-1}(x) \cdot g^{-1}\right) = \varphi(g) \cdot x \cdot \varphi(g)^{-1} = \tau_{\varphi(g)}(x). \tag{3.28}$$

Hence, $\varphi \circ \tau_g \varphi^{-1} = \tau_{\varphi(g)} \in \mathrm{Inn}(G)$, proving that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. ■

**Exercise 3.9.** Give an example of a group $G$ and subgroups $K \subset H \subset G$, such that $K$ is a normal subgroup of $H$ and $H$ is a normal subgroup of $G$, but $K$ is not a normal subgroup of $G$.

*Solution.* Consider

$$G = D_4 = \left\{e, r, r^2, r^3, s, sr, sr^2, sr^3\right\}, \tag{3.29}$$

$$H = \left\{e, r^2, s, sr^2\right\}, \tag{3.30}$$

$$K = \{e, s\}\,. \tag{3.31}$$

Then

$$[G : H] = [H : K] = 2, \tag{3.32}$$

so $K \trianglelefteq H \trianglelefteq G$. But $K \not\trianglelefteq G$, since

$$rsr^{-1} = r\left(sr^{-1}\right) = r\left(rs\right) = r^2 s \notin K. \tag{3.33}$$

Therefore, $K$ is not a normal subgroup of $G$. ■

**Exercise 3.10.** Let $H, K$ be normal subgroups of a group $G$ with $H \cap K = \{1\}$. Show that

$$hk = kh \quad \text{for all } h \in H,\ k \in K. \tag{3.34}$$

*Solution.* Consider the element $hkh^{-1}k^{-1}$.

$$hkh^{-1}k^{-1} = \left(hkh^{-1}\right)k^{-1} \in K, \tag{3.35}$$

by the normality of $K$. Again,

$$hkh^{-1}k^{-1} = h\left(kh^{-1}k^{-1}\right) \in H, \tag{3.36}$$

by the normality of $H$. Therefore, $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, so

$$hkh^{-1}k^{-1} = e \implies hk = kh. \tag{3.37}$$

■

**Exercise 3.11.** Let

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix} \in S_9. \tag{3.38}$$

Find the cycle decomposition of $\sigma$, find the cycle type of $\sigma$, and write an element of $S_9$ which is conjugated to $\sigma$.

*Solution.* One can check that

$$1 \to 2 \to 3 \to 4 \to 5 \to 1, \quad 8 \to 9 \to 8, \tag{3.39}$$

and $6, 7$ are fixed points. Therefore,

$$\sigma = (1\ 2\ 3\ 4\ 5)\,(6)\,(7)\,(8\ 9)\,. \tag{3.40}$$

So its cycle-type is $(5, 2, 1, 1)$. Any element of this cycle-type will be conjugate to $\sigma$, i.e. any

$$\tau = (a_1\ a_2\ a_3\ a_4\ a_5)\,(a_6)\,(a_7)\,(a_8\ a_9) \tag{3.41}$$

is conjugate to $\sigma$. ■

**Exercise 3.12.** In the following, verify if the maps $\varphi : G \to G$ are homomorphisms of groups. If they are, determine their kernel.

(a) $G = (\mathbb{R} \setminus \{0\},\ \cdot\ )$, the nonzero real numbers with multiplication, $\varphi(x) = x^2$.

(b) $G = (\mathbb{R}, +)$, the real numbers with addition. $\varphi(x) = x + 1$.

(c) $G$ is an abelian group, $\varphi(x) = x^3$.

*Solution.* (a) Yes, $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$, $x \mapsto x^2$ is a homomorphism, since

$$\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\,\varphi(y). \tag{3.42}$$

Its kernel is

$$\operatorname{Ker}\varphi = \left\{x \in \mathbb{R}^\times \mid \varphi(x) = 1\right\} = \left\{x \in \mathbb{R}^\times \mid x^2 = 1\right\} = \{1, -1\}. \tag{3.43}$$

(b) $\varphi : (\mathbb{R}, +) \to (\mathbb{R}, +)$, $x \mapsto x + 1$ is not a homomorphism, since $\varphi(0) \neq 0$.

(c) If $G$ is abelian, $\varphi : G \to G$, $x \mapsto x^3$ is a homomorphism, since

$$\varphi(xy) = (xy)^3 = (xy)(xy)(xy) = (xxx)(yyy) = x^3y^3 = \varphi(x)\,\varphi(y). \tag{3.44}$$

Its kernel is

$$\operatorname{Ker}\varphi = \left\{x \in G \mid x^3 = e\right\} = \{x \in G \mid \operatorname{ord}(x) = 1 \text{ or } 3\}. \tag{3.45}$$

■

**Exercise 3.13.** Let $G$ be a group, let $\varphi : G \to G$ be an automorphism, and let $Z(G)$ be the center of $G$. Show

$$\varphi(Z(G)) \subseteq Z(G). \tag{3.46}$$

*Solution.* For $z \in Z(G)$, $z$ commutes with every $x \in G$. Hence,

$$zx = xz \implies \varphi(zx) = \varphi(xz)\varphi(z)\varphi(x) = \varphi(x)\varphi(z). \tag{3.47}$$

Since $\varphi$ is an automorphism, given any $g \in G$, we can find $x \in G$ such that $\varphi(x) = g$. Hence, for any $g \in G$,

$$\varphi(z)\ g = g\ \varphi(z), \tag{3.48}$$

i.e. $\varphi(z) \in Z(G)$, proving that $\varphi(Z(G)) \subseteq Z(G)$. ■

In fact, $\varphi(Z(G)) = Z(G)$. The other containment can be shown using the fact that $\varphi^{-1}$ is also an automorphism, so $\varphi^{-1}(Z(G)) \subseteq Z(G)$. As a result,

$$Z(G) = \varphi\left(\varphi^{-1}(Z(G))\right) \subseteq \varphi(Z(G)). \tag{3.49}$$

**Exercise 3.14.** Let $G$ be a cyclic group of prime order. Determine $\operatorname{Aut}(G)$.

*Solution.* For $G = \mathbb{Z}_p$, we claim that $\mathrm{Aut}(G) \cong \mathbb{Z}_p^\times$. Define

$$\begin{aligned} \varphi : \mathrm{Aut}\left(\mathbb{Z}_p\right) &\to \mathbb{Z}_p^\times \\ f &\mapsto f(1). \end{aligned} \tag{3.50}$$

This is a homomorphism since

$$\varphi\left(f \circ g\right) = \left(f \circ g\right)(1) = f\left(g(1)\right) = f\left(g(1) \cdot 1\right) = g(1)f(1) = f(1)g(1) = \varphi(f)\varphi(g). \tag{3.51}$$

It's injective because if $f \in \operatorname{Ker}\varphi$, then $f\left(1\right) = 1$, and then $f\left(a\right) = a$ for each $a \in \mathbb{Z}_p$, i.e. $f = \mathrm{id}$.

Furthermore, $\varphi$ is surjective, because given any $b \in \mathbb{Z}_p^\times$, we can define an automorphism $f\left(a\right) = ab$, for which $f\left(1\right) = b$. Hence, $\varphi$ is an isomorphism. ■

**Exercise 3.15.** If $G/Z(G)$ is cyclic, then $G$ is abelian.

*Solution.* For simplicity of notations, we'll denote $N := Z(G)$. Since $G/N$ is cyclic,

$$G/N = \langle xN \rangle = \left\{N, xN, x^2N, \ldots, x^nN\right\}. \tag{3.52}$$

Let's take any two element $g, h \in G$. Since the cosets in $G/N$ partition $G$, we must have that $g = x^i z_1$ and $h = x^j z_2$ for some $z_1, z_2 \in N = Z(G)$. Then

$$\begin{aligned} gh &= \left(x^i z_1\right)\left(x^j z_2\right) = x^i\left(z_1 x^j\right) z_2 && (3.53)\\ &= x^i\left(x^j z_1\right) z_2 = x^j x^i\left(z_1 z_2\right) && (3.54)\\ &= x^j\left[\left(x^i z_1\right) z_2\right] = x^j\left[z_2\left(x^i z_1\right)\right] && (3.55)\\ &= \left(x^j z_2\right)\left(x^i z_1\right) = hg. && (3.56) \end{aligned}$$

Hence, $G$ is abelian. ■

**Exercise 3.16.** An $r$-cycle is even if and only if $r$ is odd.

*Solution.*

$$\left(a_1\ a_2\ \cdots a_r\right) = \left(a_1\ a_2\right)\left(a_2\ a_3\right)\cdots\left(a_{r-1}\ a_r\right), \tag{3.57}$$

so a $r$-cycle is a product of $r-1$ transitions. So it is even if and only if $r-1$ is even, i.e. $r$ is odd. ■

**Exercise 3.17.** Let $G$ be a group of order 30.

(a) Show a 3-Sylow or a 5-Sylow subgroup is normal in $G$.

(b) Show every 3-Sylow and every 5-Sylow subgroup is normal in $G$.

(c) Show $G$ has a normal subgroup of order 15.

*Solution.* We prove some preliminary result first.

**Claim 3.1:** If $N \trianglelefteq G$, and $H \trianglelefteq N$ is a $p$-Sylow subgroup of $N$, then $H \trianglelefteq G$.

*Proof.* Since $H \trianglelefteq N$, $n_p(N) = 1$. Then for any $g \in G$,

$$gHg^{-1} \subseteq gNg^{-1} = N. \tag{3.58}$$

Hence, $gHg^{-1}$ is a $p$-Sylow subgroup of $N$, since $\left|gHg^{-1}\right| = |H|$. But since $n_p(N) = 1$, we must have that $gHg^{-1} = H$, for any $g \in G$. As a result, $H \trianglelefteq G$. □

(a) Assume for the sake of contradiction that neither a 3-Sylow subgroup nor a 5-Sylow subgroup is normal. Then $n_3, n_5 > 1$.

Since $n_5 \mid 6$ and $n_5 \equiv 1 \pmod 5$, then we must have $n_5 = 6$. Therefore, there are $6 \times 4 = 24$ elements of order 5 (since the 5-Sylow subgroups intersect trivially, because the non-identity elements generate the whole subgroup since it's a cyclic group). Hence,

$$2n_3 = (\text{number of elements of order } 3) \leq 30 - 24 - 1 = 5, \tag{3.59}$$

implying that $n_3 \leq 2$. Since $n_3 \equiv 1 \pmod 3$, we must have $n_3 = 1$.

(b) We have shown earlier that $n_3 = 1$. Now we'll show that $n_5 = 1$. Let $H_3$ be the 3-Sylow subgroup and $H_5$ be a 5-Sylow subgroup. Consider $H = H_3H_5 \leq G$. Then

$$|H| = \frac{|H_3|\,|H_5|}{|H_3 \cap H_5|} = 15, \tag{3.60}$$

and from the proof of Exercise 3.24, we conclude that $H$ is cyclic. Since $[G : H] = 2$, $H$ is normal in $G$. Furthermore, since $H$ is cyclic, it has a unique 5-Sylow subgroup, which is $H_5$. Therefore, by Claim 3.1, $H_5 \trianglelefteq G$, i.e. $n_5(G) = 1$.

(c) As before, we consider the subgroup $H = H_3H_5 \leq G$, which has order 15, i.e. its index is 2. Therefore, it's normal.

■

**Exercise 3.18.** If $G$ is a group of order 385, show that its 11-Sylow subgroup is normal and its 7-Sylow subgroup is in the center of $G$.

*Solution.* $|G| = 385 = 5 \cdot 7 \cdot 11$. $n_{11} \mid 35$, so

$$n_{11} \in \{1, 5, 7, 35\}, \tag{3.61}$$

and $n_{11} \equiv 1 \pmod{11}$ forces that we must have $n_{11} = 1$. Hence, the 11-Sylow subgroup is normal. Now, $n_7 \mid 55$ gives

$$n_7 \in \{1, 5, 11, 55\}, \tag{3.62}$$

and $n_7 \equiv 1 \pmod 7$ forces that we must have $n_7 = 1$. Hence, the 7-Sylow subgroup $H$ is normal.

**Claim 3.2:** If $H \trianglelefteq G$, then $C_G(H) \trianglelefteq G$ and $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

*Proof.* Consider the action of $G$ on $H$ by conjugation. This gives rise to a group homomorphism

$$\begin{aligned} \Psi : G &\to \mathrm{Aut}(H) \\ g &\mapsto \left(h \mapsto ghg^{-1}\right). \end{aligned} \tag{3.63}$$

Then

$$\begin{aligned} \mathrm{Ker}\,\Psi &= \left\{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\right\} && (3.64) \\ &= \{g \in G \mid gh = hg \text{ for all } h \in H\} = C_G(H). && (3.65) \end{aligned}$$

Hence, $C_G(H) \trianglelefteq G$ and by the First isomorphism theorem, $G/C_G(H)$ is isomorphic to $\mathrm{im}\,\Psi \leq \mathrm{Aut}(H)$. □

Now, by Claim 3.2, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. Since $H \cong \mathbb{Z}_7$, by Exercise 3.14, $|\mathrm{Aut}(H)| = 6$. Therefore,

$$|G/C_G(H)| \,\Big|\, |\mathrm{Aut}(H)| = 6. \tag{3.66}$$

But $|G|$ is coprime with 6, and hence so is $|G/C_G(H)| = \frac{|G|}{|C_G(H)|}$. Therefore,

$$|G/C_G(H)| = 1 \implies G = C_G(H). \tag{3.67}$$

So every element of $G$ commutes with every element of $H$, proving that $H \leq Z(G)$. ■

*Alternate Solution.* We can also finish without using Claim 3.2. As before, we show $n_7 = 1$, and hence, the 7-Sylow subgroup $H$ is normal.

**Claim 3.3:** The size of conjugacy class divides $|G|$.

*Proof.* Let $G$ act on itself by conjugation. Then $\mathrm{Orb}(g)$ is the conjugacy class $\mathrm{Conj}_G(g)$ of $g$. Then by Orbit-Stabilizer theorem,

$$|G| = |\mathrm{Orb}(g)|\,|\mathrm{Stab}(g)| = |\mathrm{Conj}_G(g)|\,|\mathrm{Stab}(g)|\,. \tag{3.68}$$

□

Since normal subgroups consist of conjugacy classes (i.e. if one element of a conjugacy class is inside the normal subgroup, then so is the entire conjugacy class), the 7-Sylow subgroup $H$

consists of conjugacy classes. The possible size of the conjugacy classes are the divisors of 385, so the possible sizes are

$$1, 5, 7, 11, \ldots. \tag{3.69}$$

If $H$ contains a nontrivial conjugacy class (i.e. conjugacy class of size $> 1$), then it must be of size 5. But then there is a non-identity element $g \in H$ which has trivial conjugacy class, i.e. it's in the center.

Since $H \cong \mathbb{Z}_7$, every non-identity element generates $H$, so $g \in Z(G)$ implies $H = \langle g \rangle \subseteq Z(G)$. ■

**Exercise 3.19.** Let $G$ be a group of order 231. Show the 11-Sylow subgroup is in the center of $G$.

*Solution.* $|G| = 231 = 3 \cdot 7 \cdot 11$. Now, $n_{11} \mid 21$ gives

$$n_7 \in \{1, 3, 7, 21\}, \tag{3.70}$$

and $n_{11} \equiv 1 \pmod{11}$ forces that we must have $n_{11} = 1$. Hence, the 11-Sylow subgroup $H$ is normal. Now, by Claim 3.2, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. Since $H \cong \mathbb{Z}_{11}$, by Exercise 3.14, $|\mathrm{Aut}(H)| = 10$. Therefore,

$$|G/C_G(H)| \,\Big|\, |\mathrm{Aut}(H)| = 10. \tag{3.71}$$

But $|G|$ is coprime with 10, and hence so is $|G/C_G(H)| = \frac{|G|}{|C_G(H)|}$. Therefore,

$$|G/C_G(H)| = 1 \implies G = C_G(H). \tag{3.72}$$

So every element of $G$ commutes with every element of $H$, proving that $H \leq Z(G)$. ■

*Alternate Solution.* As before, we show $n_{11} = 1$, and hence, the 11-Sylow subgroup $H$ is normal.

> **Claim 3.4:** If $H \trianglelefteq G$ is a cyclic normal subgroup and $|H| = p$ is prime, then for any two non-identity elements $x, y \in H$, $|\mathrm{Conj}_G(x)| = |\mathrm{Conj}_G(y)|$.
>
> *Proof.* If $x, y$ belong to the same conjugacy class, then we are done. Else, we define a function $f : \mathrm{Conj}_G(x) \to \mathrm{Conj}_G(y)$ as follows: since $H = \langle x \rangle$, $y = x^k$ for some $0 < k < p$. So we define $f(z) = z^k$ for every $z \in \mathrm{Conj}_G(x)$. This is well-defined since
>
> $$f\left(gxg^{-1}\right) = \left(gxg^{-1}\right)^k = gx^k g^{-1} = gyg^{-1} \in \mathrm{Conj}_G(y). \tag{3.73}$$
>
> This is surjective, since any $gyg^{-1} \in \mathrm{Conj}_G(y)$ is just the image of $gxg^{-1}$. Therefore, $|\mathrm{Conj}_G(x)| \geq |\mathrm{Conj}_G(y)|$. Switching $x$ and $y$ in the above argument, we obtain $|\mathrm{Conj}_G(y)| \geq |\mathrm{Conj}_G(x)|$. □

The possible size of the conjugacy classes are the divisors of 231, so the possible sizes are

$$1, 3, 7, 11, \ldots. \tag{3.74}$$

The conjugacy classes of the non-identity elements are all the same. Hence, the size of their conjugacy class must divide $|H| - 1 = 10$. The only common element of divisors of 10 and divisors of $|G| = 231$ is 1. Hence, all non-identity elements are in a singleton conjugacy class, i.e. they are in the center! ■

**Exercise 3.20.** If $G$ is a group of order $p^2q$ with $p$ and $q$ primes, show that $G$ has a nontrivial normal subgroup.

*Solution.* We'll first consider the case $p^2q = 12$. Assume the contrary. Note that $12 = 2^2 \times 3$. Since $n_3 \mid 4$ and $n_3 > 1$ (since we assumed the group is simple) and $n_3 \equiv 1 \pmod 3$, we must have that $n_3 = 4$. This gives

$$(\text{number of elements of order } 3) = n_3(3-1) = 4 \cdot 2 = 8. \tag{3.75}$$

The 2-Sylow subgroups can't intersect any of the 3-Sylow subgroups. The identity element together with the other 3 elements form one 2-Sylow subgroup. Therefore, we don't have any room for any other 2-Sylow subgroups, implying $n_2 = 1$.

Now, we consider the general case: Assume for the sake of contradiction that ther exists a simple group $G$ with $|G| = p^2q$. Note that

$$p + 1 \leq n_p \leq q. \tag{3.76}$$

The first bound follows from the fact that $n_p \neq 1$, and the second bound is given by $n_p \mid q$. Now, note that $n_q \mid p^2$ and $n_q > q > p$, so we must have $n_q = p^2$. This gives us

$$p^2 \equiv 1 \pmod q \implies q \mid (p-1)(p+1). \tag{3.77}$$

Since $q > p$, the scenario $q \mid p-1$ is impossible, so we must have $q \mid p+1$. But that way $q \leq p+1$. But we already know $q \geq p+1$. Therefore, $q = p+1$. This can only happen if $p = 2$, $q = 3$, i.e. $G = 12$, which has already been done! ■

**Exercise 3.21.** How many elements of order 5 are contained in a group of order 20?

*Solution.* Since $n_5 \mid 4$ and $n_5 \equiv 1 \pmod 5$, we must have $n_5 = 1$. Therefore, there exists a unique 5-Sylow subgroup. Hence, the number of elements of order 5 is 4. ■

**Exercise 3.22.** Prove: No group of order $pq$, with $p$ and $q$ prime numbers, is simple.

*Solution.* Assume for the sake of contradiction that ther exists a simple group $G$ with $|G| = pq$. WLOG, $p < q$. Then $n_q \mid p$. But $n_q = p$ is not possible since $n_q > 1$ along with

$$n_q \equiv 1 \pmod{q} \tag{3.78}$$

would imply

$$n_q \geq q + 1 > p. \tag{3.79}$$

Hence, $n_q = 1$, and hence the $q$-Sylow subgroup is normal. ■

**Exercise 3.23.** Let $G$ be a group of order $p^m r$. Show $G$ contains a subgroup of order $p^e$ for every $e \leq m$.

*Solution.* We proceed by induction on $e$. The base case $e = 0$ is trivial. Suppose $H$ is a subgroup of order $p^e < p^m$, we shall construct a subgroup of order $p^{e+1}$.

**Claim 3.5** ($p$-group lemma)**:** If a $p$-group (group of order $p^n$) acts on a set $S$, then if $N$ is number of fixed points (i.e. singleton orbits) of this action,

$$N \equiv |S| \pmod{p}. \tag{3.80}$$

*Proof.* By Orbit-Stabilizer theorem, the possible orbit sizes are $1, p, p^2, \ldots, p^n$. Then

$$|S| = \sum_{\text{orbits}} |\mathrm{Orb}(x)| \equiv \sum_{\text{singleton orbits}} |\mathrm{Orb}(x)| = N \pmod{p}. \tag{3.81}$$

□

**Claim 3.6** (Normalizer lemma)**:** If $H$ is a $p$-subgroup of $G$, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}. \tag{3.82}$$

*Proof.* Let $H$ act on the left cosets $G/H$ by left multiplication

$$h \cdot (gH) = (hg)\, H. \tag{3.83}$$

$gH$ is a fixed-point of this action if and only if

$$\begin{aligned} h \cdot (gH) = gH \text{ for all } h \in H &\iff \left(g^{-1}hg\right) H = H \text{ for all } h \in H && (3.84)\\ &\iff g^{-1}hg \in H \text{ for all } h \in H && (3.85)\\ &\iff g \in N_G(H). && (3.86) \end{aligned}$$

Therefore, the fixed points are precisely the cosets in $N_G(H)/H$. As a result, the number of fixed points is $[N_G(H) : H]$, and hence, by $p$-group lemma, $[N_G(H) : H] \equiv [G : H] \pmod{p}$. □

Now, since $H \trianglelefteq N_G(H)$, consider the quotient group $N_G(H)/H$. Since $p \mid [G:H] = p^{m-e}r$, by Normalizer lemma, $p \mid |N_G(H)/H|$. Therefore, by Cauchy's theorem, we can find an element of order $p$ in $N_G(H)/H$.

Say $aH \in N_G(H)/H$ is an element of order $p$. Then $a^p \in H$, since it's of order $p$. Now, define

$$H' = \bigcup_{i=0}^{p-1} a^i H. \tag{3.87}$$

Then $H' \leq G$, because if we take $a^i h, a^j h_\prime \in H'$ for $h, h_\prime \in H$,

$$\left(a^i h\right)\left(a^j h_\prime\right)^{-1} = a^i h\ h_\prime^{-1} a^{-j} = a^i\ a^{-j}\ h' \in H' \tag{3.88}$$

for some $h' \in H$, since $a^{-j} \in N_G(H)$. So $H' \leq G$. Finally,

$$\left|H'\right| = \sum_{i=0}^{p-1} \left|a^i H\right| = \sum_{i=0}^{p-1} |H| = p\,|H| = p^{e+1}. \tag{3.89}$$

■

**Exercise 3.24.** Classify the groups of order 33.

*Solution.* We shall prove a general statement:

If $G$ is a group of order $pq$ and $p < q$ primes with $q \not\equiv 1 \pmod{p}$, then $G \cong \mathbb{Z}_{pq}$.

By the proof of Exercise 3.22, $n_q = 1$. $n_p \mid q$ and $q \not\equiv 1 \pmod{p}$ implies $n_p = 1$.

Therefore, $H_1 = \langle a \rangle, H_2 = \langle b \rangle$, the $p$-Sylow subgroup and the $q$-Sylow subgroup, respectively, are normal in $G$. Their intersection is trivial, since their orders are coprime. Therefore, $a$ and $b$ commute, since

$$aba^{-1}b^{-1} = \left(aba^{-1}\right)b^{-1} = a\left(ba^{-1}b^{-1}\right) \in H_1 \cap H_2 = \{e\}. \tag{3.90}$$

Now, $a$ and $b$ commute, their orders are coprime, so $\operatorname{ord}(ab) = pq$. Indeed,

$$\begin{aligned}
(ab)^n = a^n b^n = e &\iff a^n = b^{-n} \in H_1 \cap H_2 = \{e\} && (3.91)\\
&\iff a^n = b^n = e && (3.92)\\
&\iff p \mid n \text{ and } q \mid n. && (3.93)
\end{aligned}$$

So $n = pq$ is the smallest value to have $(ab)^n = e$. Now since $\operatorname{ord}(ab) = pq$, $G$ is cyclic!

Now, for $|G| = 33 = 3 \times 11$, and $11 \not\equiv 1 \pmod{3}$, so any group of order 33 is cyclic. ■

## §4 Problems on Rings from Lothar Göttsche's Notes

**Exercise 4.1.** Let $R$ be a ring with 1, and let $a \in R$ be a unit. Show that there is a *unique* $b \in R$ with $ab = ba = 1$.

*Solution.* If $a$ is a unit, there exists $b \in R$ such that $ab = ba = 1$ (by definition). To show uniqueness, suppose another $b' \in R$ exists, with $ab' = b'a = 1$. Then

$$b = b \cdot 1 = b\left(ab'\right) = (ba)\, b' = 1 \cdot b' = b'. \tag{4.1}$$

So the $b$ is unique! ■

**Exercise 4.2.** Show that the units in $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$.

*Solution.* Let $a + ib \in \mathbb{Z}[i]$ be a unit. Then

$$(a + ib)(c + id) = 1 \tag{4.2}$$

for some $c + id \in \mathbb{Z}[i]$. Taking modulus squared on both sides, we get

$$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = 1. \tag{4.3}$$

$a^2 + b^2 \in \mathbb{Z}_{\geq 0}$ that divides 1. Therefore, it has to be equal to 1. Now,

$$a^2 + b^2 = 1 \implies (a, b) = (\pm 1, 0), (0, \pm 1), \tag{4.4}$$

which corresponds to $1, -1, i, -i$. It's easy to check that they are units indeed. ■

**Exercise 4.3.** Show: The odd integers with usual addition and multiplication are not a ring.

*Solution.* The additive identity is not in the set, so it's not an abelian group with respect to addition. ■

**Exercise 4.4.** Let $R$ be a ring and $a, b \in R$. Show $(a + b)^2 = a^2 + ab + ba + b^2$ (using only the definitions).

*Solution.*

$$(a + b)^2 = (a + b)(a + b) = (a + b)\, a + (a + b)\, b = a^2 + ba + ab + b^2. \tag{4.5}$$

■

**Exercise 4.5.** An element $a$ in a ring $R$ is called *nilpotent* if there is an $n \in \mathbb{Z}_{>0}$ with $a^n = 0$. Show: if $a$ is nilpotent, then $1 + a$ is a unit.

*Solution.* We can assume WLOG that $n$ is odd, because if $n$ is even, $a^{n+1} = a^n \cdot a = 0 \cdot a = 0$, and we can just replace $n$ by $n+1$.

$$1 = 1 + a^n = (1+a)\left(1 - a + a^2 - a^3 + \cdots + a^{n-1}\right). \tag{4.6}$$

■

**Exercise 4.6.** Show: In a commutative ring $R$, $a+b$ is nilpotent if $a$ and $b$ are nilpotent. Show that this may be false if $R$ is not commutative.

*Solution.* Suppose $a^n = b^m = 0$ for $n, m \in \mathbb{Z}_{>0}$. Since the ring is commutative, we can apply Binomial formula:

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i}. \tag{4.7}$$

If $i < m$, $m+n-i \geq n$, so the term $b^{m+n-i} = 0$. If $i \geq m$, then $a^i = 0$. Thus all the summands are 0, and hence $(a+b)^{m+n} = 0$.

If $R$ is not commutative, say $R = \mathrm{Mat}_{2\times 2}$, then this assertion may not be true. For example, take

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}. \tag{4.8}$$

Then $A^2 = B^2 = 0$. But

$$A + B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.9}$$

is an invertible element, so it can't be nilpotent. ■

**Exercise 4.7.** Show that a commutative ring $R$ is an integral domain if and only if for all $a, b, c \in R$ with $a \neq 0$, the relation $ab = ac$ implies $b = c$.

*Solution.* Suppose $R$ is an ID. Let $a, b, c \in R$ with $a \neq 0$. Then

$$ab = ac \implies a(b-c) = ab - ac = 0 \implies b - c = 0 \implies b = c. \tag{4.10}$$

Conversely, suppose for all $a, b, c \in R$ with $a \neq 0$, the relation $ab = ac$ implies $b = c$. Suppose $xy = 0$ for $x, y \in R$. We need to show that this implies $x = 0$ or $y = 0$. If $x \neq 0$, then

$$xy = 0 = x \cdot 0 \implies y = 0. \tag{4.11}$$

Therefore, $R$ is an ID. ■

**Exercise 4.8.** Let $U$ be a set, and let $R$ be the set of subsets of $U$. Addition and multiplication on $R$ are defined by

$$A + B := A \cup B, \qquad A \cdot B := A \cap B. \tag{4.12}$$

Prove or disprove: $R$ a ring.

*Solution.* No. Let's first examine what's the additive identity.

$$A = A + 0 = A \cup 0. \tag{4.13}$$

for all $A \subseteq U$, so we have that $0 \subseteq A$ for all $A$. Then we must have $0 = \varnothing$.

Given any set $A$, we need to have its additive inverse, i.e. another set $B$ such that $A + B = 0$. This means

$$A \cup B = \varnothing, \tag{4.14}$$

which only happens if $A = B = \varnothing$. Therefore, this does **NOT** form a ring since the nonempty elements don't have additive inverses. ■

**Exercise 4.9.** Let $U$ be a set, and let $R$ be the set of subsets of $U$. Addition and multiplication on $R$ are defined by

$$A + B := (A \setminus B) \cup (B \setminus A), \qquad A \cdot B := A \cap B. \tag{4.15}$$

Prove or disprove: $R$ a ring.

*Solution.* Yes, $R$ is a ring.

- Addition is associative: since $A \triangle B$ denotes the elements that belong to exactly one of the sets $A$ or $B$. Therefore, $(A \triangle B) \triangle C$ denotes the elements that belong to exactly one of the sets $A \triangle B$ or $C$.

  If an element of $(A \triangle B) \triangle C$ belongs to $C$, it's not in $A \triangle B$, so it's in both $A, B$ or neither of $A, B$. On the other hand, if an element is not in $C$, then it's in $(A \triangle B)$.

  Therefore, $(A \triangle B) \triangle C$ consists of elements that belong to exactly one of $A, B, C$ or all three. Similarly, $A \triangle (B \triangle C)$ also consists of elements that belong to exactly one of $A, B, C$ or all three. Hence, they are the same!

- Additiion is clearly commutative.

- $\varnothing$ is the additive identity, since

$$A + \varnothing = (A \setminus \varnothing) \cup (\varnothing \setminus A) = A. \tag{4.16}$$

- Every set is its own additive inverse, since

$$A + A := (A \setminus A) \cup (A \setminus A) = \varnothing. \tag{4.17}$$

- Multiplication is clearly associative and commutative.

- $U$ is the multiplicative identity, since

$$A \cdot U = A \cap U = A. \tag{4.18}$$

- We have to verify the distributive law:

$$A \cap (B \triangle C) = (A \cap B) \triangle (A \triangle C). \tag{4.19}$$

  This is clearly true, since $A \cap (B \triangle C)$ consists of elements that are in $A$ and exactly one of $B$ or $C$. That means they are in $A \cap B$ or $A \cap C$ (not both), and those elements are precisely the ones that make up $(A \cap B) \triangle (A \triangle C)$.

Therefore, $R$ is a commutative unital ring. ■

**Exercise 4.10.** Let $\mathrm{GL}(2, \mathbb{R}) := \{A \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \mid \det(A) \neq 0\}$. Is $\mathrm{GL}(2, \mathbb{R})$ a subring of $M_{2\times 2}(\mathbb{R})$?

*Solution.* No, because $\mathrm{GL}(2, \mathbb{R})$ is not closed under addition, so it's not an additive subgroup of $\mathrm{Mat}_{2\times 2}(\mathbb{R})$. Indeed,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \tag{4.20}$$

where both the summands are in $\mathrm{GL}(2, \mathbb{R})$, but the sum is not. ■

**Exercise 4.11.** Let $R$ be a ring with $a^2 = a$ for all $a \in R$. Show: $R$ is commutative.

*Solution.* Since $(a+b)^2 = a + b$, we have

$$a + b = (a+b)^2 = a^2 + b^2 + ab + ba = a + b + ab + ba \implies ab + ba = 0. \tag{4.21}$$

Then

$$2a = (2a)^2 = 4a^2 = 4a \implies a + a = 0 \implies a = -a. \tag{4.22}$$

Plugging it into $ab + ba = 0$, we get

$$ab = -ba = -b(-a) = ba. \tag{4.23}$$

■

**Exercise 4.12.** Determine the group of units in $\mathbb{Z}_{12}$.

*Solution.* If $a \in \mathbb{Z}_{12}$ is a unit, then there exists some $b \in \mathbb{Z}_{12}$ such that $ab = 1$, i.e.

$$ab = 1 + 12k \text{ for some } k \in \mathbb{Z}. \tag{4.24}$$

If $d = \gcd(a, 12)$, then it divides both $ab$ and $12k$, and hence it divides 1. So $d = 1$. And, if $d = 1$, by Bezout's identity, there exists $b, k \in \mathbb{Z}$ such that

$$ab - 12k = 1. \tag{4.25}$$

Hence, $ab = 1$ in $\mathbb{Z}_{12}$. Therefore, $\mathbb{Z}_{12}^{\times} = \{1, 5, 7, 11\}$, all the numbers smaller than 12 that are coprime to 12. ■

**Exercise 4.13.** Let $R$ be a ring and let $Z(R) := \{x \in R \mid xy = yx \text{ for all } y \in R\}$. Show that $Z(R)$ is a subring of $R$. $Z(R)$ is usually called the center of $R$.

*Solution.* Clearly $0 \in Z(R)$, since $0 \cdot y = y \cdot 0 = 0$ for all $y \in R$. We need to show that given $a, b \in Z(R)$, $a - b, ab \in Z(R)$. For any $y \in R$, since $a, b \in Z(R)$,

$$(a - b)\, y = ay - by = ya - yb = y\,(a - b)\,, \tag{4.26}$$

so $a - b \in Z(R)$.

$$(ab)\, y = a\,(by) = a\,(yb) = (ay)\, b = (ya)\, b = y\,(ab)\,, \tag{4.27}$$

so $ab \in Z(R)$. Hence, $Z(R)$ is a subring. ■

**Exercise 4.14.** If $R$ is a division ring, show that $Z(R)$ is a field.

*Solution.* As before, $Z(R)$ is a subring of $R$. $Z(R)$ is also a division ring, for nonzero $a \in Z(R)$,

$$ay = ya \implies a^{-1}\,(ay)\, a^{-1} = a^{-1}\,(ya)\, a^{-1} \implies ya^{-1} = a^{-1}y, \tag{4.28}$$

for every $y \in R$, so $a^{-1} \in Z(R)$. Therefore, $Z(R)$ is a division ring. Now, we just need to show that the multiplication is commutative. It's trivial since the elements of $Z(R)$ commute with every element of $R$, so in particular, they commute with elements from $Z(R)$. ■

**Exercise 4.15.** Let $R$ be an integral domain and $a, b \in R$. Assume $a^n = b^n$ and $a^m = b^m$ for two relatively prime integers $n, m$. Show that $a = b$.

*Solution.* Since $\gcd(m, n) = 1$, by Bezout's identity, there exist $x, y \in \mathbb{Z}$ such that

$$mx + ny = 1. \tag{4.29}$$

WLOG $x > 0$ and $y < 0$. Then

$$a^m = b^m \implies (a^m)^x = (b^m)^x \implies a^{mx} = b^{mx}. \tag{4.30}$$

Similarly, $a^{-ny} = b^{-ny}$. Therefore,

$$a \cdot a^{-ny} = a^{1-ny} = a^{mx} = b^{mx} = b^{1-ny} = b \cdot b^{-ny}. \tag{4.31}$$

If $a^{-ny} = b^{-ny} = 0$, then $a = b = 0$ since we're in an integral domain. If $a^{-ny} = b^{-ny} \neq 0$, we may cancel it out to get $a = b$. ■

**Exercise 4.16.** Let $m$ be an integer which is not divisible by the square of an integer $> 1$.

(a) Show that $\mathbb{Z}[\sqrt{m}] := \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

(b) Find the units in $\mathbb{Z}[\sqrt{m}]$ for all $m < 0$.

*Solution.* (a) $\mathbb{Z}[\sqrt{m}]$ is a subring of $\mathbb{C}$, which is a field and hence it has no nonzero zero divisors. Therefore, $\mathbb{Z}[\sqrt{m}]$ also can't have nonzero zero divisors. Hence, it's an integral domain.

(b) We have already shown that for $m = -1$,

$$\mathbb{Z}\left[\sqrt{-1}\right]^\times = \mathbb{Z}[i]^\times = \{1, -1, i, -i\}. \tag{4.32}$$

Now let's assume $m = -n$ for $n > 1$. Suppose $a + b\sqrt{m} = a + ib\sqrt{n}$ is a unit. Then there exists $c, d \in \mathbb{Z}$ such that

$$\left(a + ib\sqrt{n}\right)\left(c + id\sqrt{n}\right) = 1. \tag{4.33}$$

Taking norm-squared on both sides, we get

$$\left(a^2 + nb^2\right)\left(c^2 + nd^2\right) = 1. \tag{4.34}$$

$a^2 + nb^2$ is a non-negative integer that divides 1, hence it is 1. Now, if $b \neq 0$, then

$$a^2 + nb^2 \geq nb^2 \geq n > 1. \tag{4.35}$$

Therefore, $b = 0$. But that just means $a^2 = 1$, i.e. $a = \pm 1$. Therefore, for $m = -n$ with $n > 1$,

$$\mathbb{Z}\left[\sqrt{m}\right]^\times = \{1, -1\}. \tag{4.36}$$

■

**Exercise 4.17.** Show: A finite ring with 1 (not necessarily commutative) is a division ring.

*Solution.* This is false! Consider

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}. \tag{4.37}$$

This is a finite ring with 1 (and also commutative). But this is **NOT** a division ring since 2 doesn't have any multiplicative inverse. I think the statement should be

A finite ring with 1, which doesn't have any nonzero zero-divisors, is a division ring.

Take any $a \in R$ with $a \neq 0$. Consider the set

$$\left\{a, a^2, a^3, \ldots\right\}. \tag{4.38}$$

Since our ring is finite, there must be a repitition, i.e. $a^m = a^n$ for $m < n$. After a bit of rearrangement, we get

$$0 = a^n - a^m = a^m\left(a^{n-m} - 1\right). \tag{4.39}$$

Since $a \neq 0$, $a^m \neq 0$ (this holds because the ring doesn't have any nonzero zero-divisors). Therefore,

$$a^{n-m} - 1 = 0 \implies a^{n-m} = 1 \implies a \cdot a^{n-m-1} = a^{n-m-1} \cdot a = 1, \tag{4.40}$$

implying that $a^{n-m-1} = a^{-1}$. ■

**Exercise 4.18.** Let $R$ be a commutative ring with 1. Determine the units in $R[x]$.

*Solution.* We claim that $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ is a unit if and only if $a_0$ is a unit and $a_i$ is nilpotent for all $1 \leq i \leq n$.

Let's prove the "if" direction first. Since $R \leq R[x]$, nilpotents in $R$ are also nilpotents in $R[x]$. Since nilpotent elements form an ideal in a commutative ring (Exercise 4.33), $\sum_{i=1}^{n} a_i x^i$ is nilpotent in $R[x]$. If $n$ is a nilpotent and $u$ is a unit, then $u + n$ is a unit, since

$$u + n = u\left(1 + u^{-1}n\right), \tag{4.41}$$

and $u^{-1}n$ is a nilpotent (since nilpotents form an ideal, Exercise 4.33), so $1 + u^{-1}n$ is a unit by Exercise 4.5. Since units form a group under multiplication, $u\left(1 + u^{-1}n\right)$ is a unit. Now, $a_0$ is a unit, and $\sum_{i=1}^{n} a_i x^i$ is nilpotent, so their sum $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ is a unit.

Conversely, suppose $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ is a unit. Let $g(x) = \sum_{j=1}^{m} b_j x^j$ is its inverse. Then

$$1 = f(x)g(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=1}^{m} b_j x^j\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_i b_j\right) x^k \tag{4.42}$$

Equating the coefficients of $x^0$ on both sides, we get $a_0 b_0 = 1$, i.e. $a_0$ is a unit (and so is $b_0$). Equating the coefficients of $x^{m+n}$ on both sides, we get

$$a_n b_m = 0. \tag{4.43}$$

We claim that $a_n^{l+1} b_{m-l} = 0$ for each $0 \leq l \leq m$. We prove it by induction on $l$. The base case $l = 0$ is shown above. Suppose it holds for $0, 1, \ldots, l-1$. Looking at the coefficient of $x^{m+n-l}$, we get

$$a_n b_{m-l} + a_{n-1} b_{m-l+1} + a_{n-2} b_{m-l+2} + \cdots + a_{n-l} b_m = 0. \tag{4.44}$$

Multiplying by $a_n^l$, we have

$$0 = a_n^{l+1} b_{m-l} + a_{n-1} a_n^l b_{m-l+1} + a_{n-2} a_n^l b_{m-l+2} + \cdots + a_{n-l} a_n^l b_m. \tag{4.45}$$

By inductive hypothesis, all $a_n^l b_{m-(l-j)} = 0$. Therefore, $a_n^{l+1} b_{m-l} = 0$. So we have proved that $a_n^{l+1} b_{m-l} = 0$ for each $0 \leq l \leq m$. Picking $l = m$, we get

$$a_n^{m+1} b_0 = 0. \tag{4.46}$$

Since $b_0$ is a unit, this proves $a_n^{m+1} = 0$, i.e. the leading coefficient of $f(x)$ is a nilpotent.

Since $f(x)$ is a unit, and $a_n x^n$ is a nilpotent in $R[x]$, $f(x) - a_n x^n$ is a unit (earlier we have shown that if $n$ is a nilpotent and $u$ is a unit, then $u + n$ is a unit). Then repeating the same steps on $f(x) - a_n x^n$, we get that $a_{n-1}$ is a nilpotent. Hence, repeating, all $a_i$'s are nilpotents. ■

**Exercise 4.19.** Let $R$ be a ring and let $I$ and $J$ be ideals in $R$. Which of the following are ideals of $R$

$$\begin{aligned} &I + J := \{u + v \mid u \in I,\, v \in J\}, \\ &I \cap J, \\ &I \cup J? \end{aligned} \tag{4.47}$$

Give a proof or a counterexample.

*Solution.* Yes, $I + J$ is an ideal of $R$. First, let's show that $I + J$ is an additive subgroup. Clearly, it contains 0, since $0 = 0 + 0$ and 0 is in both $I$ and $J$. Given $u_1 + v_1, u_2 + v_2 \in I + J$, where $u_i \in I$ and $v_i \in J$,

$$(u_1 + v_1) - (u_2 + v_2) = \underbrace{(u_1 - u_2)}_{\in I} + \underbrace{(v_1 - v_2)}_{\in J} \in I + J. \tag{4.48}$$

So $I + J$ is an additive subgroup of $R$. Now take any $r \in R$, and $u + v \in I + J$ for $u \in I$, $v \in J$.

$$r\,(u + v) = \underbrace{ru}_{\in I} + \underbrace{rv}_{\in J} \in I + J; \tag{4.49}$$

$$(u + v)\,r = \underbrace{ur}_{\in I} + \underbrace{vr}_{\in J} \in I + J. \tag{4.50}$$

So $I + J$ is an ideal of $R$.

$I \cap J$ is an ideal. Indeed, intersections of subgroups is a subgroup, so $I \cap J$ is an additive subgroup. Furthermore, given any $r \in R$ and $a \in I \cap J$,

$$ra \in I \text{ and } ra \in J, \tag{4.51}$$

since $I, J$ are ideals. Also

$$ar \in I \text{ and } ar \in J, \tag{4.52}$$

since $I, J$ are ideals. Therefore, $ar, ra \in I \cap J$, so $I \cap J$ is an ideal.

$I \cup J$ is not, in general, an ideal of $R$. For instance, if

$$R = \mathbb{Z}, \quad I = 2\mathbb{Z}, \quad J = 3\mathbb{Z}, \tag{4.53}$$

$I \cup J$ contains $2, 3$, but it doesn't contain $2 + 3 = 5$. So it's not an ideal. ■

**Exercise 4.20.** Let $R$ be a noncommutative ring and $a \in R$. Show by example that $aR := \{ar \mid r \in R\}$ is not always an ideal.

*Solution.* Let $R = \mathrm{Mat}_{2\times 2}(\mathbb{R})$, and take the matrix $a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Then

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \tag{4.54}$$

So the ideal $aR$ is

$$aR = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \mid x, y \in \mathbb{R} \right\}. \tag{4.55}$$

We'll show that this is not an ideal by picking an element $b \in aR$ and $s \in R$ such that $sb \notin aR$. That will prove that $aR$ is not an ideal. We pick $b = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$, $s = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$,

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \notin aR. \tag{4.56}$$

■

**Exercise 4.21.** Let $R$ be a ring, $I \subseteq R$ an ideal.

(a) Show that $r(I) := \{r \in R \mid ra = 0 \text{ for all } a \in I\}$ is an ideal in $R$.

(b) Show that $[R : I] := \{x \in R \mid xr \in I \text{ for all } r \in R\}$ is an ideal in $R$.

*Solution.* (a) Clearly $0 \in r(I)$. To show that it's an additive subgroup, let $r, r' \in r(I)$,

$$\left(r - r'\right) a = ra - r'a = 0 - 0 = 0 \tag{4.57}$$

for all $a \in I$. Now, let $r \in r(I)$ and $s \in R$.

$$(rs)\, a = r\,(sa) = 0, \quad \text{forall } a \in I \tag{4.58}$$

since $sa \in I$ for $I$ is an ideal. Furthermore,

$$(sr)\, a = s\,(ra) = s \cdot 0 = 0. \tag{4.59}$$

Therefore, $sr, rs \in r(I)$, proving $r(I)$ is an ideal.

(b) Clearly $0 \in [R : I]$, since $0 \cdot r = 0 \in I$ for all $r \in R$. To show that it's an additive subgroup, let $x, x' \in [R : I]$,

$$\left(x - x'\right) r = xr - x'r \in I, \quad \forall\, r \in R; \tag{4.60}$$

since $xr, xr' \in I$. Therefore, $x - x' \in [R : I]$. Now, let $s \in R$ and $x \in [R : I]$.

$$(sx)\, r = s\,(xr) \in I, \tag{4.61}$$

since $xr \in I$ and $I$ is an ideal, so $s(xr) \in I$. Furthermore,

$$(xs)\, r = x\,(sr) \in I, \tag{4.62}$$

since $x \in [R : I]$. Therefore, $sx, xs \in [R : I]$, , proving $[R : I]$ is an ideal.

■

**Exercise 4.22.** Prove that a subring of an integral domain is an integral domain.

*Solution.* If there's no nonzero zero-divisor in the larger ring, there can't be any nonzero zero-divisor in the subring. ■

**Exercise 4.23.** Is there an integral domain with precisely 10 elements?

*Solution.* No. Finite integral domains are fields (Exercise 4.17), and hence, their cardinalities have to be prime powers. ■

**Exercise 4.24.** Let $R$ be a ring such that $x^3 = x$ for every $x \in R$. Show that $R$ is a commutative ring.

*Solution.* We proceed by a sequence of steps.

1. If $x^2 = 0$, then $x = 0$. Indeed, if $x^2 = 0$,

$$x = x^3 = x^2 \cdot x = 0 \cdot x = 0. \tag{4.63}$$

2. If $xy = 0$, then $yx = 0$.

$$yx = (yx)^3 = yxyxyx = y\,(xy)\,xyx = 0. \tag{4.64}$$

3. $xy = x^2y^2xy$ for all $x, y \in R$.

$$0 = yx - yx = yx - y^3x = y\left(x - y^2x\right) = \left(x - y^2x\right)y \tag{4.65}$$

by 2. Multiplying by $x^2$ to the left, we have

$$0 = x^2\left(x - y^2x\right)y = x^3y - x^2y^2xy = xy - x^2y^2xy. \tag{4.66}$$

Therefore, $xy = x^2y^2xy$.

4. $(xy - yx)yx = 0$ for all $x, y \in R$. By 3,

$$0 = x^2y^2xy - xy = x^2y^2xy - (xy)^3 = xxyyxy - xyxyxy = x\,(xy - yx)\,yxy. \tag{4.67}$$

By 2,

$$0 = (xy - yx)\,yxyx = (xy - yx)\,yxyxyx = (xy - yx)\,(yx)^3 = (xy - yx)\,yx. \tag{4.68}$$

5. $xy = yx$ for all $x, y \in R$. For this, we'll show that $(xy - yx)^2 = 0$, then we'll be done by 1.

$$\begin{aligned}(xy - yx)^2 &= (xy - yx)\,xy - (xy - yx)\,yx &(4.69)\\ &= -(yx - xy)\,xy - (xy - yx)\,yx &(4.70)\\ &= -0 - 0 = 0 &(4.71)\end{aligned}$$

by 4. Hence, we are done!

■

**Exercise 4.25.** Let $R$ be a ring with 1 and let $\varphi : R \to S$ be a surjective homomorphism of rings. Show that $\varphi(1)$ is the unit element of $S$.

*Solution.* Since $\varphi$ is surjective, any $s \in S$ is of the form $s = \varphi(r)$ for some $r \in R$. Then

$$\begin{aligned}\varphi(1) \cdot s = \varphi(1)\varphi(r) = \varphi(1 \cdot r) = \varphi(r) = s, &\tag{4.72}\\ s \cdot \varphi(1) = \varphi(r)\varphi(1) = \varphi(r \cdot 1) = \varphi(r) = s. &\tag{4.73}\end{aligned}$$

Hence, $\varphi(1)$ is the unit element of $S$. ■

**Exercise 4.26.** Let $k$ be a field. Find all automorphisms $\varphi$ of $k[x]$ with the property that $\varphi(a) = a$ for all $a \in k$.

*Solution.* Every homomorphism $f : k[x] \to k[x]$ is uniquely determined by where it sends $x$. Since $f$ is an automorphism, let $g = f^{-1}$. Suppose

$$f(x) = P(x) \in k[x] \text{ and } g(x) = Q(x). \tag{4.74}$$

Then since $f \circ g = \mathrm{id}$,

$$x = f(g(x)) = P(Q(x)). \tag{4.75}$$

The degree of $P(Q(x))$ is $\deg P \cdot \deg Q$, which has to be equal to $\deg x = 1$. Hence, both $\deg P = \deg Q = 1$. Therefore,

$$P(x) = ax + b \tag{4.76}$$

for $a, b \in k$ with $a \neq 0$. Then

$$f(x) = ax + b \tag{4.77}$$

is, indeed, invertible since its inverse is given by

$$g(x) = a^{-1}x - a^{-1}b. \tag{4.78}$$

So all such automorphisms $k[x] \to k[x]$ are of the form

$$\sum_{i=1}^{n} a_i x^i \mapsto \sum_{i=1}^{n} a_i (ax+b)^i \text{ for } a \in k^\times, b \in k. \tag{4.79}$$

■

**Exercise 4.27.** Prove that every ideal in $\mathbb{Z}[i]$ contains a nonzero integer.

*Solution.* Let $I$ be a nonzero ideal. Then pick nonzero $a + ib \in I$. Since $I$ is an ideal, it contains any element of the form $xr$ for $x \in I$ and $r \in R = \mathbb{Z}[i]$. Choosing $x = a + ib$ and $r = a - ib$, we have

$$(a+ib)(a-ib) = a^2 + b^2 \in I. \tag{4.80}$$

$a^2 + b^2$ is an integer, and its nonzero since $a^2 + b^2 = 0$ if and only if $a = b = 0$, which isn't the case as we've picked $a + ib \neq 0$. Therefore, $I$ contains a nonzero integer, namely $a^2 + b^2$. ■

**Exercise 4.28.** Show that the kernel of the homomorphism $\varphi : \mathbb{C}[x,y] \to \mathbb{C}[t] : x \mapsto t^2$, $y \mapsto t^3$ is the principal ideal generated by $y^2 - x^3$.

*Solution.* We'll have to show that $\operatorname{Ker}\varphi = \left(y^2 - x^3\right)$. The inclusion $\supseteq$ is clear, since

$$\varphi\left(y^2 - x^3\right) = \varphi(y)^2 - \varphi(x)^3 = \left(t^3\right)^2 - \left(t^2\right)^3 = 0, \tag{4.81}$$

so we have $\left(y^2 - x^3\right) \subseteq \operatorname{Ker}\varphi$.

Let $g(x,y) \in \operatorname{Ker}\varphi$. We consider $\mathbb{C}[x,y] = \mathbb{C}[x][y]$, i.e. we consider $g$ to be a polynomial in $y$, and we divide by $y^2 - x^3$ (which is a monic polynomial in $\mathbb{C}[x][y]$).

$$g(x,y) = \left(y^2 - x^3\right) q(x,y) + r(x,y), \tag{4.82}$$

with $\deg_y r(x,y) < \deg_y \left(y^2 - x^3\right) = 2$, so $\deg_y r(x,y) \leq 1$. We write

$$r(x,y) = r_0(x) + r_1(x)y, \tag{4.83}$$

where $r_0(x), r_1(x) \in \mathbb{C}[x]$. Now, since $g(x,y), y^2 - x^3 \in \operatorname{Ker}\varphi$, we have $r(x,y) \in \operatorname{Ker}\varphi$. Now,

$$0 = \varphi(r(x,y)) = r_0\left(t^2\right) + r_1(t^2)t^3. \tag{4.84}$$

The terms of $r_0\left(t^2\right)$ are all of the form $t^{\text{even}}$ and the terms of $r_1(t^2)t^3$ are all of the form $t^{\text{odd}}$. Therefore, their sum can be 0 if and only if $r_0 = r_1 = 0$, in which case $r(x,y) = 0$. In other words, $g \in \left(y^2 - x^3\right)$, proving that $\operatorname{Ker}\varphi \subseteq \left(y^2 - x^3\right)$. ■

**Exercise 4.29.** Let $R$ be a ring and $I$ an ideal in $R$. Let $\sqrt{I} := \{x \in R \mid x^n \in I \text{ for some } n > 0\}$. Show

(a) $\sqrt{I}$ is an ideal in $R$ which contains $I$. $\sqrt{I}$ is usually called the radical of $I$.

(b) $\sqrt{\sqrt{I}} = \sqrt{I}$.

*Solution.* Here, we need the hypothesis that $R$ is commutative. Without that $\sqrt{I}$ fails to be an ideal, since if $I = (0)$, the $\sqrt{I}$ is the set of all nilpotent elements, which need not be closed under addition if $R$ is non-commutative (Exercise 4.6). So we'll assume $R$ is commutative.

(a) It's clear that $I \subseteq \sqrt{I}$. Clearly, $0 \in \sqrt{I}$. To show that it's an additive subgroup, take $x, y \in \sqrt{I}$. Then $x^n, y^m \in I$ for some $m, n > 0$. Then

$$(x-y)^{m+n} = \sum_{i=0}^{m+n} \pm \binom{m+n}{i} x^i y^{m+n-i}. \tag{4.85}$$

If $i < n$, $m+n-i > m$, so $y^{m+n-i} \in I$. Since $I$ is an ideal, $x^i y^{m+n-i} \in I$. On the other hand, if $i \geq n$, $x^i \in I$, so that $x^i y^{m+n-i} \in I$. Therefore, all summands are in $I$, so $(x-y)^{m+n} \in I$, proving that $x - y \in \sqrt{I}$.

Now, for $x \in \sqrt{I}$ and $r \in R$, $x^n \in I$ for some $n > 0$. Then

$$(rx)^n = r^n x^n \in I, \tag{4.86}$$

so $rx \in \sqrt{I}$. Hence, $\sqrt{I}$ is an ideal of $R$.

(b) By (a), $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. Now, let $x \in \sqrt{\sqrt{I}}$.

$$\begin{aligned} x \in\in \sqrt{\sqrt{I}} &\implies x^n \in \sqrt{I} \text{ for some } n > 0 \\ &\implies (x^n)^m = x^{mn} \in I \text{ for some } m, n > 0 \\ &\implies x \in \sqrt{I}. \end{aligned}$$

So $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$.

■

**Exercise 4.30.** Let $R$ be a ring and let $A, B$ be ideals in $R$ such that $A \cap B = \{0\}$. Show that for all $a \in A$, $b \in B$, $ab = 0$.

*Solution.* Since $A$ is an ideal and $a \in A$, $ab \in A$. Similarly, since $B$ is an ideal and $b \in B$, $ab \in B$. Therefore, $ab \in A \cap B = \{0\}$, so $ab = 0$. ■

**Exercise 4.31.** Let $R$ be a ring (commutative with 1) and let $S$ be a subring. The *conductor* $C(S)$ of $S$ in $R$ is the set of all $\alpha \in R$ such that $\alpha R \subseteq S$.

(a) Prove that $C(S)$ is an ideal of $R$ and also an ideal of $S$.

(b) Prove that $C(S)$ is the largest ideal of $S$ which is also an ideal of $R$.

(c) Determine $C(S)$ in the following cases:

(i) $R = \mathbb{C}[x]$, $S = \mathbb{C}\left[x^2, x^3\right]$.

(ii) $R = \mathbb{Z}[\omega]$, $\omega = \dfrac{-1+\sqrt{-3}}{2}$, $S = \mathbb{Z}\left[\sqrt{-3}\right]$.

*Solution.* (a) Clearly $0 \in C(S)$, since $0R = 0 \subseteq S$. To show that it's an additive subgroup, let $\alpha_1, \alpha_2 \in C(S)$. Then for any $r \in R$,

$$(\alpha_1 - \alpha_2) r = \underbrace{\alpha_1 r}_{\in S} - \underbrace{\alpha_2 r}_{\in S} \in S. \tag{4.87}$$

For $\alpha \in C(S)$ and $r \in R$,

$$(r\alpha) R = \alpha (rR) \subseteq \alpha R \subseteq S, \tag{4.88}$$

so $r\alpha \in C(S)$. Therefore, $C(S)$ is an ideal of $R$. It's also an ideal of $S$, since $r\alpha \in C(S)$ for every $r \in R$ implies $r\alpha \in C(S)$ for every $r \in S$ as $S \leq R$.

(b) Let $I \trianglelefteq R$ and $I \subseteq S$. We'll prove that $I \subseteq C(S)$. For $a \in I$, $aR \subseteq I$ since $I \trianglelefteq R$. But $I \subseteq S$. So we have

$$aR \subseteq I \subseteq S \implies a \in C(S), \tag{4.89}$$

proving $I \subseteq C(S)$.

(c) By (b), $C(S)$ is the largest ideal of $R$ contained in $S$.

(i) Here, $S = \mathbb{C}\left[x^2, x^3\right]$ contains all the polynomials whose $x^1$ term is missing, i.e. the $x^1$ term has coefficient 0. $C(S)$ is the largest ideal of $R$ contained in $S$. So let $f(x) \in C(S) \trianglelefteq R = \mathbb{C}[x]$. Since $C(S)$ is an ideal, $xf(x) \in C(S)$.

But $C(S)$ is contained in $S$, so $xf(x)$ has $x^1$'s coefficient 0. In other words, $f(x)$ has no constant term. But $f(x) \in C(S) \subseteq S$ already implies $f(x)$ has no $x^1$ term. Therefore,

$$f(x) = a_2 x^2 + a_3 x^3 + \cdots + a_n x^n. \tag{4.90}$$

In other words, $C(S) = x^2\mathbb{C}[x]$.

(ii) Note that $\sqrt{3} = 2\omega + 1$, so

$$S = \mathbb{Z}\left[\sqrt{3}\right] = \mathbb{Z}[2\omega + 1] = \mathbb{Z}[2\omega]. \tag{4.91}$$

$C(S)$ is the largest ideal of $\mathbb{Z}[\omega]$ that is contained in $\mathbb{Z}[2\omega]$. Let $a + b\omega \in C(S)$. Since $C(S) \subseteq \mathbb{Z}[2\omega]$, we must have that $b$ is even.

Since $C(S) \trianglelefteq \mathbb{Z}[\omega]$, $\omega(a + b\omega) \in C(S) \subseteq \mathbb{Z}[2\omega]$.

$$\omega(a + b\omega) = a\omega + b\omega^2 = a\omega + b(-1 - \omega) = -b + (a - b)\omega \tag{4.92}$$

So $a - b$ is even. But we have already proved $b$ is even. So $a$ is even. Therefore, $C(S)$ is $2\mathbb{Z}[\omega]$.

■

**Exercise 4.32.** Let $I, J$ be ideals of a ring, such that $I + J = R$. Prove that $IJ = I \cap J$.

*Solution.* $R$ needs to be commutative and have 1, otherwise this fails. Let

$$R = 2\mathbb{Z}, \quad I = 4\mathbb{Z}, \quad J = 6\mathbb{Z}. \tag{4.93}$$

Then $I + J = R$. But $I \cap J = 12\mathbb{Z}$ and $IJ = 24\mathbb{Z}$. For noncommutative $R$, consider

$$R = k\langle x, y\rangle, \quad I = \langle x\rangle, \quad J = \langle x - 1\rangle. \tag{4.94}$$

Then indeed, $I + J = R$ since it contains 1. But the element $(x-1)yx \neq xy(x-1)$ is in $I \cap J$ but it's not in $IJ$.

Now, suppose $R$ is a commutative ring with 1. Let $ij \in IJ$, for $i \in I$ and $j \in J$. Then $ij \in I$ since $I$ is an ideal, and $ij \in J$ since $J$ is an ideal. Therefore, $IJ \subseteq I \cap J$.

Now, let $x \in I \cap J$. Since $I + J = R$, there exists $i \in I$ and $j \in J$ such that

$$i + j = 1. \tag{4.95}$$

Multiplying on the left by $x$,

$$xi + xj = x. \tag{4.96}$$

$x \in J$ implies $xi \in JI = IJ$. $x \in I$ implies $xj \in IJ$. Therefore, $x = xi + xj$ is in $IJ$, proving $I \cap J \subseteq IJ$. ■

Lothar says,

> From now on until the end of the lectures a ring is a commutative ring with 1 and a homomorphism $\varphi : R \to S$ of rings satisfies $\varphi(1) = 1$.

**Exercise 4.33.** Let $R$ be a commutative ring with 1. An element $r \in R$ is called *nilpotent* if there exists an $n \in \mathbb{Z}_{>0}$ with $r^n = 0$. Let

$$N(R) := \{r \in R \mid r \text{ is nilpotent}\}. \tag{4.97}$$

(a) Determine $N(\mathbb{Z}/4\mathbb{Z})$.

(b) Show that $N(R)$ is an ideal in $R$.

(c) Show that $N(R) \subseteq P$ for every prime ideal $P \subseteq R$.

(d) Show that 0 is the only nilpotent element of $R/N(R)$.

*Solution.* (a) Nilpotents are zero-divisors, in particular. The only zero divisors in $\mathbb{Z}_4$ are $0, 2$. Both of them are nilpotents since $0^1 = 0, 2^2 = 0$. Therefore,

$$N(\mathbb{Z}_4) = \{0, 2\}. \tag{4.98}$$

(b) Since $N(R) = \sqrt{(0)}$, it's clearly an ideal, by Exercise 4.29.

(c) Let $\mathfrak{p}$ be a prime ideal, and let $x \in N(R)$ with $x^n = 0$. Then $x^n = 0 \in \mathfrak{p}$. Let

$$m = \min\left\{i > 0 \mid x^i \in \mathfrak{p}\right\}. \tag{4.99}$$

If $m = 1$, we are done! So assume $m \neq 1$. Then

$$x^m = x \cdot x^{m-1} \in \mathfrak{p}, \tag{4.100}$$

then either $x \in \mathfrak{p}$ or $x^{m-1} \in \mathfrak{p}$. We already assumed $m \neq 1$, so $x \notin \mathfrak{p}$. Therefore, $x^{m-1} \in \mathfrak{p}$, which contradicts the minimality of $\mathfrak{p}$. Hence, $x \in \mathfrak{p}$, i.e. $N(R) \subseteq \mathfrak{p}$.

(d) Let $r + N(R) \in R/N(R)$ be a nilpotent element. Then

$$0 + N(R) = (r + N(R))^n = r^n + N(R) \text{ for some } n > 0. \tag{4.101}$$

This means $r^n \in N(R)$ is a nilpotent, i.e. for some $m > 0$, we have

$$0 = (r^n)^m = r^{mn}. \tag{4.102}$$

So $r$ is a nilpotent, i.e. $r + N(R) = 0 + N(R)$. Hence, 0 is the only nilpotent in $R/N(R)$.

■

**Exercise 4.34.** Let $k$ be a field and $f \in k[x]$. Let $R := k[x]/\langle f \rangle$. Show that $N(R) = 0$ (see previous exercise) if and only if $f$ is not divisible by the square of a polynomial (aka, square-free).

*Solution.* Since $k$ is a field, any polynomial $f \in k[x]$ can be written as a product of powers of irreducibles:

$$f = p_1^{e_1} \cdots p_k^{e_k}, \tag{4.103}$$

where $p_i$'s are irreducibles.

Suppose $f$ is square-free. Then $e_i = 1$ for each $i$. If $g + (f) \in N\left(\frac{k[x]}{(f)}\right)$, then for some $n > 0$, $g^n \in (f)$. Then

$$f = p_1 \cdots p_k \mid g^n. \tag{4.104}$$

Therefore, each $p_i \mid g^n$. But since $p_i$'s are irreducibles (and thus primes, since $k[x]$ is a UFD), $p_i \mid g^n$ if and only if $p_i \mid g$. Therefore, $f \mid g$, i.e.

$$g + (f) = 0 + (f), \quad \text{i.e. } N\left(\frac{k[x]}{(f)}\right) = 0. \tag{4.105}$$

Conversely, suppose $N\left(\frac{k[x]}{(f)}\right) = 0$. Write $f = p_1^{e_1} \cdots p_k^{e_k}$ as a product of irreducibles. Assume for the sake of contradiction that at least one of the $e_i$'s is greater than 1.

Take $g = p_1 \cdots p_k$. Then $g + (f) \neq 0 + (f)$ since $f \nmid g$. Now, let $n = \max\{e_1, \ldots, e_k\} \geq 2$. Then

$$g^n = p_1^n \cdots p_k^n, \tag{4.106}$$

which is divisible by $p_1^{e_1} \cdots p_k^{e_k}$, i.e.

$$[g + (f)]^n = 0 + (f), \tag{4.107}$$

proving that $g + (f) \in N(\frac{k[x]}{(f)})$. But we started with $N\left(\frac{k[x]}{(f)}\right) = 0$. Contradiction! Hence, $f$ must be square-free. ■

**Exercise 4.35.** Determine the maximal ideals of $\mathbb{R}[x] / \left(x^2\right)$ and $\mathbb{R}[x] / \left(x^2 + x + 1\right)$.

*Solution.* We'll use Exercise 4.37. An ideal $\mathfrak{m}$ of $\mathbb{R}[x]/(f(x))$ is maximal if and only if $\pi^{-1}(\mathfrak{m})$ (that contains $f(x)$) is maximal in $\mathbb{R}[x]$. A maximal ideal is prime, so it contains all the nilpotents (Exercise 4.33). Therefore,

$$\left[x + \left(x^2\right)\right]^2 = x^2 + \left(x^2\right) = 0 + \left(x^2\right), \tag{4.108}$$

so $\overline{x} = x + \left(x^2\right)$ is a nilpotent in $\mathbb{R}[x]/\left(x^2\right)$. So $\overline{x} \in \mathfrak{m}$, i.e. $\pi^{-1}(\mathfrak{m})$ contains $x$ and $x^2$. We claim $\pi^{-1}(\mathfrak{m}) = (x)$, because if a nonzero real number $c \in \pi^{-1}(\mathfrak{m})$, then it's the whole $\mathbb{R}[x]$. Therefore, $\pi^{-1}(\mathfrak{m}) = (x)$. So the only maximal ideal of $\mathbb{R}[x]/(x^2)$ is $(\overline{x})$.

We claim that $\mathbb{R}[x] / \left(x^2 + x + 1\right)$ is a field. For $ax + b \in \left(x^2 + x + 1\right)$,

$$(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd = ac(-x - 1) + (ad + bc)x + bd \tag{4.109}$$

$$= (ad + bc - ac)x + (bd - ac). \tag{4.110}$$

(The equality is $\mathbb{R}[x] / \left(x^2 + x + 1\right)$.) Then we can solve for $c, d$ to make this quantity 1:

$$c = \frac{a}{a^2 - ab + b^2}, \quad d = \frac{b - a}{a^2 - ab + b^2}. \tag{4.111}$$

(Of course $a^2 - ab + b^2 \neq 0$ for $a \neq 0$, $b \neq 0$.) Therefore,

$$\frac{a}{a^2 - ab + b^2}x + \frac{b - a}{a^2 - ab + b^2} = (ax + b)^{-1}. \tag{4.112}$$

So $\mathbb{R}[x] / \left(x^2 + x + 1\right)$ is a field, and hence its unique maximal ideal is (0). ■

**Exercise 4.36.** Prove that the ideal $I = \left\langle x + y^2, y + x^2 + 2xy^2 + y^4 \right\rangle$ in $\mathbb{C}[x, y]$ is a maximal ideal.

*Solution.* We claim that $I = (x, y)$. Indeed, $x + y^2 \in (x, y)$, and $y + x^2 + 2xy^2 + y^4 \in (x, y)$. Therefore, $I \subseteq (x, y)$.

Now,

$$y + x^2 + 2xy^2 + y^4 = y + \left(x + y^2 - y^2\right)^2 + 2\left(x + y^2 - y^2\right) y^2 + y^4 \tag{4.113}$$

$$= y + \left(x + y^2\right) P - y^4 + (x + y^2)Q - 2y^4 + y^4 \tag{4.114}$$

$$= y + \left(x + y^2\right) P + (x + y^2)Q \tag{4.115}$$

for some $P, Q \in \mathbb{C}[x, y]$. Therefore, $y \in I$. Since $y \in I$, $y^2 \in I$, and hence from $x + y^2 \in I$ we have $x \in I$. As a result, $(x, y) \in I$.

So we have proved $I = (x, y)$. This is a maximal ideal because

$$R/I = \frac{\mathbb{C}\,[x, y]}{(x, y)} \cong \mathbb{C}, \tag{4.116}$$

is a field, so $I$ is a maximal ideal. ■

**Exercise 4.37.** Let $R$ be a ring, and let $I$ be an ideal of $R$. Let $\overline{R} := R/I$. For an ideal $M \subseteq R$ containing $I$ let $\overline{M} = M/I$. Show that $\overline{M}$ is maximal in $\overline{R}$ if and only if $M$ is maximal in $R$.

*Solution.* Preimage of ideals under a homomorphism is an ideal, and image of ideals under a surjective homomorphism is an ideal. Therefore, if $\overline{M}$ is maximal and $M$ is not, there exists an ideal

$$M \subsetneq L \subsetneq R. \tag{4.117}$$

Taking the image under $\pi$, we have

$$M/I \subsetneq L/I \subsetneq R/I, \tag{4.118}$$

contradicting the maximality of $\overline{M} = M/I$. Similarly, if $M$ is maximal but $\overline{M}$ is not, then there exists an ideal

$$\overline{M} \subsetneq \overline{L} \subsetneq \overline{R}. \tag{4.119}$$

Taking the preimage under $\pi$, we get

$$M \subsetneq \pi^{-1}\left(\overline{L}\right) \subsetneq R, \tag{4.120}$$

contradicting the maximality of $M$. ■

**Exercise 4.38.** Give an example of a ring in which some prime ideal is not a maximal ideal.

*Solution.* Consider the ring $\mathbb{Z}[x]$. The ideal $(x)$ is prime, since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is an ID. But $(x)$ is not maximal since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is not a field. ■

**Exercise 4.39.** Let $R$ be a commutative ring with 1 and let $I$ be an ideal that is contained in a finite union $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$ of prime ideals of $R$. Show that $I \subseteq \mathfrak{p}_i$ for some $i$.

*Solution.* We shall prove it by induction on $n$. The base case $n = 1$ is clearly true. Suppose the statement is true for $n - 1$. For each $i$, if $I$ is contained in $\bigcup_{j \neq i} \mathfrak{p}_j$, then we're done by the inductive hypothesis. So suppose that's not the case, so we can pick $x_i \in I$ such that $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$. Then it has to be

$$x_i \in \mathfrak{p}_i. \tag{4.121}$$

Now, take the element

$$y = x_1 + x_2 x_3 \cdots x_n \in I. \tag{4.122}$$

It's in $I$ because each $x_i \in I$. Therefore, $y \in \mathfrak{p}_k$ for some $k$.

If $y \in \mathfrak{p}_1$, since $x_1 \in \mathfrak{p}_1$, $x_2 x_3 \cdots x_n \in \mathfrak{p}_1$. But since $\mathfrak{p}_1$ is prime, that would imply some $x_i \in \mathfrak{p}_1$. But by construction, $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$, so in particular, $x_i \notin \mathfrak{p}_1$.

If $y \in \mathfrak{p}_k$ for $k > 1$, then since $x_k \in \mathfrak{p}_k$, $x_2 x_3 \cdots x_n \in \mathfrak{p}_k$. So we have $x_1 \in \mathfrak{p}_k$. But by construction, $x_1 \notin \bigcup_{j \neq 1} \mathfrak{p}_j$, so in particular, $x_1 \notin \mathfrak{p}_k$.

Therefore, we arrive at a contradiction in all cases! ■

**Exercise 4.40.** Let $f : R \to S$ be a surjective ring homomorphism with kernel $K$. Show:

(a) If $P$ is a prime ideal of $R$ containing $K$, then $f(P)$ is a prime ideal of $S$.

(b) If $Q$ is a prime ideal of $S$, then $f^{-1}(Q)$ is a prime ideal of $R$ containing $K$.

*Solution.* (a) Since $f$ is a surjective homomorphism, $f(P)$ is an ideal of $S$.

If $f(P) = S$, that means there exists some $r \in P$ such that $f(r) = 1$. Then

$$1 - r \in \operatorname{Ker} f = K \subseteq P. \tag{4.123}$$

$1 - r \in P$ and $r \in P$ together gives us $1 \in P$, which means $P = R$, which is a contradiction since a prime ideal is never the whole ring. Therefore, $f(P) \neq S$.

Now, let $a, b \in S$ with $ab \in f(P)$. Since $f$ is surjective, $a = f(x)$ and $b = f(y)$ for some $x, y \in R$. Then

$$f(xy) = f(x) f(y) = ab \in f(P). \tag{4.124}$$

This means $xy \in P + K = P$. Therefore, $x \in P$ or $y \in P$. WLOG $x \in P$, so that $f(x) = a \in f(P)$, proving that $f(P)$ is a prime ideal.

(b) $f^{-1}(Q)$ is an ideal since $f$ is a homomorphism. It contains $K$ since $Q$ contains 0, so $f^{-1}(Q)$ contains $f^{-1}(0) = K$.

It's easy to see that $f^{-1}(Q) \neq R$. Since $Q$ is prime, it doesn't contain 1, so $f^{-1}(Q)$ doesn't contain 1 either, so $f^{-1}(Q) \neq R$.

Now, suppose $a, b \in R$ with $ab \in f^{-1}(Q)$. Then $f(ab) \in Q$. But $f(ab) = f(a)f(b)$. Since $Q$ is prime, $f(a) \in Q$ or $f(b) \in Q$. WLOG $f(a) \in Q$, so that $a \in f^{-1}(Q)$. Therefore, $Q$ is prime.

■

**Exercise 4.41.** Let $R$ be a ring with 1, $M$ an ideal in $R$. Suppose every element of $R \setminus M$ is a unit in $R$. Show that $M$ is the unique maximal ideal of $R$.

*Solution.* Let $M' \neq M$ be a maximal ideal. Then $M' \not\subseteq M$, so it contains some element not in $M$, say $u$. By hypothesis, $u$ is a unit. So

$$1 = u \cdot u^{-1} \in M'. \tag{4.125}$$

But that means for every $r \in R$,

$$r = r \cdot 1 \in M', \tag{4.126}$$

proving $M' = R$. ■

**Exercise 4.42.** Show: The ring $2\mathbb{Z}$ of even integers contains a maximal ideal $M$, such that $2\mathbb{Z}/M$ is not a field.

*Solution.* In $R = 2\mathbb{Z}$, $\mathfrak{m} = 4\mathbb{Z}$ is a maximal ideal. But $R/\mathfrak{m} = \left\{\overline{0}, \overline{2}\right\}$, which is not a field since it has no multiplicative identity. ■

**Exercise 4.43.** Find the greatest common divisors of the following polynomials in $\mathbb{Q}[x]$.

(a) $x^3 - 6x^2 + x + 4$ and $x^5 - 6x + 1$.

(b) $x^2 + 1$ and $x^6 + x^3 + x + 1$.

*Solution.* (a) Let's first factorize $f(x) := x^3 - 6x^2 + x + 4$. We can see that 1 is a root of this polynomial. In fact,

$$x^3 - 6x^2 + x + 4 = (x - 1)\left(x^2 - 5x - 4\right). \tag{4.127}$$

$x^2 - 5x - 4$ is irreducible since it has no rational root. Now, 1 is not a root of $g(x) := x^5 - 6x + 1$, so $x - 1$ doesn't divide $g$. Furthermore, $x^2 - 5x - 4$ also doesn't divide $g$, as can be checked easily.

Therefore, $\gcd(f, g) = 1$.

(b) Note that

$$x^6 + x^3 + x + 1 = \left(x^2 + 1\right)\left(x^4 - x^2 + x + 1\right), \tag{4.128}$$

so their gcd is $x^2 + 1$.

■

**Exercise 4.44.** Let $k$ be a field and let $a_0, \ldots, a_n \in k$ be distinct elements and let $b_0, \ldots, b_n \in k$. Show: There is at most one polynomial $f \in k[x]$ of degree $n$ with $f(a_i) = b_i$ for $i = 0, \ldots, n$.

*Solution.* Suppose there are at least two such polynomaials $f, f'$. Then $\deg(f - f') \leq n$. But

$$(f - f')(a_i) = f(a_i) - f'(a_i) = b_i - b_i = 0. \tag{4.129}$$

Therefore, $f - f'$ has $n + 1$ roots, while its degree is at most $n$. This can happen only if it's the zero polynomial, i.e. $f = f'$. ■

**Exercise 4.45.** Let $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ and let

$$f = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Q}[x] \tag{4.130}$$

(note that the leading coefficient is 1). Let $b \in \mathbb{Q}$ be a zero of $f$. Show that $b \in \mathbb{Z}$.

*Solution.* Suppose $b = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ and $q \neq 0$, and $\gcd(p, q) = 1$. Then $f(b) = 0$, so we have

$$\sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = 0, \tag{4.131}$$

where $a_n = 1$. Multiplying by $q^n$, we have

$$\sum_{i=0}^{n} a_i p^i q^{n-i} = 0. \tag{4.132}$$

Except for the $i = n$ term, all the terms are divisible by $q$, and the RHS is obviously divisible by $q$. Hence,

$$q \mid a_n p^n = p^n. \tag{4.133}$$

Therefore, $q = 1$, since $p$ and $q$ has no common factor other than 1. So $b = p \in \mathbb{Z}$. ■

**Exercise 4.46.** Let $f, g \in k[x]$ be polynomials with coefficients in a field $k$. Assume the both $f$ and $g$ factor into linear factors i.e. $f = (x + a_1) \cdot \cdots \cdot (x + a_n)$, $g = (x + b_1) \cdot \cdots \cdot (x + b_m)$. Then the greatest common divisor is the product of the common linear factors.

*Solution.* It's clear that the product of the common linear factors is a common divisor of $f$ and $g$. Another common divisor would be the product of a subcollection of these common linear factors, so that clearly divides the product of all common linear factors. ■

**Exercise 4.47.** Prove or disprove the following statement: The ring $\mathbb{Z}[x]$ is a principal ideal domain.

*Solution.* This is false. Because the ideal $(2, x) \trianglelefteq \mathbb{Z}[x]$ is not a principal ideal. If it were, $(2, x) = (f)$, then $f$ must divide 2. But that would mean $f$ is a constant polynomial $\pm 1$ or $\pm 2$. In the first case, $(f) = \mathbb{Z}[x]$, and in the second case, $2 \mid x$, which is not possible. ■

**Exercise 4.48.** If $a + bi \in \mathbb{Z}[i]$ is not a unit, show that $a^2 + b^2 > 1$.

*Solution.* If $a^2 + b^2 = 0$, that would just imply $a = b = 0$, which is 0. If $a^2 + b^2 = 1$,

$$1 = a^2 + b^2 = (a + ib)(a - ib), \tag{4.134}$$

proving $a + ib$ is a unit. Therefore, ■

**Exercise 4.49.** Show that $\mathbb{Z}\left[\sqrt{2}\right]$ is an Euclidean domain.

*Solution.* Let $N\left(a + b\sqrt{2}\right) = \left|a^2 - 2b^2\right|$ be the norm function. We claim that $\mathbb{Z}[\sqrt{2}]$ of $\mathbb{R}$ is an ED under this function. $N$ is multiplicative, so $N(xy) = N(x)N(y) \geq N(x)$ for $x, y \neq 0$. So now we need to verify the second property of Euclidean function.

Let $\alpha = a + b\sqrt{2}$, and $\beta = c + d\sqrt{2}$. Then $\alpha/\beta \in \mathbb{Q}[\sqrt{2}]$ is given by

$$\frac{\alpha}{\beta} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} = q_1 + q_2\sqrt{2}. \tag{4.135}$$

Let $m$ and $n$ be the integers closest to $q_1$ and $q_2$, respectively. Therefore, we have $|m - q_1| \leq \frac{1}{2}$ and $|n - q_2| \leq \frac{1}{2}$.

We take $\gamma = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and

$$\delta = \beta\left((q_1 - m) + \sqrt{2}(q_2 - n)\right) = \beta\left(\frac{\alpha}{\beta} - \gamma\right) = \alpha - \gamma\beta \in \mathbb{Z}[\sqrt{2}]$$

Then we have $\alpha = \beta\gamma + \delta$. Now we need to show that if $N(\delta)$ is nonzero, then $N(\delta) < N(\beta)$.

$N$ is multiplicative not only in $\mathbb{Z}[\sqrt{2}]$, but also in $\mathbb{Q}[\sqrt{2}]$.

$$N(\delta) = N(\beta)N\left((q_1 - m) + \sqrt{2}(q_2 - n)\right) = N(\beta)\left|(q_1 - m)^2 - 2(q_2 - n)^2\right| \tag{4.136}$$

$$\leq N(\beta)\left(|q_1 - m|^2 + 2|q_2 - n|^2\right) \leq N(\beta)\left(\frac{1}{4} + 2 \times \frac{1}{4}\right) \tag{4.137}$$

$$\leq \frac{3}{4}N(\beta) < N(\beta) \tag{4.138}$$

Therefore, $N$ is an euclidean function, and that's why $\mathbb{Z}[\sqrt{2}]$ is an ED. ■

**Exercise 4.50.** Give an example that division with rest need not be unique in a Euclidean domain.

*Solution.* $\mathbb{Z}$ is an ED with the norm function $N(a) = |a|$. Then division with rest (remainder) is not unique in $\mathbb{Z}$. For instance, if we divide 7 by 3,

$$7 = 3 \cdot 2 + 1, \tag{4.139}$$

here the remainder is 1, and $N(1) = 1 < 3 = N(3)$. But also,

$$7 = 3 \cdot 3 + (-2), \tag{4.140}$$

here the remainder is $-2$, and $N(-2) = 2 < 3 = N(3)$. So division with remainder is not unique. ■

**Exercise 4.51.** Let $m, n \in \mathbb{Z}$. Show that their greatest common divisor in $\mathbb{Z}$ is the same as their greatest common divisor in $\mathbb{Z}[i]$.

*Solution.* Let $d = \gcd_{\mathbb{Z}}(m, n)$ and $d' = \gcd_{\mathbb{Z}[i]}(m, n)$ (which is not unique, it's unique up to multiplication by a unit, which are $\pm 1, \pm i$ in $\mathbb{Z}[i]$).

Since $\mathbb{Z} \subseteq \mathbb{Z}[i]$, $d$ is a common divisor of $m$ and $n$ in $\mathbb{Z}[i]$. Therefore, $d \mid d'$ in $\mathbb{Z}[i]$.

Since $d = \gcd_{\mathbb{Z}}(m, n)$, by Bezout's identity, there exists integers $x, y$ such that

$$d = mx + ny. \tag{4.141}$$

Since $d' \mid m$ and $d' \mid n$ (in $\mathbb{Z}[i]$), we have that $d' \mid mx + ny = d$ (in $\mathbb{Z}[i]$). In general, any common divisor of $m$ and $n$ in $\mathbb{Z}[i]$ also divides $d$. Therefore, $d = d'$ up to multiplication by a unit. ■

**Exercise 4.52.** Prove that

(a) $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

(b) $x^2 + 1$ is irreducible in $\mathbb{F}_7[x]$.

*Solution.* (a) If it wasn't irreducible, then it would split into degree-1 terms, i.e. it would have roots. But $f(0) = f(1) = 1 \neq 0$, so $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

(b) If it wasn't irreducible, then it would split into degree-1 terms, i.e. it would have roots. But since 7 is a prime of the form $4k - 1$, there doesn't exist any $x$ with $x^2 + 1 = 0$.

■

**Exercise 4.53.** Let $R$ be a commutative ring with no nonzero nilpotent elements (i.e. $a^n = 0$ implies $a = 0$). If $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ is a zero divisor, show that there is an element $b \neq 0$ in $R$ with $ba_0 = ba_1 = \cdots = ba_n = 0$.

*Solution.* In fact, we don't need the condition that $R$ has no nonzero nilpotent. Since $f$ is a zero divisor, let $g \neq 0$ be a polynomial of **minimal degree** such that $fg = 0$. We'll show that $\deg g = 0$.

$$f = \sum_{i=0}^{n} a_i x^i, \quad g = \sum_{i=0}^{m} b_i x^i. \tag{4.142}$$

Then

$$fg = \sum_{k=0}^{m+n} \left( \sum_{i+j=k} a_i b_j \right) x^k = 0. \tag{4.143}$$

Looking at the coefficient of $x^{m+n}$, we see that $a_n b_m = 0$. Therefore, $\deg(a_n g) < m$. But

$$f \cdot (a_n g) = a_n \cdot (fg) = 0, \tag{4.144}$$

and $a_n g$ is a polynomial of degree less than $\deg g$ with $f \cdot (a_n g) = 0$. This contradicts the minimality of $\deg g$. Hence, $a_n g = 0$.

We'll prove that $a_{n-l} g = 0$ for every $0 \leq l \leq n$. We'll prove it by induction on $l$. The base case $l = 0$ has already been done. Now suppose

$$a_n g = a_{n-1} g = \cdots = a_{n-l+1} g = 0. \tag{4.145}$$

As a result,

$$a_n b_j = a_{n-1} b_j = \cdots = a_{n-l+1} b_j = 0, \tag{4.146}$$

for every $0 \leq j \leq m$. Let's look at the coefficient of $x^{m+n-l}$ in (4.143).

$$a_n b_{m-l} + a_{n-1} b_{m-l+1} + a_{n-2} b_{m-l+2} + \cdots + a_{n-l} b_m = 0. \tag{4.147}$$

By (4.146), all the terms of (4.147) except the last one is 0. Therefore, the last one $a_{n-l} b_m$ also has to be 0. Therefore, $\deg(a_{n-l} g) < m$. But

$$f \cdot (a_{n-l} g) = a_{n-l} \cdot (fg) = 0, \tag{4.148}$$

and by the minimality of $\deg g$, we must have that $a_{n-l} g = 0$. Therefore, by induction, $a_i g = 0$ for each $i = 0, 1, \ldots, n$. As a result, $a_i b_j = 0$ for each $0 \leq i \leq n, 0 \leq j \leq m$.

Since $g \neq 0$, it has a nonzero coefficient, and we can take that to be $b$, and we'll have $b a_i = 0$ for each $0 \leq i \leq n$. ■

**Exercise 4.54.** Let $k$ be a field. Show that $k[x_1, x_2]$ is not a principal ideal domain.

*Solution.* The ideal $(x_1, x_2)$ is not a principal ideal. If if were, $(x_1, x_2) = (f)$ for some $f \in k[x_1, x_2]$. Then $f \mid x_1$, and $f \mid x_2$ forces $f \in k$. But that would mean $(f) = (0)$ or $(f) = k$. So $(x_1, x_2) \neq (f)$. ■

**Exercise 4.55.** Prove $1 + x + x^3 + x^4$ is irreducible in $k[x]$ for any field $k$.

*Solution.*

$$1+x+x^3+x^4=(1+x)+x^3(1+x)=(1+x)\left(1+x^3\right), \tag{4.149}$$

is not irreducible in any field $k$. ■

**Exercise 4.56.** Prove $x^4+2x+2$ is irreducible in $\mathbb{Q}[x]$.

*Solution.* We'll apply Eisenstein's criterion. $2 \mid a_0, a_1, a_2, a_3$, $2 \nmid a_4$, $2^2 \nmid a_0$. So by Eisenstein's criterion, $x^4+2x+2$ is irreducible in $\mathbb{Q}[x]$. ■

**Exercise 4.57.** Let $p$ be a prime number, $c \in \mathbb{Q}$. Show $x^p-c$ is irreducible over $\mathbb{Q}$ if and only if it has no zero in $\mathbb{Q}$.

*Solution.* If it's irreducible over $\mathbb{Q}$, it doesn't have any root in $\mathbb{Q}$. Now, conversely, suppose $f(x)=x^p-c$ has no root in $\mathbb{Q}$. Assume for the sake of contradiction that $x^p-c$ is reducible, i.e $x^p-c=fg$ for some $f,g \in \mathbb{Q}[x]$ with $\deg f, \deg g \geq 1$. We assume both $f$ and $g$ are monic, since otherwise their leading terms would be $a$ and $a^{-1}$, and we can make the leading terms 1 multiplying by $a^{-1}$ and $a$, respectively.

Now, suppose $\deg f = n \geq 1$. It splits into linear factors in $\mathbb{C}$, say

$$f(x)=\prod_{i=1}^{n}(x-r_i). \tag{4.150}$$

Consider the number

$$r=\prod_{i=1}^{n} r_i. \tag{4.151}$$

It's a product of complex numbers, but it's $\pm$ the constant term of $f$. So $r \in \mathbb{Q}$. Also,

$$r^p=\prod_{i=1}^{n} r_i^p=\prod_{i=1}^{n} c=c^n. \tag{4.152}$$

Since $n<p$, $\gcd(n,p)=1$. So we can find $a,b \in \mathbb{Z}$ with $ap+bn=1$. Then

$$\left(c^a r^b\right)^p=c^{ap}\left(r^p\right)^b=c^{ap}\left(c^n\right)^b=c^{ap+bn}=c. \tag{4.153}$$

This $c^a r^b$ is a rational number, which is a root of $x^p-c$. Therefore, assuming $x^p-c$ is reducible, we got that a root must exist in $\mathbb{Q}$. Hence, if no roots exist in $\mathbb{Q}$, $x^p-c$ must be irreducible. ■

**Exercise 4.58.** Let $k$ be a field, $a,b \in k$. Show that $f \in k[x]$ is irreducible if and only if $f(ax+b)$ is irreducible.

*Solution.* Here, we need the condition that $a \neq 0$. For $a \neq 0$, $x \mapsto ax+b$ is an automorphism of $k[x]$ (Exercise 4.26). We'll show that automorphism preserves irreducible elements. Indeed, if

$f = gh$ is reducible, where $g$ and $h$ are not units, then under an automorphism $\Psi$,

$$\Psi(f) = \Psi(g)\,\Psi(h), \tag{4.154}$$

and $\Psi(g)$ and $\Psi(h)$ are not units, because if they were, then their inverse images would also be units, since $\Psi$ is an automorphism. Therefore, $\Psi(f)$ is also reducible.

Similarly, one can show that $\Psi(f)$ reducible implies $f$ reducible, by taking $\Psi^{-1}$ in the previous argument. Therefore, $f$ irreducible if and only if $\Psi(f)$ irreducible. ■

**Exercise 4.59.** Prove that the kernel of the homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{R};\ x \mapsto 1 + \sqrt{2}$ is a principal ideal and find a generator for this ideal.

*Solution.* For notational simplicity, let's write $\alpha := 1 + \sqrt{2}$. Then $\alpha - 1 = \sqrt{2}$, so that

$$(\alpha - 1)^2 - 2 = 0. \tag{4.155}$$

So $f(\alpha) = 0$ for $f(x) = x^2 - 2x - 1 \in \mathbb{Z}[x]$. Furthermore, this is the minimal polynomial for $\alpha$, since there's no degree-1 polynomial whose root is $\alpha$. We claim that $\operatorname{Ker}\varphi = (f)$.

Since $\varphi$ sends $x$ to $\alpha$, it sends a general $g(x) \in \mathbb{Z}[x]$ to $g(\alpha)$. Therefore, if $g \in (f)$, then $g = fh$ for some $h \in \mathbb{Z}[x]$. Then

$$\varphi(g) = g(\alpha) = f(\alpha)\,h(\alpha) = 0, \tag{4.156}$$

so $g \in \operatorname{Ker}\varphi$. Therefore, $(f) \subseteq \operatorname{Ker}\varphi$. Now, for $g \in \operatorname{Ker}\varphi$, we perform an Euclidean division on $g$ by $f$:

$$g = fq + r, \tag{4.157}$$

where $r = 0$ or $\deg r < \deg f = 2$. $fq \in \operatorname{Ker}\varphi$ (as shown above), so that $r \in \operatorname{Ker}\varphi$. But if $r \neq 0$, then $\deg r = 0, 1$, in which case $r(\alpha)$ can't be 0. Hence, $r = 0$, so $g = fq \in (f)$.

Therefore, $\operatorname{Ker}\varphi = (f) = \left(x^2 - 2x - 1\right)$. ■

**Exercise 4.60.** Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$.

(a) $x^2 + 27x + 213$.

(b) $x^3 + 6x + 12$.

(c) $x^5 - 3x^4 + 3$.

*Solution.* (a) We'll apply Eisenstein's criterion. $3 \mid a_0, a_1$, $3 \nmid a_2$, $3^2 \nmid a_0$. So by Eisenstein's criterion, $x^2 + 27x + 213$ is irreducible in $\mathbb{Q}[x]$.

(b) $3 \mid a_0, a_1, a_2$, $3 \nmid a_3$, $3^2 \nmid a_0$. So by Eisenstein's criterion, $x^3 + 6x + 12$ is irreducible in $\mathbb{Q}[x]$.

(Choosing $p = 2$ wouldn't have worked here since $2^2 \mid 12$.)

(c) $3 \mid a_0, a_1, a_2, a_3, a_4$, $3 \nmid a_5$, $3^2 \nmid a_0$. So by Eisenstein's criterion, $x^5 - 3x^4 + 3$ is irreducible in $\mathbb{Q}[x]$.

■

**Exercise 4.61.** Factor $x^5 + 5x + 5$ into irreducible factors in $\mathbb{Q}[x]$ and $\mathbb{F}_2[x]$.

*Solution.* For $\mathbb{Q}$, we'll apply Eisenstein's criterion. $5 \mid a_0, a_1, a_2, a_3, a_4$, $5 \nmid a_5$, $5^2 \nmid a_0$. So by Eisenstein's criterion, $x^5 + 5x + 5$ is irreducible in $\mathbb{Q}[x]$.

In $\mathbb{F}_2[x]$,

$$f(x) = x^5 + 5x + 5 = x^5 + x + 1. \tag{4.158}$$

$f(0) = f(1) = 1$, so $f$ doesn't have any linear factors. Let's check if it has any quadratic factors. The only irreducible quadratic in $\mathbb{F}_2[x]$ is $x^2 + x + 1$. After a polynomial long division, we find that $x^2 + x + 1$ divides $f$:

$$x^5 + x + 1 = \left(x^2 + x + 1\right)\left(x^3 + x^2 + 1\right). \tag{4.159}$$

$x^3 + x^2 + 1$ is irreducible because it has no roots in $\mathbb{F}_2$. ■

**Exercise 4.62.** Suppose that a polynomial $x^4 + bx^2 + c \in \mathbb{Q}[x]$ is the product of two factors of degree 2 in $\mathbb{Q}[x]$. What can one say about the coefficients of these factors?

*Solution.* Suppose

$$x^4 + bx^2 + c = \left(x^2 + px + q\right)\left(x^2 + rx + s\right) = x^4 + (p+r)x^3 + (q + s + pr)x^2 + (ps + rq)x + qs. \tag{4.160}$$

Since the coefficients of $x^3$ is 0, we have $r = -p$. Substituting this, we get

$$q + s - p^2 = b \tag{4.161}$$

$$p(s - q) = 0 \tag{4.162}$$

$$qs = c \tag{4.163}$$

Now we have two cases:

- if $p = 0$, then
$$x^4 + bx^2 + c = \left(x^2 + q\right)\left(x^2 + s\right) \tag{4.164}$$
with $q + s = b$ and $qs = c$.
- if $p \neq 0$, then we must have $s - q = 0$. Then,
$$x^4 + bx^2 + c = \left(x^2 + px + q\right)\left(x^2 - px + q\right), \tag{4.165}$$
where $q^2 = c$, $2q - p^2 = b$.

■

**Exercise 4.63.** Factor the following polynomials in $\mathbb{Q}[x]$

(a) $x^3 + 2x^2 + 3x + 1$.

(b) $x^4 + 2x^3 + 3x^2 + 2x + 1$.

*Solution.* (i) Reduction modulo 2 gives rise to the polynomial $x^3 + x + 1$. If this were reducible, it would have a linear factor, i.e. it would have a root. Plugging $0, 1$ in $x^3 + x + 1$, we get $1 \neq 0$ both times. So $x^3 + x + 1$ has no roots in $\mathbb{F}_2$. Therefore, it's irreducible in $\mathbb{F}_2[x]$, and as a result, it's irreducible in $\mathbb{Q}[x]$.

(ii) Reduction modulo 2 gives $x^4 + x^2 + 1$, which is (Fresher's dream[1])

$$x^4 + x^2 + 1 = \left(x^2 + x + 1\right)^2. \tag{4.166}$$

In $\mathbb{Q}[x]$, one can check that

$$\left(x^2 + x + 1\right)^2 = x^4 + x^2 + 1 + 2x^3 + 2x^2 + 2x = x^4 + 2x^3 + 3x^2 + 2x + 1. \tag{4.167}$$

$x^2 + x + 1$ can't be factored further since it's irreducible.

■

**Exercise 4.64.** Let $p \in \mathbb{Z}$ be a prime number. Let $f = \sum_{i=0}^{2n+1} a_i x^i \in \mathbb{Z}[x]$ be a polynomial of odd degree. Suppose $p \nmid a_{2n+1}$, $p^2 \mid a_0, \ldots, a_n$, $p \mid a_{n+1}, \ldots, a_{2n}$ and $p^3 \nmid a_0$. Show that $f$ is irreducible in $\mathbb{Q}[x]$.

*Solution.* By Gauss' lemma, $f$ is irreducible in $\mathbb{Q}[x]$ if and only if it's irreducible in $\mathbb{Z}[x]$. Assume for the sake of contradiction that $f$ is reducible in $\mathbb{Z}[x]$. Then $f = gh$ for $g, h \in \mathbb{Z}[x]$. Reducing to mod $p$, we obtain

$$gh \equiv a_{2n+1} x^{2n+1}. \tag{4.168}$$

Therefore, other than the leading terms of $g$ and $h$, the rest of those polynomaials are divisible by $p$.

$$g = Ax^{m_1} + pg', \quad h = Bx^{m_2} + ph', \tag{4.169}$$

where $p \nmid A, B$ since $p \nmid AB = a_{2n+1}$. Then

$$f = gh = AB\ x^{m_1+m_2} + Ap\ x^{m_1} h' + Bp\ x^{m_2} g' + p^2\ g'h'. \tag{4.170}$$

WLOG, $m_1 \leq m_2$, then $m_1 \leq n$. Now, the coefficient of $x^{m_1}$ modulo $p^2$ is

$$a_{m_1} \equiv Ap\ h'(0) \pmod{p^2}. \tag{4.171}$$

[1] Although the term is Freshman's dream, my obsession with using gender-neutral language knows no bounds.

Since $m_1 \leq n$, $a_{m_1} \equiv 0 \pmod{p^2}$. Since $p \nmid A$, then we must have $p \mid h'(0)$. But then the constant term of $f$ would be

$$a_0 = p^2 \; g'(0) \; h'(0), \tag{4.172}$$

divisible by $p^3$, which is a contradiction! ■

# §5 Problem Set 3

All rings in this problem sheet are commutative with 1. Morphisms of rings send 1 to 1.

**Exercise 5.1.** Let $R$ be the ring $\mathbb{Z} \times \mathbb{Z}$.

(a) Show that every ideal of $R$ is principal.

(b) Describe all prime and maximal ideals of $R$.

*Solution.* First, let's show that any ideal in a product ring $R \times S$ is of the form $I \times J$ for $I \trianglelefteq R$ and $J \trianglelefteq S$. Let $\pi_1 : R \times S \to R$ and $\pi_2 : R \times S \to S$ be projections, which are surjective homomorphisms. If $\mathfrak{a} \trianglelefteq R \times S$, then $\pi_i(\mathfrak{a})$ are also ideals, since $\pi_i$ are surjective homomorphisms. Let

$$I = \pi_1(\mathfrak{a}) \trianglelefteq R, \quad J = \pi_2(\mathfrak{a}) \trianglelefteq S. \tag{5.1}$$

Then $\mathfrak{a} \subseteq I \times J$. Now, given any $(r, s) \in I \times J$, there exists some $s' \in S$ such that $(r, s') \in \mathfrak{a}$, and there exists some $r' \in R$ such that $(r', s) \in \mathfrak{a}$. We have

$$\left(r, ss'\right) = (1, s)\left(r, s'\right) \in \mathfrak{a}, \text{ and } \left(r', ss'\right) = \left(1, s'\right)\left(r', s\right) \in \mathfrak{a}. \tag{5.2}$$

Therefore, their difference, $(r - r', 0) \in \mathfrak{a}$. As a result,

$$\left(r - r', 0\right) + \left(r', s\right) = (r, s) \in \mathfrak{a}. \tag{5.3}$$

Hence, $\mathfrak{a} = I \times J$.

(a) Now, any ideal of $\mathbb{Z} \times \mathbb{Z}$ is of the form $I \times J$ for $I, J \trianglelefteq \mathbb{Z}$. And since $\mathbb{Z}$ is a PID, we have $I = (m)$ and $J = (n)$ for some $m, n \in \mathbb{Z}$. We claim that $I \times J = \langle (m, n) \rangle$.

$(m, n) \in I \times J$, so $\langle (m, n) \rangle \subseteq I \times J$. And any element of $I \times J$ is of the form $(am, bn)$, for some $a, b \in \mathbb{Z}$. Then

$$(am, bn) = (a, b) \cdot (m, n) \in \langle (m, n) \rangle. \tag{5.4}$$

Therefore, $I \times J = \langle m \rangle \times \langle n \rangle = \langle (m, n) \rangle$.

(b) Let $I \times J$ be an ideal of $\mathbb{Z} \times \mathbb{Z}$. Then

$$\frac{\mathbb{Z} \times \mathbb{Z}}{I \times J} \cong \frac{\mathbb{Z}}{I} \times \frac{\mathbb{Z}}{J}. \tag{5.5}$$

The products of two rings is an integral domain if and only if one the products is 0 and the other is an ID. Because otherwise, if both are nonzero, then

$$(1, 0) \cdot (0, 1) = (0, 0) \tag{5.6}$$

would lead to nonzero zero-divisors. Therefore, in order for $\frac{\mathbb{Z}}{I} \times \frac{\mathbb{Z}}{J}$ to be an ID, we must have that one of these is 0, WLOG, $\frac{\mathbb{Z}}{J} = 0$, i.e. $J = \mathbb{Z}$.

Then $\frac{\mathbb{Z}}{I}$ is an ID if and only if $I = (0)$ or $I = (p)$ for prime $p$. And $\frac{\mathbb{Z}}{I}$ is a field if and only if $I = (p)$ for prime $p$. Therefore, the prime ideals of $\mathbb{Z} \times \mathbb{Z}$ are

$$(0) \times \mathbb{Z},\ (p) \times \mathbb{Z},\ \mathbb{Z} \times (0),\ \mathbb{Z} \times (p); \tag{5.7}$$

and the maximal ideals are

$$(p) \times \mathbb{Z},\ \mathbb{Z} \times (p). \tag{5.8}$$

■

**Exercise 5.2.** Let $R$ be a ring. Define

$$J(R) = \bigcap_{\mathfrak{m} \trianglelefteq R \text{ maximal ideal}} \mathfrak{m}. \tag{5.9}$$

This ideal is called **Jacobson radical**.

(a) Show that $x \in J(R)$ if and only if $1 + xy$ is invertible for every $y \in R$.

(b) Let $\varphi : R \to S$ be a surjective homomorphism of rings. Show that $\varphi(J(R)) \subseteq J(S)$.

*Solution.* (a) Suppose $x \in J(R)$ and Assume for the sake of contradiction that there exists some $y \in R$ such that $1 + xy$ is not invertible. Then $1 + xy$ is contained in a maximal ideal $\mathfrak{m}$ (since the proper ideal $(1 + xy)$ is contained in a maximal ideal, assuming axiom of choice). $x \in J(R)$ implies $x \in \mathfrak{m}$, so we have $xy \in \mathfrak{m}$ since it's an ideal. But that gives us

$$1 = (1 + xy) - xy \in \mathfrak{m}, \tag{5.10}$$

which is not possible since maximal ideals are proper ideals.

Conversely, suppose $1 + xy$ is invertible for every $y \in R$, and assume for the sake of contradiction that $x \notin J(R)$. Then there exists a maximal ideal $\mathfrak{m}$ that doesn't contain $x$. Now,

$$(x) + \mathfrak{m} \supsetneq \mathfrak{m}, \tag{5.11}$$

so by the maximality of $\mathfrak{m}$, it has to be the whole $R$. Therefore, there exists $y \in R$ and $m \in \mathfrak{m}$ such that

$$xy + m = 1. \tag{5.12}$$

That would give us $m = 1 - xy$, which is invertible by hypothesis. But that can't happen, since maximal ideals can't contain invertible elements.

(b) Let $y \in \varphi(J(R))$. Then $y = \varphi(x)$ for some $x \in J(R)$. We'll show that $1 + sy$ is invertible for any $s \in S$, which will prove that $y \in J(S)$.

Given $s \in S$, since $\varphi$ is surjective, there exists $r \in R$ such that $s = \varphi(r)$. Let $u = (1 + rx)^{-1}$. Then

$$f(u)[1 + sy] = f(u) f(1 + rx) = f(u(1 + rx)) = f(1) = 1. \tag{5.13}$$

Hence, $1 + sy$ is invertible, and thus $y \in J(R)$. This proves that $\varphi(J(R)) \subseteq J(S)$.

■

**Exercise 5.3.** Let $R$ be the ring $\underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ times}} =: \mathbb{Z}^n$.

(a) Show that $R$ has a finite number of ring automorphisms.

(b) Find the number of automorphisms.

*Solution.* Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ where we have 1 at the $i$-th component and 0 everywhere else. Note that $e_i^2 = e_i$, so $e_i$ is an idempotent. An automorphism $\mathbb{Z}^n \to \mathbb{Z}^n$ will map idempotents to idempotents. The only idempotents of $\mathbb{Z}^n$ are vectors consisting of 0 and 1 only. Therefore,

$$f(e_i) = \left(c_1^{(i)}, \ldots, c_n^{(i)}\right), \tag{5.14}$$

where $c_j^{(i)}$'s are either 0 or 1.

Furthermore, if $i \neq j$, then $e_i \cdot e_j = 0$. So $f(e_i) \cdot f(e_j) = 0$. Therefore, for $i \neq j$, $f(e_i)$ and $f(e_j)$ can't contain 1 in the same coordinates.

Let $O_i \subseteq \{1, \ldots, n\}$ be the collection of indices where $f(e_i)$'s component is 1, i.e.

$$O_i = \left\{ j \mid c_j^{(i)} = 1 \right\}. \tag{5.15}$$

Then the $O_i$'s are pairwise disjoint, as argued above. Also, each $O_i$ is nonempty, since $\operatorname{Ker} f$ is trivial. Now,

$$\sum_{i=1}^{n} f(e_i) = f\left(\sum_{i=1}^{n} e_i\right) = f(1, \ldots, 1) = (1, \ldots, 1). \tag{5.16}$$

Also, the $j$-th component of $\sum_{i=1}^{n} f(e_i)$ is

$$\sum_{i=1}^{n} c_j^{(i)} = 1, \tag{5.17}$$

so that means exactly one $c_j^{(i)} = 1$ and the rest are all 0's. Therefore, the set $\{f(e_i)\}_{i=1}^n$ is just a permutation of $\{e_i\}_{i=1}^n$.

Each $f \in \operatorname{Aut}(\mathbb{Z}^n)$ corresponds to one permutation, and each permutation corresponds to one automorphism. Hence, $|\operatorname{Aut}(\mathbb{Z}^n)| = n!$. ■

**Exercise 5.4.** Let $\varphi : R \to S$ be a morphism of rings. Prove or show a counterexample of the following:

(a) If $\mathfrak{p}_1, \mathfrak{p}_2$ are prime ideals of $R$, then $\mathfrak{p}_1 + \mathfrak{p}_2$ is a prime ideal of $R$.

(b) If $\sqrt{I}$ is a prime ideal of $R$, then $I$ is a prime ideal.

(c) If $\mathfrak{p} \trianglelefteq S$ is a prime ideal, then $\varphi^{-1}(\mathfrak{p}) \trianglelefteq R$ is a prime ideal.

(d) If $\mathfrak{m} \trianglelefteq S$ is a maximal ideal, then $\varphi^{-1}(\mathfrak{m}) \trianglelefteq R$ is a maximal ideal.

*Solution.* (a) False. Take $\mathfrak{p}_1 = (p_1), \mathfrak{p}_2 = (p_2)$ prime ideals of $R = \mathbb{Z}$, where $p_1, p_2$ are distinct primes. Then $(p_1) + (p_2) = (1) = \mathbb{Z}$ is the whole ring, which is not a prime ideal.

(b) False. Take $I = \left(p^2\right)$ in $R = \mathbb{Z}$, which is not a prime ideal. Then

$$\sqrt{(p^2)} = \left\{a \in \mathbb{Z} \mid a^n \in \left(p^2\right) \text{ for some } n > 0\right\} = \{a \in \mathbb{Z} \mid a \in (p)\} = (p), \tag{5.18}$$

is a prime ideal.

(c) True. The proof is written in Exercise 4.40(b).

(d) False. Take $\mathbb{Z} \hookrightarrow \mathbb{Q}$. The only maximal ideal of $\mathbb{Q}$ is $(0)$, whose preimage is $(0)$, and it's not maximal in $\mathbb{Z}$.

More generally, we can take any injective homomorphism $R \to \mathbb{F}$ where $R$ is NOT a field and $\mathbb{F}$ is a field.

■

**Exercise 5.5.** Let $R$ be a ring such that $x = x^2$ for all $x \in R$.

(a) Show that $x + x = 0$ for all $x \in R$.

(b) Show that every finitely generated ideal of $R$ is principal.

*Solution.* (a)

$$x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x. \tag{5.19}$$

Cancelling out $x + x$, we get $x + x = 0$.

(b) It suffices to show that every ideal $(x, y)$ generated by two elements is principal. We claim that

$$(x, y) = (x + y + xy). \tag{5.20}$$

Indeed, $x + y + xy \in (x, y)$, so $(x + y + xy) \subseteq (x, y)$. Now,

$$x(x + y + xy) = x^2 + xy + x^2y = x + xy + xy = x. \tag{5.21}$$

So $x \in (x + y + xy)$. Similarly, $y \in (x + y + xy)$. Hence, $(x + y + xy) = (x, y)$.

Then by induction, $(x_1, \ldots, x_n)$ is principal.

■

**Exercise 5.6.** Let $R$ be a ring.

(a) Assume that every ideal $I \trianglelefteq R$ satisfies $I = \sqrt{I}$. Show that if $J, K \trianglelefteq R$ are ideals and there exists an integer $m > 0$ such that $J^m = K^m$, then $J = K$.

(b) Assume instead that there exists an ideal $I \trianglelefteq R$ such that $I = I^2$ and $I \neq \sqrt{I}$. Show that there exist two distinct ideals $J \neq K$ such that $J^m = K^m$ for all $m > 1$.

(c) Assume now that there exists an ideal $I \trianglelefteq R$ such that $I \neq \sqrt{I}$ and the chain of ideals

$$I \supseteq I^2 \supseteq I^3 \supseteq \cdots \tag{5.22}$$

is stationary. Prove that there exists an ideal $I_0 \trianglelefteq R$ such that $I_0 = I_0^2$, and $\sqrt{I_0} \neq I_0$.

*Solution.* (a) Firstly, note that $\sqrt{I^m} = \sqrt{I}$. Indeed, since $I^m \subseteq I$, we have $\sqrt{I^m} \subseteq \sqrt{I}$. Now, for $a \in \sqrt{I}$, $a^n \in I$ for some $I$. Then

$$a^{mn} = a^n \cdot a^n \cdot \cdots \cdot a^n \in I^m, \tag{5.23}$$

so $a \in \sqrt{I^m}$. So $\sqrt{I} \subseteq \sqrt{I^m}$.

Now, since $J^m = K^m$, we have

$$J = \sqrt{J} = \sqrt{J^m} = \sqrt{K^m} = \sqrt{K} = K. \tag{5.24}$$

(b) Since $I \neq \sqrt{I}$, we can find $z \in \sqrt{I} - I$. Then $z^n \in I$, and assume $n$ is the minimal, so $n > 1$. Now, we take

$$x = z^{\lceil \frac{n}{2} \rceil} \notin I. \tag{5.25}$$

Then $x \in \sqrt{I}$ since $x^2 = z^n$ (or $z^{n+1}$) is in $I$. We take

$$J = I, \quad K = I + (x)\,. \tag{5.26}$$

Then $J \neq K$, since $x \in K$ and $x \notin J$. We'll prove that $J^m = K^m$ for each $m > 1$. Indeed, since $I^2 = I$, $J^m = I^m = I$ for each $m \geq 2$.

Now, since $I \subseteq K$, $I = I^2 \subseteq K^2$. Also, a general element of $K^2$ looks like

$$\sum_{\text{finite}} (i + rx)\left(i' + r'x\right) \tag{5.27}$$

for $i, i' \in I$ and $r, r' \in R$. Simplifying, we get

$$(i + rx)\left(i' + r'x\right) = ii' + rx\ i' + r'x\ i + rr'\ x^2, \tag{5.28}$$

and each term is in $I$, so $K^2 \subseteq I$. Therefore, $K^2 = I = J^2$.

$I \subseteq K$ gives $I = I^m \subseteq K^m$. Suppose $K^{m-1} = I$. Then $K^m = IK \subseteq I$. Therefore, $K^m = I$ provided $K^{m-1} = I$. Since we already proved that $K^2 = I$, we have $K^m = I$ for each $m \geq 2$.

(c) Since the chain $I \supseteq I^2 \supseteq I^3 \supseteq \cdots$ is stationary, there exists some $k \geq 1$ such that

$$I^k = I^{k+1} = I^{k+2} = I^{k+3} = \cdots. \tag{5.29}$$

We take $I_0 = I^k$. Then

$$I_0^2 = \left(I^k\right)^2 = I^{2k} = I^k = I_0. \tag{5.30}$$

Since $I \neq \sqrt{I}$, we can find $x \in \sqrt{I}$, $x \notin I$. Then $x \notin I^k = I_0$ since $I$ contains $I^k$. And $x \in \sqrt{I} = \sqrt{I^k} = \sqrt{I_0}$.

Therefore, we found $I_0$ such that $I_0 = I_0^2$, and $I_0 \neq \sqrt{I_0}$.

■

**Exercise 5.7.** Let $G$ be a group and $p$ a prime number, and $|G| = p^n$ for some integer $n > 0$.

(a) Show that $G$ has a subgroup of order $p^m$ for all $0 \leq m \leq n$.

(b) Show that $G$ has a normal subgroup of order $p^m$ for all $0 \leq m \leq n$.

*Solution.* (a) This is just Exercise 3.23.

(b) We proceed by induction on $n$. The base case $n = 1$ is trivial. Suppose the statement is true for $1, \ldots, n-1$.

Every $p$-group has a nontrivial center (this can be seen by the class-equation.) Therefore, $Z(G)$ contains an element of order $p$ (by Cauchy's theorem), say $a$. Then consider $N = \langle a \rangle$, which is a normal subgroup of order $p$.

So we can consider the quotient $G/N$ which has order $p^{n-1}$, and the quotient map $\pi : G \to G/N$. By inductive hypothesis, $G/N$ has a normal subgroup $N_i$ of order $p^i$ for each $0 \leq i \leq n-1$. Then we just consider $\pi^{-1}(N_i) \trianglelefteq G$, which is normal since preimage of normal subgroups are normal.

$$\left|\pi^{-1}(N_i)\right| = |N_i|\,|\mathrm{Ker}\,\pi| = p^i \cdot p = p^{i+1}. \tag{5.31}$$

Therefore, $G$ has a normal subgroup of order $p^m$ for each $1 \leq m \leq n$. THe normal subgroup of order $p^0$ is the trivial one, $\{e\}$.

■

## §6 Problem Set 4

**Exercise 6.1.** Factor the following polynomials in irreducible factors in $\mathbb{Z}[x]$.

(a) $x^4 + x^2 - x + 2$;

(b) $(x-1)^3 - 2$;

(c) $x^3 + x - 1$.

*Solution.* (a) By checking $f(\pm 1)$, $f(\pm 2)$, we can see that it has no rational root. So the irreducible factors must have degree 2. But in $\mathbb{F}_2[x]$, the polynomial is

$$x^4 + x^2 + x = x\left(x^3 + x + 1\right), \tag{6.1}$$

and $x^3 + x + 1$ is irreducible in $\mathbb{F}_2$ since it doesn't have any roots. In $\mathbb{Z}[x]$, the decomposiition of $x^4 + x^2 - x + 2$ is a product of two degree-2 polynomials (assuming it's reducible). That means, in $\mathbb{F}_2[x]$ as well, we can write $x^4 + x^2 - x + 2$ as a product of two degree-2 polynomials (which might not be irreducible though). But that's not the case, since the decomposiition of $x^4 + x^2 - x + 2$ in $\mathbb{F}_2[x]$ is a product of a degree-1 and a degree-3 polynomials. Therefore, $x^4 + x^2 - x + 2$ is irreducible.

(b) This is $y^3 - 2$, which is irreducible by Eisenstein's criterion.

(c) We reduce it to $\mathbb{F}_2$. If it was reducible, it would have a degree-1 factor, i.e. a root in $\mathbb{F}_2$. But no element of $\mathbb{F}_2$ is a root of $x^3 + x - 1$, so it's irreducible over $\mathbb{F}_2$, and hence it's irreducible over $\mathbb{Z}$.

■

**Exercise 6.2.** (a) Compute the degree of the field extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[4]{5}\right)$.

(b) Compute the degree of the field extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[4]{5}, i\right)$.

(c) Let $\alpha = \sqrt[4]{5} + i$. Find the minimal polynomial $P(x)$ of $\alpha$ over $\mathbb{Q}$.

(d) Find the splitting field of $P(x)$.

*Solution.* (a) $\sqrt[4]{5}$ is a root of $x^4 - 5 \in \mathbb{Q}[x]$. So the degree of the minimal polynomial of $\sqrt[4]{5}$ in $\mathbb{Q}[x]$ is at most 4.

Furthermore, by Eisenstein, $x^4 - 5$ is irreducible, so no polynomial of degree less than 4 has $\sqrt[4]{5}$ as a root. Therefore, $x^4 - 5 \in \mathbb{Q}[x]$ is the minimal polynomial if $\sqrt[4]{5}$. Hence, the degree of the field extension is 4, i.e.

$$\left[\mathbb{Q}\left(\sqrt[4]{5}\right) : \mathbb{Q}\right] = 4. \tag{6.2}$$

(b) $i$ is a root of $x^2+1 \in \mathbb{Q}\left(\sqrt[4]{5}\right)[x]$. Since $\mathbb{Q}\left(\sqrt{45}\right) \subseteq \mathbb{R}$, it doesn't contain any non-real complex numbers, so there doesn't exist any degree-1 polynomial in $\mathbb{Q}\left(\sqrt[4]{5}\right)[x]$ with root $i$. Hence $x^2+1$ is the minimal polynomial of $i$ in $\mathbb{Q}\left(\sqrt[4]{5}\right)[x]$. As a result,

$$\left[\mathbb{Q}\left(\sqrt[4]{5}, i\right) \subseteq \mathbb{Q}\left(\sqrt[4]{5}\right)\right] = \deg\left(x^2+1\right) = 2. \tag{6.3}$$

By tower law,

$$\left[\mathbb{Q}\left(\sqrt[4]{5}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[4]{5}, i\right) : \mathbb{Q}\left(\sqrt[4]{5}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{5}\right) : \mathbb{Q}\right] = 2 \times 4 = 8. \tag{6.4}$$

(c)

$$\begin{aligned}
\alpha = \sqrt[4]{5} + i &\implies (\alpha - i)^4 = 5 && (6.5)\\
&\implies \alpha^4 - 4i\alpha^3 - 6\alpha^2 + 4i\alpha + 1 = 5 && (6.6)\\
&\implies \alpha^4 - 6\alpha^2 - 4 = 4i\alpha\left(\alpha^2 - 1\right) && (6.7)\\
&\implies \left(\alpha^4 - 6\alpha^2 - 4\right)^2 = -16\alpha^2\left(\alpha^2-1\right)^2 && (6.8)\\
&\implies \alpha^8 + 4\alpha^6 - 4\alpha^4 + 64\alpha^2 + 16 = 0. && (6.9)
\end{aligned}$$

Therefore, $\alpha$ is a root of the polynomial $x^8 + 4x^6 - 4x^4 + 64x^2 - 16$. We'll show that this is the minimal polynomial of $\alpha$ over $\mathbb{Q}$.

Note that $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}\left(\sqrt[4]{5}, i\right)$. Now,

$$i = \frac{\alpha^4 - 6\alpha^2 - 4}{4\alpha\left(\alpha^2 - 1\right)} \tag{6.10}$$

implies that $i \in \mathbb{Q}(\alpha)$. Then $\sqrt[4]{5} \in \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt[4]{5}, i\right)$, and as a result

$$\left[\mathbb{Q}\left(\sqrt[4]{5} + i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[4]{5}, i\right) : \mathbb{Q}\right] = 8. \tag{6.11}$$

So the minimal polynomial of $\alpha$ over $\mathbb{Q}$ has degree 8. We found a polynomial of degree 8 which has $\alpha$ as a root. Therefore, $P(x) = x^8 + 4x^6 - 4x^4 + 64x^2 - 16$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$.

(d) Let's list the roots of $P(x)$.

$$P(x) = x^8 + 4x^6 - 4x^4 + 64x^2 - 16. \tag{6.12}$$

All the terms have even degree, so the roots come in $\pm$ pair. But since it's a real polynomial, the roots will come in complex-conjugate pairs. Furthermore, the coefficients are integers, so the roots will come in algebraic-conjugate pairs. This gives all the roots:

$$\pm\left(\sqrt[4]{5} + i\right),\ \pm\left(\sqrt[4]{5} - i\right),\ \pm\left(i\sqrt[4]{5} + i\right),\ \pm\left(i\sqrt[4]{5} - i\right). \tag{6.13}$$

All these are in $\mathbb{Q}\left(\sqrt[4]{5} + i\right) = \mathbb{Q}\left(\sqrt[4]{5}, i\right)$. This is the smallest field that contains $\sqrt[4]{5} + i$.

Therefore, the splitting field of $P(x)$ is $\mathbb{Q}\left(\sqrt[4]{5}+i\right) = \mathbb{Q}\left(\sqrt[4]{5}, i\right)$.

■

**Exercise 6.3.** (a) Show that $P(x) = x^5 + x^4 + 1$ is not irreducible in $\mathbb{F}_2[x]$.

(b) Find the inverse of $x$, in case it exists, in $\mathbb{F}_2[x]/(P(x))$.

(c) Describe all zero-divisors in $\mathbb{F}_2[x]/(P(x))$.

(d) Find the decomposiition in irreducible polynomials of $x^5 + x^4 + 4x + 1 \in \mathbb{Z}[x]$.

*Solution.* (a) $P(x) = x^5 + x^4 + 1$ is divisible by $x^2 + x + 1$ in $\mathbb{F}_2[x]$.

$$x^5 + x^4 + 1 = \left(x^2 + x + 1\right)\left(x^3 + x + 1\right) \text{ in } \mathbb{F}_2[x].. \tag{6.14}$$

(b) In $\mathbb{F}_2[x]/(P(x))$,

$$1 = -1 = x^5 + x^4 = x\left(x^4 + x^3\right). \tag{6.15}$$

Therefore, $x^4 + x^3$ is the inverse of $x$ in $\mathbb{F}_2[x]/(P(x))$.

(c) Let $f \in \mathbb{F}_2[x]$ with $\deg f \leq 4$. Then $f$ is a zero divisor in $\mathbb{F}_2[x]/(P(x))$ if and only if there exists another polynomial $g \in \mathbb{F}_2[x]$ such that

$$P(x) = \left(x^2 + x + 1\right)\left(x^3 + x + 1\right) \mid fg. \tag{6.16}$$

Since $x^2 + x + 1, x^3 + x + 1$ are irreducibles, they are also primes (since $k[x]$ is a PID, and Exercise 6.6). Hence,

$$x^2 + x + 1 \mid f \text{ or } x^2 + x + 1 \mid g. \tag{6.17}$$

Similarly,

$$x^3 + x + 1 \mid f \text{ or } x^3 + x + 1 \mid g. \tag{6.18}$$

If both the irreducibles divide one of $f, g$, then that element is 0. Therefore, the zero divisors of $\mathbb{F}_2[x]/(P(x))$ are multiples of $x^2 + x + 1, x^3 + x + 1$.

(d) It's easy to check that $x^5 + x^4 + 4x + 1$ has no roots in $\mathbb{Q}$, because $\pm 1$ is not a root. Therefore, if it's reducible, it has a degree-2 and a degree-3 factor:

$$\begin{aligned} & x^5 + x^4 + 4x + 1 \\ = & \left(x^2 + Ax + B\right)\left(x^3 + Cx^2 + Dx + E\right) \\ = & x^5 + (A + C)\,x^4 + (D + B + AC)\,x^3 + (E + AD + BC)\,x^2 + (AE + BD)\,x + BE, \end{aligned} \tag{6.19}$$

where $A, B, C, D, E \in \mathbb{Z}$. So we have a system:

$$\begin{aligned} A + C &= 1 \\ D + B + AC &= 0 \\ E + AD + BD &= 0 \\ AE + BD &= 4 \\ BE &= 1. \end{aligned} \tag{6.20}$$

$BE = 1$ gives $B = E = 1$ or $B = E = -1$. In the first case, we have

$$A + D = 4. \tag{6.21}$$

Substituting $C = 1 - A$ and $D = 4 - A$, we get

$$0 = D + B + AC = (4 - A) + 1 + A(1 - A) = 5 - A^2, \tag{6.22}$$

which has no solution in $\mathbb{Z}$. In the case $B = E = -1$,

$$A + D = -4. \tag{6.23}$$

Substituting $C = 1 - A$ and $D = -4 - A$, we get

$$0 = D + B + AC = (-4 - A) - 1 + A(1 - A) = -5 - A^2, \tag{6.24}$$

which has no solution in $\mathbb{Z}$. Therefore, $x^5 + x^4 + 4x + 1$ is irreducible in $\mathbb{Z}[x]$.

■

**Exercise 6.4.** (a) Consider the polynomial $x^7 - 19 \in \mathbb{Q}[x]$ and write its splitting field over $\mathbb{Q}$ as $E = \mathbb{Q}(\alpha, \beta)$, for $\alpha, \beta \in \mathbb{C}$.

(b) Compute $[E : \mathbb{Q}]$.

(c) Find the decomposition in irreducible polynomials of $x^7 - 19$ in $\mathbb{F}_2[x]$.

*Solution.* (a) The roots of the polynomial $P(x) = x^7 - 19$ are

$$\sqrt[7]{19}\omega_7^k \text{ for } k = 0, 1, \ldots, 6, \tag{6.25}$$

where $\omega_7$ is a primitive 7-th root of unity

$$\omega_7 = e^{\frac{2\pi i}{7}}. \tag{6.26}$$

We claim that the splitting field is $\mathbb{Q}\left(\sqrt[7]{19}, \omega_7\right)$. Clearly, $\mathbb{Q}\left(\sqrt[7]{19}, \omega_7\right)$ contains all the roots of $P(x)$. This is the smallest field $E$ that contains all the roots of $P(x)$, since

$$\sqrt[7]{19} = \sqrt[7]{19}\omega_7^0 \in E, \quad \sqrt[7]{19}\omega_7^1 \in E. \tag{6.27}$$

Therefore, $\omega_7^1 \in E$. Hence, $\mathbb{Q}\left(\sqrt[7]{19}, \omega_7\right) \subseteq E$.

Therefore, $E = \mathbb{Q}\left(\sqrt[7]{19}, \omega_7\right)$.

(b) Let's prove a general result first.

**Claim 6.1:** If $[\mathbb{F}(\alpha) : \mathbb{F}]$ and $[\mathbb{F}(\beta) : \mathbb{F}]$ are coprime, then

$$[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}]\,[\mathbb{F}(\beta) : \mathbb{F}]. \tag{6.28}$$

*Proof.* By tower law,

$$[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = [\mathbb{F}(\alpha, \beta) : \mathbb{F}(\alpha)]\,[\mathbb{F}(\alpha) : \mathbb{F}]. \tag{6.29}$$

So $m := [\mathbb{F}(\alpha) : \mathbb{F}]$ divides $[\mathbb{F}(\alpha, \beta) : \mathbb{F}]$. Similarly, $n := [\mathbb{F}(\beta) : \mathbb{F}]$ divides $[\mathbb{F}(\alpha, \beta) : \mathbb{F}]$. Therefore, $mn$ divides $[\mathbb{F}(\alpha, \beta) : \mathbb{F}]$, since they are coprime. Moreover,

$$[\mathbb{F}(\alpha, \beta) : \mathbb{F}(\alpha)] \leq [\mathbb{F}(\beta) : \mathbb{F}], \tag{6.30}$$

because the minimal polynomial of $\beta$ over $\mathbb{F}$ is also a polynomaial in $\mathbb{F}(\alpha)$ with $\beta$ as a root. Therefore, combining (6.29) and (6.30),

$$[\mathbb{F}(\alpha, \beta) : \mathbb{F}] \leq mn. \tag{6.31}$$

Combining this with $mn \mid [\mathbb{F}(\alpha, \beta) : \mathbb{F}]$, we have $[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = mn$. □

$\left[\mathbb{Q}\left(\sqrt[7]{19}\right) : \mathbb{Q}\right]$ is 7, since $\sqrt[7]{19}$ is the root of $x^7 - 19$, which is irreducible by Eisenstein. So $x^7 - 19$ is the minimal polynomaial of $\sqrt[7]{19}$ over $\mathbb{Q}$.

Now, $\omega_7$ is the root of the irreducible polynomial (over $\mathbb{Q}$) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. So we have $[\mathbb{Q}(\omega_7) : \mathbb{Q}] = 6$. Since $\gcd(6, 7) = 1$, by Claim 6.1,

$$\left[\mathbb{Q}\left(\sqrt[7]{19}, \omega_7\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[7]{19}\right) : \mathbb{Q}\right][\mathbb{Q}(\omega_7) : \mathbb{Q}] = 7 \times 6 = 42. \tag{6.32}$$

(c) Reducing to $\mathbb{F}_2[x]$, we have

$$x^7 + 1. \tag{6.33}$$

Clearly, 1 is a root of this polynomial. Furthermore, $1 = -1$, and

$$\frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \tag{6.34}$$

so

$$x^7 + 1 = (x + 1)\left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right). \tag{6.35}$$

$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ has no roots in $\mathbb{F}_2$, as can be checked easily. So it has no degree-1 factors. The only degree-2 irreducible polynomial is $x^2 + x + 1$, which doesn't divide $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Therefore, it has no degree-2 factors either.

The only degree-3 irreducible polynomials are $x^3+x+1$ and $x^3+x^2+1$. One can check that their product is, indeed, $x^6+x^5+x^4+x^3+x^2+x+1$. Therefore,

$$x^7+1=(x+1)\left(x^3+x+1\right)\left(x^3+x^2+1\right). \tag{6.36}$$

■

**Exercise 6.5.** A ring is called **local** if it has a unique maximal ideal.

(a) Let $\varphi: R\to S$ be a morphism of nontrivial rings. Show that if $R$ is local then $\operatorname{im}\varphi$ is local.

(b) Show that a ring $R$ is local if and only if $R\setminus R^*$ is an ideal.

(c) Show that the only idempotents in a local ring are $0,1$.

*Solution.* (a) Let $\mathfrak{m}$ be the unique maximal ideal of $R$. Then $\varphi(\mathfrak{m})\trianglelefteq\varphi(R)=:S'$. $\varphi(\mathfrak{m})$ is a proper ideal, since it doesn't contain 1.

Let $\mathfrak{a}\trianglelefteq S'$ be a proper ideal. Then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}'$. Now, $\varphi^{-1}(\mathfrak{a})$ is a proper ideal of $R$, so it is contained in the unique maximal ideal $\mathfrak{m}$. Hence, $\mathfrak{a}$ is contained in $\varphi(\mathfrak{m})$.

Therefore, every proper ideal $\mathfrak{a}\trianglelefteq S'$ is contained in $\varphi(\mathfrak{m})$. In particular, $\mathfrak{m}'$ is also contained in $\varphi(\mathfrak{m})$. But since $\mathfrak{m}'$ is maximal, we must have that $\mathfrak{m}'=\varphi(\mathfrak{m})$, and hence this is the unique maximal ideal of $\operatorname{im}\varphi=S'$.

(b) Let $R\setminus R^\times$ be an ideal. We claim that this is the unique maximal ideal. Indeed, it is a maximal ideal, since adding an element from $R^\times$ would make it the whole $R$. If there is another maximal ideal $\mathfrak{m}$, since $\mathfrak{m}$ doesn't contain any unit, we must have $\mathfrak{m}\subseteq R\setminus R^\times$. Therefore, $\mathfrak{m}=R\setminus R^\times$ by the maximality of $\mathfrak{m}$.

Now, suppose $R$ is local, and let $\mathfrak{m}$ be the unique maximal ideal. We want to show that $\mathfrak{m}=R\setminus R^\times$. Clearly $\mathfrak{m}\subseteq R\setminus R^\times$ since maximal ideals don't contain units. Take $x\in R\setminus R^\times$. Then $(x)$ is a proper ideal, so it is contained in some maximal ideal, and $\mathfrak{m}$ is the only maximal ideal. Hence,

$$x\in(x)\subseteq\mathfrak{m}. \tag{6.37}$$

Therefore, $R\setminus R^\times\subseteq\mathfrak{m}$, proving that $\mathfrak{m}=R\setminus R^\times$. In particular, $R\setminus R^\times$ is an ideal.

(c) Let $R$ be a local ring with $\mathfrak{m}$ being the unique maximal ideal. Indeed, 0 and 1 are idempotents. If $x$ is an idempotent, we have

$$0=x^2-x=x(x-1). \tag{6.38}$$

Since maximal ideals are prime, we have $x\in\mathfrak{m}$ or $x-1\in\mathfrak{m}$. Note that both can't simultaneously happen, since that would imply $1\in\mathfrak{m}$, i.e. $\mathfrak{m}=R$, which is not possible.

If $x\in\mathfrak{m}$, $x-1\notin\mathfrak{m}$, so we have that $x-1$ is a unit. Multiplying $x(x-1)=0$ by the inverse of $x-1$, we get $x=0$.

If $x - 1 \in \mathfrak{m}$, $x \notin \mathfrak{m}$, so we have that $x$ is a unit. Multiplying $x(x-1) = 0$ by the inverse of $x$, we get $x - 1 = 0$.

Therefore, $x = 0, 1$ are the only idempotents.

■

**Exercise 6.6.** Prove the following:

(a) If $x \in R \setminus \{0\}$ is prime, then it is irreducible.

(b) Let $R$ be a principal ideal domain. Then every irreducible element is prime.

(c) Show that a principal ideal domain is a unique factorization domain.

*Solution.* (a) Let $x = ab$. Then $x \mid ab$, so we have $x \mid a$ or $x \mid b$. WLOG, $x \mid a$, so $a = xc$. This gives

$$x = ab = xcb. \tag{6.39}$$

Cancelling $x$ (since it's nonzero), we get $cb = 1$, i.e. $b$ is a unit. So every factorization $x = ab$ consists of one unit element. Therefore, $x$ is irreducible.

(b) Let $x$ be an irreducible element in a PID $R$. Suppose $x \mid ab$, and $x \nmid a$. We want to show that $x \mid b$.

Consider the ideal $(x, a)$. Since $R$ is PID, then $(x, a) = (y)$ for some $y \in R$. Then $x \in (y)$ gives us that $x = yr$ for some $r \in R$. Since $x$ is irreducible, $r$ or $y$ is a unit.

If $r$ is a unit, then $y = xr^{-1} \in (x)$. So we have $(x) = (y)$. But this can't be the case, since $x \nmid a$, so $a \notin (x)$, but $a \in (y)$.

So $y$ is a unit, and hence $(y) = R$. Therefore, since $(x, a) = R$, we have some $r, s \in R$ such that

$$rx + sa = 1. \tag{6.40}$$

Multiplying by $b$, we get

$$b = rxb + sab = rxb + sx. \tag{6.41}$$

The LHS is divisible by $x$, so $x \mid b$, and we are done!

(c) Let $R$ be a PID. We'll first show that any nonzero non-unit is a product of irreducibles (or primes, since primes and irreducibles are the same in a PID). Assume for the sake of contradiction that $r \in R$ is a nonzero non-unit that can't be written as a product of irreducibles. Then $r$ itself is not an irreducible. Since $r$ is not irreducible, we can write

$$r = r_1 s_1, \tag{6.42}$$

where $r_1, s_1$ are not units. If both of them can be written as a product of irreducibles, then $r$ is a product of irreducibles. So one of them (WLOG it's $r_1$) can't be written as a product of irreducibles. Similarly, since $r_1$ is not irreducible,

$$r_1 = r_2 s_2 \tag{6.43}$$

where $r_2, s_2$ are not units. Then we repeat the same procedure as before. One of $r_2, s_2$ can't be written as a product of irreducibles. WLOG it's $r_2$. We keep doing this, to obtain

$$\cdots \mid r_3 \mid r_2 \mid r_1 \mid r. \tag{6.44}$$

This gives rise to an increasing chain of ideals:

$$(r) \subseteq (r_1) \subseteq (r_2) \subseteq (r_3) \subseteq \cdots . \tag{6.45}$$

Since every PID is Noetherian (a ring where every increasing chain of ideals eventually stabilizes, or equivalently, a ring where every ideal is finitely generated), this chain eventually stabilizes. Therefore,

$$(r_n) = (r_{n+1}) = (r_{n+2}) = \cdots , \tag{6.46}$$

for some $n$. Since $(r_n) = (r_{n+1})$, $r_{n+1} = r_n a$ for some $a \in R$. Then

$$r_n = r_{n+1} s_{n+1} = r_n a s_{n+1}, \tag{6.47}$$

and cancelling out $r_n$ (since we're in a PID, it's an ID, in particular, so cancelling a nonzero element is allowed), we have that $s_{n+1}$ is a unit. But that contradicts the construction. Therefore, we arrive at a contradiction, starting from the assumption that there exists an element $r$ that can't be written as a product of irreducibles. So the assumption must be wrong all along, i.e. every element can be written as a product of irreducibles.

Now, we'll show the uniqueness. Let $r$ be a nonzero non-unit, and

$$r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m, \tag{6.48}$$

are two decomposiition into irreducibles. Since $p_1$ is a prime and $p_1 \mid q_1 q_2 \cdots q_m$, we have that $p_1 \mid q_i$ for some $i$. After reordering, say $p_1 \mid q_1$. So $q_1 = p_1 u$ for some $u \in R$. Since $q_1$ is irreducible, $u$ is a unit. So we have

$$p_1 p_2 \cdots p_n = (p_1 u)\, q_2 \cdots q_m. \tag{6.49}$$

We can cancel out $p_1$ to obtain

$$p_2 \cdots p_n = (u q_2) \cdots q_m. \tag{6.50}$$

unit $\times$ irreducible is also an irreducible. Indeed, if $u$ is a unit and $i$ is a unit, if we write

$ui = ab$, then

$$i = \left(u^{-1}a\right) b. \tag{6.51}$$

Since $i$ is irreducible, either $b$ is a unit, or $u^{-1}a$ is a unit. In the latter case, we have $a$ is a unit (since units form a group). Therefore, from $ui = ab$, we have either $a$ or $b$ is a unit, and hence, $ui$ is an irreducible.

Therefore, in (6.50), we can rewrite $q_2 = uq_2$, since $uq_2$ is irreducible.

$$p_2 \cdots p_n = q_2 \cdots q_m. \tag{6.52}$$

We then keep repeating this process. If $n < m$, then we have

$$1 = q_{n+1} \cdots q_m, \tag{6.53}$$

proving that each $q_{n+1}, \ldots, q_m$ are all units. That's a contradiction, since irreducibles are, by definition, non-units. Hence, $n = m$, and $p_i$ is an unit multiple of $q_i$ (after reordering, of course).

Therefore, $R$ is a UFD.

■

**Exercise 6.7.** (a) Let $p$ be a prime number and $g(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree $n$. Show that $g(x)$ has exactly $n$ distinct roots in every field $\mathbb{F}_{p^m}$, for $m$ positive integer such that $n \mid m$.

(b) Let $K$ be any field and let $G \subset K^*$ be a multiplicative subgroup. Assume that $|G| = n$ for some positive integer $n$. Show that $G$ is cyclic.

(c) Let $p$ be a prime number and consider the polynomial $f(x) \in \mathbb{F}_p[x]$, which can be factored in $\mathbb{F}_p[x]$ in the following way:

$$f(x) = f_1(x)^{\alpha_1} f_2(x)^{\alpha_2} \cdots f_m(x)^{\alpha_m} \tag{6.54}$$

where the polynomials $f_i(x)$ are irreducible and $\alpha_i$ are positive integers. Show that the splitting field of $f(x)$ over $\mathbb{F}_p$ is $\mathbb{F}_{p^n}$, where $n$ is the least common multiple of the degrees of the $f_i(x)$'s.

(d) Find a formula for the number of monic **irreducible** polynomials of degree $n$ in $\mathbb{F}_p[x]$.

*Solution.* (a) Since $g$ is irreducible, the ideal $(g)$ is maximal in $\mathbb{F}_p[x]$, and hence $\mathbb{F}_p[x]/(g)$ is a field. Its size is $p^n$, so $\mathbb{F}_p[x]/(g) \cong \mathbb{F}_{p^n}$.

The class of $x$ is a root of $g$ in $\mathbb{F}_p[x]/(g)$. $\mathbb{F}_p[x]/(g) \cong \mathbb{F}_{p^n}$ naturally embeds into $\mathbb{F}_{p^m}$ for $n \mid m$. Therefore, $g$ has a root in $\mathbb{F}_{p^m}$.

The Frobenius map $\varphi(y) = y^p$ is a ring homomorphism, and fixes $\mathbb{F}_p$ (Fermat's little theorem). Writing $g = \sum c_i x^i$ with $c_i \in \mathbb{F}_p$,

$$g(\alpha^p) = \sum c_i \alpha^{pi} = \sum c_i^p \alpha^{pi} = \left(\sum c_i \alpha^i\right)^p = g(\alpha)^p = 0. \tag{6.55}$$

By induction, $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$ are all roots of $g$.

To show that they are distinct, suppose $\alpha^{p^i} = \alpha^{p^j}$ with $0 \leq i < j \leq n-1$. Since $\varphi$ is injective (any homomorphism from a field is either zero or injective), applying it $i$ times in reverse gives $\alpha^{p^k} = \alpha$ with $k = j - i$, $1 \leq k \leq n-1$. The set

$$S = \{y \in \mathbb{F}_{p^m} : y^{p^k} = y\} \tag{6.56}$$

is a subfield (closed under sums and products as $y \mapsto y^{p^k}$ is a homomorphism, and under inverses), contains $\mathbb{F}_p$, and has at most $p^k$ elements, being the root set of $x^{p^k} - x$. It contains $\alpha$, hence contains $\mathbb{F}_p(\alpha)$, which has $p^n > p^k$ elements. Contradiction.

So $g$ has $n$ distinct roots in $\mathbb{F}_{p^m}$; as $\deg g = n$, these are exactly its roots.

(b) Let $|G| = n$. Let $\psi(d)$ denotes the number of elements in $G$ with order $d$. We claim that $\psi(d) \leq \varphi(d)$, where $\varphi$ is the Euler totient function.

This claim is obviously true when there is no element of order $d$. Now suppose that $\psi(d) \geq 1$. Let $a$ be an element of order $d$. Then consider $H = \langle a \rangle$ be the cyclic subgroup generated by $a$.

$$H = \left\{1, a, a^2, \ldots, a^{d-1}\right\}. \tag{6.57}$$

Then all the elements of $H$ are a solution to $x^d - 1 = 0$, and $|H| = d$. But $\mathbb{F}_q$ is a field, so the polynomial $x^d - 1$ has at most $d$ roots. So $H$ contains all the elements of $G$ having order $d$.

Now, $H$ is isomorphic to the additive group $\mathbb{Z}/d\mathbb{Z}$. In $\mathbb{Z}/d\mathbb{Z}$, the elements that have order $d$ are precisely the ones which are coprime with $d$. Therefore, the number of elements in $H$ with order $d$ is $\varphi(d)$. So $\psi(d) = \varphi(d)$. Hence, $\psi(d) \leq \varphi(d)$ for all $d$.

$$n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n \tag{6.58}$$

Therefore, we must have $\psi(d) = \varphi(d)$ for every $d \mid n$. In particular, $\psi(n) = \varphi(n) \geq 1$. So there exists an element of $G$ that has order $n = |G|$. Therefore, $G$ is a cyclic group.

(c) Let $d_i = \deg f_i$ and $n = \operatorname{lcm}(d_1, \ldots, d_m)$. The polynomials $f$ and $f_1 \cdots f_m$ have the same roots, so they have the same splitting field $L$.

Let's first show that $L \subseteq \mathbb{F}_{p^n}$. Each $d_i \mid n$, so by (a) each $f_i$ has $d_i$ roots in $\mathbb{F}_{p^n}$, i.e. splits there. Hence $f$ splits in $\mathbb{F}_{p^n}$, and the subfield generated by its roots, $L$, lies in $\mathbb{F}_{p^n}$ (with

respect to a fixed copy). Thus $|L| = p^k$. Now,

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : L]\,[L : \mathbb{F}_p] = [\mathbb{F}_{p^n} : L] \cdot k. \tag{6.59}$$

So $k \mid n$.

To show $\mathbb{F}_{p^n} \subseteq L$, note that $L$ contains a root $\beta_i$ of each $f_i$, and $[\mathbb{F}_p(\beta_i) : \mathbb{F}_p] = d_i$. By the tower law,

$$k = [L : \mathbb{F}_p] = [L : \mathbb{F}_p(\beta_i)]\,[\mathbb{F}_p(\beta_i) : \mathbb{F}_p] = [L : \mathbb{F}_p(\beta_i)] \cdot d_i. \tag{6.60}$$

So $d_i \mid k$ for all $i$, so $n \mid k$. Hence $k = n$ and $L \cong \mathbb{F}_{p^n}$.

(d) Let $P_d$ be the set of degree-$d$ irreducible polynomials in $\mathbb{F}_p[x]$. We claim that

$$x^{p^n} - x = \prod_{d \mid n} \prod_{f \in P_d} f. \tag{6.61}$$

Notice that $x^{p^n} - x = x\left(x^{p^n-1} - 1\right)$. Since $\left|\mathbb{F}_{p^n}^\times\right| = p^n - 1$, every element of $\mathbb{F}_{p^n}^\times$ is a root of $x^{p^n-1} - 1$. Therefore, every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^n} - x$, and no root is repeated.

If $f \in P_d$ with $d \mid n$, then $f$ splits in $\mathbb{F}_{p^n}$. Therefore, $f \mid x^{p^n} - x$. Conversely, let $f$ be a monic irreducible (over $\mathbb{F}_p$) factor of $x^{p^n} - x$, with $\deg f = d$. Then $f$ has a root $\alpha \in \mathbb{F}_{p^n}$. By tower law,

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)]\,[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)] \deg f. \tag{6.62}$$

So $d = \deg f \mid n$. Therefore, (6.61) holds! Counting degrees, we have

$$p^n = \sum_{d \mid n} d\,|P_d|\,. \tag{6.63}$$

Using Möbius inversion formula, we can transform an equation of the form $g(n) = \sum_{d \mid n} f(d)$ to $f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$, where $\mu$ is the Möbius function defined by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1, \\ (-1)^k & \text{if } m \text{ is squarefree, and } m = p_1 p_2 \cdots p_k, \\ 0 & \text{if } m \text{ is not squarefree.} \end{cases} \tag{6.64}$$

So using the Möbius inversion formula, we have

$$n\,|P_n| = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d \implies \boxed{|P_n| = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d}. \tag{6.65}$$

■

## §7 Problems on Fields from Lothar Göttsche's Notes

**Exercise 7.1.** Let $k$ be a field. Find all elements $a \in k$ with $a = a^{-1}$.

*Solution.* $a = a^{-1}$ implies

$$a^2 = 1 \implies a^2 - 1 = 0 \implies (a+1)(a-1) = 0. \tag{7.1}$$

A field is an ID, in particular. So $(a+1)(a-1) = 0$ implies $a+1 = 0$ or $a-1 = 0$, i.e. $a = \pm 1$. (Note that if $\operatorname{char} k = 2$, then $1 = -1$, so there is only one solution $a = 1$.) ■

**Exercise 7.2.** Let $F$ be a field with precisely 8 elements. Prove or disprove: The characteristic of $F$ is 2.

*Solution.* We'll prove the general result:

> Let $\mathbb{F}$ be a field with $|\mathbb{F}| = p^n$ for some prime $p$. Then $\operatorname{char} \mathbb{F} = p$.

$\operatorname{char} \mathbb{F}$ is the order of 1 in the additive group $(\mathbb{F}, +)$. Since the order of an element divides the order of the group, $\operatorname{char} \mathbb{F} \mid p^n$. But the characteristic of a field (if it's positive) is a prime number. So $\operatorname{char} \mathbb{F} = p$. ■

**Exercise 7.3.** Let $a = 2^{\frac{1}{p}} \in \mathbb{C}$ for a prime number $p$. Show that $[\mathbb{Q}(a) : \mathbb{Q}] = p$ and the only intermediate fields of $\mathbb{Q}(a)/\mathbb{Q}$ are $\mathbb{Q}$ and $\mathbb{Q}(a)$.

*Solution.* The minimal polynomial of $a$ is $x^p - 2$, which is irreducible by Eisenstein. $\mathbb{Q}(a)$ is a $\mathbb{Q}$-vector space with basis $1, a, \ldots, a^{p-1}$, so we have $[\mathbb{Q}(a) : \mathbb{Q}] = p$.

If there is an intermediate field $\mathbb{Q} \leq F \leq \mathbb{Q}(a)$, then by tower law,

$$p = [\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : F][F : \mathbb{Q}]. \tag{7.2}$$

Since $p$ is a prime number, either $[\mathbb{Q}(a) : F] = 1$ or $[F : \mathbb{Q}] = 1$. The former gives $F = \mathbb{Q}(a)$, and the latter gives $F = \mathbb{Q}$. ■

**Exercise 7.4.** Let $a$ be a positive rational number, which is not a square in $\mathbb{Q}$. Show that $[\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}] = 4$.

*Solution.* $\sqrt[4]{a}$ is a root of $x^4 - a$. Since $\sqrt[4]{a}$ is irrational, $x^4 - a$ doesn't have any degree-1 factor in $\mathbb{Q}[x]$. Since $a$ is not a square in $\mathbb{Q}$, $x^4 - a$ doesn't split into two degree-2 polynomials either. Therefore, $x^4 - a$ is irreducible in $\mathbb{Q}[x]$, and hence, it's the minimal polynomial of $\alpha = \sqrt[4]{a}$.

Now, $\mathbb{Q}(\alpha)$ is a $\mathbb{Q}$-vector space with basis $1, \alpha, \alpha^2, \alpha^3$. So $[\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}] = 4$. ■

**Exercise 7.5.** Let $K/k$ be a field extension. Let $\alpha \in K$ be a zero of an irreducible polynomial $x^3 - ax + b \in k[x]$. Find explicitly the inverse of $1 + \alpha$ in $k(\alpha)$ in the form $u + v\alpha + w\alpha^2$ with $u, v, w \in k$.

*Solution.*

$$1 = (1+\alpha)\left(u + v\alpha + w\alpha^2\right) = u + (u+v)\alpha + (v+w)\alpha^2 + w\alpha^3 \tag{7.3}$$
$$= u + (u+v)\alpha + (v+w)\alpha^2 + w(a\alpha - b) \tag{7.4}$$
$$= (u - wb) + (u + v + wa)\alpha + (v+w)\alpha^2. \tag{7.5}$$

So we have a system of equations:

$$\begin{aligned} u - wb &= 1 \\ u + v + wa &= 0 \\ v + w &= 0 \end{aligned} \tag{7.6}$$

Substituting $w = -v$, we have

$$\begin{aligned} u + vb &= 1 \\ u + v - va &= 0. \end{aligned} \tag{7.7}$$

From this we have,

$$v = \frac{1}{a+b-1}. \tag{7.8}$$

So

$$w = -\frac{1}{a+b-1}. \tag{7.9}$$

Then

$$u = 1 + wb = 1 - \frac{b}{a+b-1} = \frac{a-1}{a+b-1}. \tag{7.10}$$

Therefore,

$$(1+\alpha)^{-1} = \frac{a-1}{a+b-1} + \frac{1}{a+b-1}\,\alpha - \frac{1}{a+b-1}\,\alpha^2. \tag{7.11}$$

■

**Exercise 7.6.** Let $n \in \mathbb{Z}_{\geq 1}$. Construct a field extension $K \subset \mathbb{C}$ of $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$.

*Solution.* Let $p$ be a prime number. Then the minimal polynomial of $p^{\frac{1}{n}}$ is $x^n - p$ (which is irreducible by Eisenstein). Therefore, $\left[\mathbb{Q}\left(p^{\frac{1}{n}}\right) : \mathbb{Q}\right] = n$. ■

**Exercise 7.7.** Let $p, q$ be distinct prime numbers and let $K := \mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$. Prove the following:

(a) $[K : \mathbb{Q}] = 4$,

(b) $K = \mathbb{Q}\left(\sqrt{p} + \sqrt{q}\right)$,

(c) The minimal polynomial of $\sqrt{p}+\sqrt{q}$ over $\mathbb{Q}$ is

$$x^4 - 2(p+q)x^2 + (p-q)^2. \tag{7.12}$$

*Solution.* (a) By tower law,

$$[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}(\sqrt{p})]\,[\mathbb{Q}(\sqrt{p}):\mathbb{Q}] \tag{7.13}$$

$\left[\mathbb{Q}\left(\sqrt{p}\right):\mathbb{Q}\right] = 2$, because $\left\{1,\sqrt{p}\right\}$ is a basis of $\mathbb{Q}\left(\sqrt{p}\right)$ over $\mathbb{Q}$.

$\left[\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right):\mathbb{Q}\left(\sqrt{p}\right)\right]$ is either 1 or 2, because $\sqrt{q}$ is a root of $x^2-q$. If it's 1, then $\sqrt{q}\in\mathbb{Q}\left(\sqrt{p}\right)$. But in that case,

$$a+b\sqrt{p} = \sqrt{q} \text{ for some } a,b\in\mathbb{Q}. \tag{7.14}$$

Squaring and simplifying, we have

$$2ab\sqrt{p} = q - a^2 - b^2p. \tag{7.15}$$

If $a=0$, then $q=b^2p$. Say $b=\frac{m}{n}$ with $m,n\in\mathbb{Z}$ with $\gcd(m,n)=1$. Then

$$pm^2 = qn^2. \tag{7.16}$$

But then $p \mid qn^2$ implies $p \mid n^2$. This gives $p^2 \mid n^2$. But that implies $p^2 \mid pm^2$, i.e. $p \mid m^2$. This contradicts $\gcd(m,n)=1$.

If $b=0$, then $q=a^2$, which is not possible since $\sqrt{q}\notin\mathbb{Q}$. If $ab\neq 0$, then

$$\sqrt{p} = \frac{q-a^2-b^2p}{2ab}, \tag{7.17}$$

which is not possible since $\sqrt{p}\notin\mathbb{Q}$. Therefore, $\left[\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right):\mathbb{Q}\left(\sqrt{p}\right)\right]=2$. Hence,

$$[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}(\sqrt{p})]\,[\mathbb{Q}(\sqrt{p}):\mathbb{Q}] = 2\cdot 2 = 4. \tag{7.18}$$

(b) Since $\sqrt{p}+\sqrt{q}\in\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right)$, we have that $\mathbb{Q}\left(\sqrt{p}+\sqrt{q}\right)\subseteq\mathbb{Q}\left(\sqrt{p},\sqrt{q}\right)$. Now, we need to show the other inclusion.

$$\left(\sqrt{p}+\sqrt{q}\right)^2 = p+q+2\sqrt{pq}, \tag{7.19}$$

so $\sqrt{pq}\in\mathbb{Q}\left(\sqrt{p}+\sqrt{q}\right)$. Now,

$$\sqrt{pq}\,(\sqrt{p}+\sqrt{q}) = p\sqrt{q}+q\sqrt{p}. \tag{7.20}$$

So $p\sqrt{q}+q\sqrt{p}\in\mathbb{Q}\left(\sqrt{p}+\sqrt{q}\right)$. Therefore,

$$(p\sqrt{q}+q\sqrt{p}) - q\,(\sqrt{p}+\sqrt{q}) = (p-q)\sqrt{q}. \tag{7.21}$$

Since $p-q \in \mathbb{Q}$, we have that $\sqrt{q} \in \mathbb{Q}\left(\sqrt{p}+\sqrt{q}\right)$. Then we have $\sqrt{p} \in \mathbb{Q}\left(\sqrt{p}+\sqrt{q}\right)$. Hence, $\mathbb{Q}\left(\sqrt{p}+\sqrt{q}\right) \supseteq \mathbb{Q}\left(\sqrt{p}, \sqrt{q}\right)$.

(c) Let $\alpha = \sqrt{p}+\sqrt{q}$. So

$$\begin{aligned}
\alpha^2 = p+q+2\sqrt{pq} &\implies 2\sqrt{pq} = \alpha^2 - (p+q) \\
&\implies 4pq = \alpha^4 + (p+q)^2 - 2\alpha^2 (p+q) \\
&\implies \alpha^4 - 2\alpha^2 (p+q) + \left[(p+q)^2 - 4pq\right] = 0 \\
&\implies \alpha^4 - 2\alpha^2 (p+q) + (p-q)^2 = 0.
\end{aligned}$$

So $\alpha$ is a root of $x^4 - 2(p+q)x^2 + (p-q)^2$. The degree of the field extension $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, this is the minimal polynomial of $\alpha$ over $\mathbb{Q}$.

■

**Exercise 7.8.** Determine the minimal polynomial of $\sqrt{3}+\sqrt{5}$ over each of the following fields.

(a) $\mathbb{Q}$.

(b) $\mathbb{Q}\left(\sqrt{5}\right)$.

(c) $\mathbb{Q}\left(\sqrt{15}\right)$.

*Solution.* (a) The minimal polynomial of $\sqrt{3}+\sqrt{5}$ over $\mathbb{Q}$ is $x^4 - 2(3+5)x^2 + (3-5)^2$. (Exercise 7.7c)

(b) Clearly, $\sqrt{3}+\sqrt{5} \notin \mathbb{Q}\left(\sqrt{5}\right)$, as we have shown earlier that $\sqrt{q} \notin \mathbb{Q}\left(\sqrt{p}\right)$. (Exercise 7.7a) So the minimal polynomial can't have degree-1. Let $\alpha = \sqrt{3}+\sqrt{5}$. Then

$$\alpha - \sqrt{5} = \sqrt{3} \implies \alpha^2 - 2\alpha\sqrt{5} + 5 = 3. \tag{7.22}$$

Therefore, $\alpha$ is a root of $x^2 - 2\sqrt{5}x + 2$. So it is the minimal polynomial of $\sqrt{3}+\sqrt{5}$ over $\mathbb{Q}\left(\sqrt{5}\right)$.

(c) Since $\mathbb{Q}\left(\sqrt{3}, \sqrt{5}\right) = \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$, we'll first show that

$$\mathbb{Q}\left(\sqrt{3}, \sqrt{5}\right) \neq \mathbb{Q}\left(\sqrt{15}\right). \tag{7.23}$$

Assume for the sake of contradiction that $\sqrt{3} \in \mathbb{Q}\left(\sqrt{15}\right)$. Then

$$\sqrt{3} = a + b\sqrt{15} \text{ for some } a, b \in \mathbb{Q}. \tag{7.24}$$

Squaring and rearranging, we have

$$3 - a^2 - 15b^2 = 2ab\sqrt{15}. \tag{7.25}$$

If $ab \neq 0$, this just gives us that $\sqrt{15} \in \mathbb{Q}$, which is not possible. If $a = 0$, we have $3 = 15b^2$, which is also not possible since $\frac{1}{\sqrt{5}} \notin \mathbb{Q}$. If $b = 0$, we have $3 = a^2$, which is also not possible since $\sqrt{3} \notin \mathbb{Q}$. Therefore, $\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right) : \mathbb{Q}\left(\sqrt{15}\right)\right]$ is not 1. Now,

$$\alpha^2 = 3 + 5 + 2\sqrt{15} = 8 + 2\sqrt{15}. \tag{7.26}$$

Therefore, $x^2 - 8 - 2\sqrt{15}$ is a degree-2 monic polynomial which has $\alpha$ as a root. Since there is no degree-1 polynomial in $\mathbb{Q}\left(\sqrt{15}\right)[x]$ which has $\alpha$ has a root, this is the minimal polynomial.

Therefore, the minimal polynomial of $\sqrt{3}+\sqrt{5}$ over $\mathbb{Q}\left(\sqrt{15}\right)$ is $x^2 - 8 - 2\sqrt{15}$.

■

**Exercise 7.9.** Let $a := \sqrt{2}$, $b := 3^{\frac{1}{3}} \in \mathbb{C}$. Show $[\mathbb{Q}(a,b) : \mathbb{Q}] = 6$.

*Solution.* $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$ since $\sqrt{2}$'s minimal polynomial is $x^2 - 2$ (irreducible by Eisenstein), and $\left[\mathbb{Q}\left(3^{\frac{1}{3}}\right) : \mathbb{Q}\right] = 3$ since $3^{\frac{1}{3}}$'s minimal polynomial is $x^3 - 3$ (irreducible by Eisenstein). Since $\gcd(2,3) = 1$, we have $[\mathbb{Q}(a,b) : \mathbb{Q}] = 6$, by Claim 6.1. ■

**Exercise 7.10.** Determine $\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right) : \mathbb{Q}\right]$.

*Solution.* This is a special case of Exercise 7.7. ■

**Exercise 7.11.** Assume $[k(a) : k] = n$, $[k(b) : k] = m$ and $n, m$ are relatively prime. Show that $[k(a,b) : k] = nm$.

*Solution.* This is just Claim 6.1. ■

**Exercise 7.12.** Decide whether or not $i$ is in the field

(a) $\mathbb{Q}\left(\sqrt{-2}\right)$.

(b) $\mathbb{Q}\left(\sqrt[4]{-2}\right)$.

(c) $\mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$.

*Solution.* (a) Suppose $i \in \mathbb{Q}\left(\sqrt{-2}\right) = \left\{a + bi\sqrt{2} | a, b \in \mathbb{Q}\right\}$. Then

$$i = a + bi\sqrt{2} \text{ for some } a, b \in \mathbb{Q}. \tag{7.27}$$

Squaring and rearranging, we have

$$-1 - a^2 + 2b^2 = 2abi\sqrt{2}. \tag{7.28}$$

If $ab \neq 0$, the LHS is a real number but the RHS is imaginary. If $a = 0$, we have $2b^2 = 1$, but that's not possible since $\frac{1}{\sqrt{2}} \notin \mathbb{Q}$. If $b = 1$, we have $a^2 = -1$, which has no solution in $\mathbb{Q}$. Therefore, $i \notin \mathbb{Q}\left(\sqrt{-2}\right)$.

(b) $\sqrt[4]{-2}$ is a root of $x^4+2$, which is irreducible over $\mathbb{Q}$ by Eisenstein. Therefore, $\left[\mathbb{Q}\left(\sqrt[4]{-2}\right) : \mathbb{Q}\right] = 4$. Suppose $i \in \mathbb{Q}\left(\sqrt[4]{-2}\right)$. Now, notice that the roots of $x^4 + 2$ are:

$$r_1 = \sqrt[4]{-2} = \sqrt[4]{2}e^{\frac{i\pi}{4}}, \quad r_2 = ir_1, \quad r_3 = -r_1, \quad r_4 = -ir_1. \tag{7.29}$$

The splitting field of $x^4 + 2$ is $\mathbb{Q}(r_1, i)$. This is equal to $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$. Indeed,

$$r_1 = \sqrt[4]{2}e^{\frac{i\pi}{4}} = \sqrt[4]{2}\,\frac{1+i}{\sqrt{2}} \in \mathbb{Q}\left(\sqrt[4]{2}, i\right). \tag{7.30}$$

So we have $\mathbb{Q}(r_1, i) \subseteq \mathbb{Q}\left(\sqrt[4]{2}, i\right)$. Similarly,

$$r_1 - r_2 = (1-i)\,r_1 = (1-i)\,\sqrt[4]{2}\frac{1+i}{\sqrt{2}} = \left[\sqrt[4]{2}\right]^3. \tag{7.31}$$

If we square this,

$$\left[\sqrt[4]{2}\right]^6 = 2\sqrt{2}. \tag{7.32}$$

So $\sqrt{2} \in \mathbb{Q}(r_1, i)$. Dividing $\left[\sqrt[4]{2}\right]^3$ by $\sqrt{3}$, we have that $\sqrt[4]{2} \in \mathbb{Q}(r_1, i)$. Therefore, $\mathbb{Q}(r_1, i) \subseteq \mathbb{Q}\left(\sqrt[4]{2}, i\right)$ is the splitting field of $x^4 + 2$.

Now, if $i \in \mathbb{Q}\left(\sqrt[4]{-2}\right)$, then

$$\mathbb{Q}\left(\sqrt[4]{-2}\right) = \mathbb{Q}\left(\sqrt[4]{-2}, i\right) = \mathbb{Q}\left(\sqrt[4]{2}, i\right). \tag{7.33}$$

Now,

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\left(\sqrt[4]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8, \tag{7.34}$$

since $i$ is a root of $x^2 + 1$, and it's irreducible over $\mathbb{Q}\left(\sqrt[4]{2}\right)$ since $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is a subfield of $\mathbb{R}$.

Now,

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\right] = 8 \text{ and } \left[\mathbb{Q}\left(\sqrt[4]{-2}\right) : \mathbb{Q}\right] = 4. \tag{7.35}$$

Therefore, we arrive at a contradiction! So $i \notin \mathbb{Q}\left(\sqrt[4]{-2}\right)$.

(c) Suppose $i \in \mathbb{Q}(\alpha)$. Then $\mathbb{Q}(i) \subseteq \mathbb{Q}(\alpha)$. Then

$$3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(i)]\,[\mathbb{Q}(i) : \mathbb{Q}] = 2\,[\mathbb{Q}(\alpha) : \mathbb{Q}(i)], \tag{7.36}$$

which is not possible since $2 \nmid 3$. Therefore, $i \notin \mathbb{Q}(\alpha)$.

■

**Exercise 7.13.** Let $\alpha := e^{2\pi i/7}$, $\beta := e^{2\pi i/5}$. Prove that $\beta \notin \mathbb{Q}(\alpha)$.

*Solution.* Assume for the sake of contradiction that $\beta \in \mathbb{Q}(\alpha)$. Then $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$. Then

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] [\mathbb{Q}(\beta) : \mathbb{Q}]. \tag{7.37}$$

Now, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ since $\alpha$ is a root of the irreducible (over $\mathbb{Q}$) polynomial $x^6 + x^5 + \cdots + 1$. And, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$ since $\beta$ is a root of the irreducible (over $\mathbb{Q}$) polynomial $x^4 + x^3 + \cdots + 1$. Therefore,

$$6 = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot 4. \tag{7.38}$$

This is not possible since $4 \nmid 6$. ■

**Exercise 7.14.** Let $\alpha, \beta$ be complex numbers with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. Determine the possiblities for $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$.

*Solution.* By tower law

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]. \tag{7.39}$$

Now, the minimal polynomial of $\beta$ over $\mathbb{Q}$ has degree 3. So the minimal polynomial of $\beta$ over $\mathbb{Q}(\alpha)$ has degree at most 3. So the possiblities of $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ are $3, 6, 9$. We now show that all are achievable.

- Let $\alpha = \sqrt[3]{2}$, and $\beta = 2\sqrt[3]{2}$. Then $\left[\mathbb{Q}\left(\sqrt[3]{2}, 2\sqrt[3]{2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$.
- Let $\alpha = \sqrt[3]{2}$, and $\beta = \omega\sqrt[3]{2}$, where $\omega = e^{\frac{2\pi i}{3}}$ is a cubic root of unity. Then

  $$\mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}\right) = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right). \tag{7.40}$$

  The minimal polynomials of $\sqrt[3]{2}$ and $\omega$ over $\mathbb{Q}$ are $x^3 - 2$ and $x^2 + x + 1$, respectively. Therefore, $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, and they are coprime. Therefore,

  $$\left[\mathbb{Q}\left(\sqrt[3]{2}, \omega\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] [\mathbb{Q}(\omega) : \mathbb{Q}] = 6. \tag{7.41}$$

- Let $\alpha = \sqrt[3]{2}$, and $\beta = \sqrt[3]{3}$. Then $\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{3}\right) : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] \leq 3$, since $x^3 - 3$ is a polynomial with root $\sqrt[3]{3}$. Now, we claim that this is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$. This would be reducible if and only if it had a linear factor, i.e. $x^3 - 3$ has a root in $\mathbb{Q}\left(\sqrt[3]{2}\right)$. Since $\mathbb{Q}\left(\sqrt[3]{2}\right)$ is a subfield of $\mathbb{R}$, it can only contain the real root $\sqrt[3]{3}$.

  If $\sqrt[3]{3} \in \mathbb{Q}\left(\sqrt[3]{2}\right)$, then

  $$\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4} \text{ for some } a, b, c \in \mathbb{Q}. \tag{7.42}$$

  Taking trace (studied from here: https://qk206.user.srcf.net/notes/galois_theory.pdf, Section 2.2) and noting that $\mathrm{Tr}\left(\sqrt[3]{3}\right) = \mathrm{Tr}\left(\sqrt[3]{2}\right) = \mathrm{Tr}\left(\sqrt[3]{4}\right) = 0$, we get that $a = 0$.

Then cubing the equation, we have

$$3 = 2b^3 + 4c^3 + 6bc\left(b\sqrt[3]{2} + c\sqrt[3]{4}\right) = 2b^3 + 4c^3 + 6bc\sqrt[3]{3}. \tag{7.43}$$

If $bc \neq 0$, we have that $\sqrt[3]{3} \in \mathbb{Q}$. If $b = 0$, we have $4c^3 = 3$, which has no solution in $\mathbb{Q}$. If $c = 0$, we have $2b^3 = 3$, which has no solution in $\mathbb{Q}$.

Therefore, $\sqrt[3]{3} \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$. And hence, $x^3 - 3$ is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$. Hence,

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{3}\right) : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3 \cdot 3 = 9. \tag{7.44}$$

■

**Exercise 7.15.** Let $\alpha, \beta$ be complex roots of irreducible polynomials $f, g \in \mathbb{Q}[x]$ respectively. Let $F := \mathbb{Q}(\alpha)$, $K := \mathbb{Q}(\beta)$. Show that $f$ is irreducible in $K[x]$ if and only if $g$ is irreducible in $F[x]$.

*Solution.* By tower law,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]. \tag{7.45}$$

Therefore, $f$ (which is the minimal polynomial of $\alpha$ over $\mathbb{Q}$) is irreducible over $\mathbb{Q}(\beta)$ implies

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = \deg f = [\mathbb{Q}(\alpha) : \mathbb{Q}]. \tag{7.46}$$

Therefore,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]. \tag{7.47}$$

As a result,

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]. \tag{7.48}$$

So the minimal polynomial $g$ of $\beta$ over $\mathbb{Q}$ is irreducible over $\mathbb{Q}(\alpha)$ (because otherwise, the degree $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ would be smaller).

Therefore, $f$ irreducible over $\mathbb{Q}(\beta)$ implies $g$ irreducible over $\mathbb{Q}(\alpha)$. Swapping $f$ and $g$, $\alpha$ and $\beta$, we get the reverse implication as well! ■

**Exercise 7.16.** Let $a \in \mathbb{C}$ be algebraic over $\mathbb{Q}$. We say that $a$ is an *algebraic integer* if it satisfies a monic equation $a^n + b_{n-1}a^{n-1} + \cdots + b_0 = 0$, with $b_0, \ldots, b_{n-1} \in \mathbb{Z}$.

(a) Let $a \in \mathbb{C}$ be algebraic over $\mathbb{Q}$. Show there exists a positive integer $m$ such that $ma$ is an algebraic integer.

(b) If $r \in \mathbb{Q}$ is an algebraic integer, then $r \in \mathbb{Z}$.

(c) Let $\alpha$ be an algebraic integer satisfying $\alpha^3 + \alpha + 1 = 0$ and $\beta$ an algebraic integer satisfying $\beta^2 + \beta - 3 = 0$. Show that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers.

*Solution.* (a) Since $a$ is algebraic over $\mathbb{Q}$, it's a root of a polynomial in $\mathbb{Q}[x]$. So

$$\sum_{i=0}^{n} c_i a^i = 0. \tag{7.49}$$

We can assume WLOG that $c_n > 0$ (otherwise, just multiply the whole thing by $-1$). Now, we can turn this into a polynomial in $\mathbb{Z}[x]$ multiplying by the lcm of the denominators of the coefficients.

$$\sum_{i=0}^{n} b_i a^i = 0, \quad b_i \in \mathbb{Z}, b_n > 0. \tag{7.50}$$

Multiplying by $b_n^{n-1}$, we have

$$\begin{aligned} 0 &= \sum_{i=0}^{n} b_i b_n^{n-1} a^i && (7.51)\\ &= (b_n a)^n + b_{n-1}(b_n a)^{n-1} + b_{n-2} b_n (b_n a)^{n-2} + \cdots + b_1 b_n^{n-2}(b_n a) + b_1 b_n^{n-1}. && (7.52) \end{aligned}$$

Therefore, $b_n a$ is a root of a monic integer polynomial. Hence, $b_n a$ is an algebraic integer.

(b) Exercise 4.45.

(c) We'll prove an intermediate result first.

**Claim 7.1:** If $V \subseteq \mathbb{C}$ is a finite-dimensional $\mathbb{Q}$-vector space and $x \in \mathbb{C}$ with $xV \subseteq V$, then $x$ is an algebraic number, i.e. $x \in \overline{\mathbb{Q}}$.

*Proof.* Let $e_1, \ldots, e_n$ be a $\mathbb{Q}$-basis for $V$. Then

$$\begin{aligned} xe_1 &= a_{11}e_1 + \cdots + a_{1n}e_n \\ xe_2 &= a_{21}e_1 + \cdots + a_{2n}e_n \\ &\cdots \\ xe_n &= a_{n1}e_1 + \cdots + a_{nn}e_n. \end{aligned} \tag{7.53}$$

Then we have $\det(xI - A) = 0$, where

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}. \tag{7.54}$$

Now, $\det(xI - A) = 0$ is a monic polynomial equation in $x$ with coefficients in $\mathbb{Q}$. Therefore, $x \in \overline{\mathbb{Q}}$. □

Now, let

$$V = \operatorname{span}_{\mathbb{Q}} \left\{ \alpha^i \beta^j \mid i = 0, 1, 2 \text{ and } j = 0, 1 \right\}. \tag{7.55}$$

Then $(\alpha + \beta)V \subseteq V$. So $\alpha + \beta \in \overline{\mathbb{Q}}$. Also, notice that the coefficients $a_{ij}$ in $A$ (7.54) are

integers. Therefore, $\alpha+\beta$ is an algebraic integer. Similarly, $\alpha\beta V \subseteq V$, and the coefficients $a_{ij}$ in $A$ (7.54) are integers. Therefore, $\alpha\beta$ is an algebraic integer.

■

**Exercise 7.17.** Let $k$ be a field and assume $x^n - a$ is irreducible over $K$ and $m \mid n$. Let $u$ be a zero of $x^n - a$ over an extension $K/k$. Show $[k(u^m) : k] = n/m$. Determine the minimal polynomial of $u^m$ over $k$.

*Solution.* Let $d = \frac{n}{m}$, and $v = u^m$. Since $x^d - a$ is a degree-$d$ polynomial with $v$ as a root, we have

$$[k(u^m) : k] \leq d. \tag{7.56}$$

Now, by tower law,

$$n = [k(u) : k] = [k(u) : k(v)]\,[k(v) : k] \tag{7.57}$$

$[k(u) : k(v)]$ is at most $m$, since $v = u^m$, so $u$ is a root of a degree-$m$ polynomial $x^m - v \in k(v)[x]$. Therefore,

$$n = [k(u) : k(v)]\,[k(v) : k] \leq m\,[k(v) : k]. \tag{7.58}$$

This gives

$$[k(v) : k] \geq \frac{n}{m} = d. \tag{7.59}$$

Therefore, $[k(u^m) : k] = d$, and the minimal polynomial of $v$ over $k$ is $x^d - a$. ■

**Exercise 7.18.** Let $k$ be a field, let $a, b$ be algebraic over $k$ with $[k(a) : k] = n$, $[k(b) : k] = m$. Show that $[k(a,b) : k] \leq nm$ with equality if $n$ and $m$ are relatively prime.

*Solution.* As in the proof of Claim 6.1, $[k(a,b) : k] \leq nm$. If $\gcd(n,m) = 1$, we have equality, as we proved in Claim 6.1. ■

**Exercise 7.19.** Show that $\overline{\mathbb{Q}}$ is algebraically closed.

*Solution.* Let $f = \sum_{i=0}^{n} a_i x^i \in \overline{\mathbb{Q}}[x]$, and $\beta$ is a root of $f$. We need to show that $\beta \in \overline{\mathbb{Q}}$.

Let $K = \mathbb{Q}(a_0, \ldots, a_n)$. Then $\mathbb{Q} \leq K$ is a finite extension (since we're adding finitely many algebraic elements). $K \leq K(\beta)$ is also a finite extension whose degree is at most $n$ (as $\beta$ is a root of a degree-$n$ polynomial in $K[x]$). Therefore, by tower law,

$$\mathbb{Q} \leq K(\beta) = \mathbb{Q}(a_0, \ldots, a_n, \beta) \tag{7.60}$$

is also a finite extension, and hence, algebraic. In particular, $\beta$ is a root of a polynomial in $\mathbb{Q}[x]$. So $\beta \in \overline{\mathbb{Q}}$. ■

**Exercise 7.20.** Let $f = x^4 + x^2 + 1 \in \mathbb{Q}[x]$. Let $\omega := \frac{-1+\sqrt{3}i}{2}$. Show that $\mathbb{Q}(\omega)$ is the splitting field of $f$ over $\mathbb{Q}$ and that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

We can factorize $x^4 + x^2 + 1$ as

$$x^4 + x^2 + 1 = .\left(x^2 + x + 1\right)\left(x^2 - x + 1\right). \tag{7.61}$$

The roots of the first one are $\omega, \omega^2$. The roots of the second one are $-\omega, -\omega^2$. Therefore, the splitting field is $\mathbb{Q}(\omega)$, since all the roots are in $\mathbb{Q}(\omega)$. Furthermore, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ because the minimal polynomial of $\omega$ over $\mathbb{Q}$ is $x^2 + x + 1$.

**Exercise 7.21.** Determine the degrees of the splitting fields of the following polynomials over $\mathbb{Q}$.

(a) $x^4 + 1$.

(b) $x^6 + 1$.

(c) $x^4 - 2$.

(d) $x^6 + x^3 + 1$.

*Solution.* (a) $r = e^{\frac{2\pi i}{4}} = \frac{1+i}{\sqrt{2}}$ is a root of $x^4 + 1$, then the other roots are $ir, -r, -ir$. Then the splitting field is

$$\mathbb{Q}(r, ir, -r, -ir) = \mathbb{Q}(r, i) = \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}, i\right) = \mathbb{Q}\left(\sqrt{2}, i\right). \tag{7.62}$$

Then we have

$$\left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4, \tag{7.63}$$

since $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$, and $x^2 + 1$ is the minimal polynomial of $i$ over $\mathbb{Q}\left(\sqrt{2}\right)$ (since it's a subfield of $\mathbb{R}$, $x^2 + 1$ is irreducible).

(b) $r = e^{\frac{i\pi}{6}}$ is a root of $x^6 + 1$. The other roots are

$$r\zeta^j = e^{i\frac{\pi + 2\pi j}{6}}, \tag{7.64}$$

for $j = 0, 1, \ldots, 5$, where $\zeta = e^{\frac{2\pi i}{6}}$ is 6-th root of unity. We can list the roots:

$$r_1 = \frac{\sqrt{3}}{2} + \frac{1}{2}i, \quad r_2 = i, \quad r_3 = -\frac{\sqrt{3}}{2} + \frac{1}{2}i \tag{7.65}$$

$$r_4 = -\frac{\sqrt{3}}{2} - \frac{1}{2}i, \quad r_5 = -i, \quad r_6 = \frac{\sqrt{3}}{2} - \frac{1}{2}i. \tag{7.66}$$

Therefore, the splitting field is

$$\mathbb{Q}(r_1, \ldots, r_6) = \mathbb{Q}\left(\sqrt{3}, i\right). \tag{7.67}$$

Then we have $\left[\mathbb{Q}\left(\sqrt{3}, i\right)\right] = 4$, as (a).

(c) The roots of $x^4 - 2$ are

$$\sqrt[4]{2}, \quad \sqrt[4]{2}i, \quad -\sqrt[4]{2}, \quad -\sqrt[4]{2}i. \tag{7.68}$$

So the splitting field is

$$\mathbb{Q}\left(\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}, -\sqrt[4]{2}i\right) = \mathbb{Q}\left(\sqrt[4]{2}, i\right). \tag{7.69}$$

Applying tower law,

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\left(\sqrt[4]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 4 \cdot 2 = 8. \tag{7.70}$$

(d) The roots of $y^2 + y + 1$ are $e^{\frac{2\pi i}{3}}$ and $e^{\frac{4\pi i}{3}}$. Therefore, the roots of $x^6 + x^3 + 1$ are the cube-roots of these:

$$e^{\frac{2\pi i}{9}}, \quad e^{\frac{8\pi i}{9}}, \quad e^{\frac{14\pi i}{9}}, \qquad e^{\frac{4\pi i}{9}}, \quad e^{\frac{10\pi i}{9}}, \quad e^{\frac{16\pi i}{9}}. \tag{7.71}$$

Now, $e^{\frac{2\pi i}{9}}$ is a primitive 9-th root of unity, and it generates all the 9-th root of unities (which are the other roots). Therefore, the splitting field is

$$\mathbb{Q}\,(\text{roots}) = \mathbb{Q}\left(e^{\frac{2\pi i}{9}}\right). \tag{7.72}$$

Now, the degree $\left[\mathbb{Q}\left(e^{\frac{2\pi i}{9}}\right) : \mathbb{Q}\right] \leq 6$ since $x^6 + x^3 + 1$ is a polynomial whose root is $e^{\frac{2\pi i}{9}}$. To show that it's irreducible, take $x \to x + 1$,

$$(x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3, \tag{7.73}$$

which is irreducible by Eisenstein. Therefore, $x^6 + x^3 + 1$ is the minimal polynomial of $e^{\frac{2\pi i}{9}}$ over $\mathbb{Q}$. Hence,

$$\left[\mathbb{Q}\left(e^{\frac{2\pi i}{9}}\right) : \mathbb{Q}\right] = 6. \tag{7.74}$$

■

**Exercise 7.22.** Let $p$ be a prime number. Show that the degree of the splitting field of $x^p - 1$ over $\mathbb{Q}$ is $p - 1$.

*Solution.* The roots of $x^p - 1$ are:

$$1, \quad e^{\frac{2\pi i}{p}}, \quad e^{\frac{4\pi i}{p}}, \quad \cdots, \quad e^{\frac{2(p-1)\pi i}{p}}. \tag{7.75}$$

$e^{\frac{2\pi i}{p}}$ is a primitive $p$-th root of unity, which generates the other roots. Therefore, the splitting field is

$$\mathbb{Q}\,(\text{roots}) = \mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right). \tag{7.76}$$

Now, the degree $\left[\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right) : \mathbb{Q}\right] \leq p - 1$ since $\sum_{i=0}^{p-1} x^i = x^{p-1} + \cdots + x + 1$ is a polynomial

whose root is $e^{\frac{2\pi i}{p}}$. To show that it's irreducible, take $x \to x+1$,

$$\sum_{i=0}^{p-1}(x+1)^i = \frac{(x+1)^p - 1}{x} \tag{7.77}$$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1} \tag{7.78}$$

which is irreducible by Eisenstein. Therefore, $\sum_{i=0}^{p-1} x^i$ is the minimal polynomial of $e^{\frac{2\pi i}{p}}$ over $\mathbb{Q}$. Hence,

$$\left[\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right) : \mathbb{Q}\right] = p - 1. \tag{7.79}$$

■

**Exercise 7.23.** Let $f := x^3 + ax + b \in \mathbb{Q}[x]$. Find necessary and sufficient conditions on $a$ and $b$ so that the degree of the splitting field of $f$ over $\mathbb{Q}$ is 3.

*Solution.* Let $\alpha$ be a root of $f(x)$ in its splitting field $K$. Performing polynomial long division of $f(x)$ by $(x-\alpha)$ yields the exact quadratic quotient:

$$Q(x) = \frac{x^3 + ax + b}{x - \alpha} = x^2 + \alpha x + (\alpha^2 + a) \in \mathbb{Q}(\alpha)[x]. \tag{7.80}$$

The remaining two roots of the cubic, $\beta$ and $\gamma$, must be the roots of $Q(x) = 0$. We construct the tower of field extensions:

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta, \gamma) = K. \tag{7.81}$$

By the Tower Law, the total degree of the splitting field is:

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]. \tag{7.82}$$

We claim that $[K : \mathbb{Q}] = 3$ if and only if $f$ is irreducible and $\sqrt{-4a^3 - 27b^2} \in \mathbb{Q}$.

**($\Rightarrow$)** Assume that $[K : \mathbb{Q}] = 3$. First, suppose $f(x)$ is reducible over $\mathbb{Q}$. Because $\deg(f) = 3$, it must factor into either three linear polynomials or one linear and one quadratic polynomial. If it factors into three linear polynomials, all roots lie in $\mathbb{Q}$, meaning $K = \mathbb{Q}$ and $[K : \mathbb{Q}] = 1$. If it factors into a quadratic, adjoining a root produces an extension of degree 2, meaning $[K : \mathbb{Q}] = 2$. Both cases contradict $[K : \mathbb{Q}] = 3$, so $f(x)$ must be irreducible over $\mathbb{Q}$.

Since $f(x)$ is irreducible, the base extension has degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3$. Substituting this into equation (3):

$$3 = [K : \mathbb{Q}(\alpha)] \cdot 3 \implies [K : \mathbb{Q}(\alpha)] = 1. \tag{7.83}$$

This implies that $K = \mathbb{Q}(\alpha)$, meaning the remaining roots $\beta$ and $\gamma$ must already reside inside $\mathbb{Q}(\alpha)$. Consequently, their difference $(\beta - \gamma)$ must also belong to $\mathbb{Q}(\alpha)$.

By applying the standard quadratic formula to $Q(x)$, we find the root difference satisfies:

$$(\beta - \gamma)^2 = B^2 - 4AC = \alpha^2 - 4(\alpha^2 + a) = -3\alpha^2 - 4a. \tag{7.84}$$

Thus, for $\beta, \gamma \in \mathbb{Q}(\alpha)$, the element $-3\alpha^2 - 4a$ must be a perfect square in $\mathbb{Q}(\alpha)$. We express this square as a linear combination of the vector space basis $\{1, \alpha, \alpha^2\}$ over $\mathbb{Q}$:

$$\left(c_0 + c_1\alpha + c_2\alpha^2\right)^2 = -3\alpha^2 - 4a \quad \text{for } c_0, c_1, c_2 \in \mathbb{Q}. \tag{7.85}$$

Expanding the left side and reducing higher powers of $\alpha$ using the relations $\alpha^3 = -a\alpha - b$ and $\alpha^4 = -a\alpha^2 - b\alpha$, we equate the coefficients of $1, \alpha, \alpha^2$ to set up the system:

$$c_0^2 - 2bc_1c_2 = -4a \tag{7.86}$$

$$2c_0c_1 - bc_2^2 - 2ac_1c_2 = 0 \tag{7.87}$$

$$c_1^2 + 2c_0c_2 - ac_2^2 = -3 \tag{7.88}$$

From equation (7.87), we isolate $2c_0 = \frac{bc_2^2}{c_1} + 2ac_2$. Introducing the scaling ratio $k = \frac{c_2}{c_1}$ yields $c_2 = kc_1$ and $c_0 = c_1\left(\frac{bk^2+2ak}{2}\right)$. Substituting these into equation (7.87) gives:

$$c_1^2\left(1 + ak^2 + bk^3\right) = -3 \implies c_1^2 = \frac{-3}{1 + ak^2 + bk^3} \tag{7.89}$$

Substituting our parameterized forms into equation (7.86) and clearing the denominators yields:

$$3b^2k^4 - 4abk^3 - 4a^2k^2 - 24bk - 16a = 0 \tag{7.90}$$

This polynomial possesses the rational root $k = -\frac{2a}{3b}$. Evaluating the denominator under this root gives:

$$1 + ak^2 + bk^3 = 1 + a\left(\frac{4a^2}{9b^2}\right) + b\left(-\frac{8a^3}{27b^3}\right) = \frac{27b^2 + 4a^3}{27b^2} \tag{7.91}$$

Substituting this back into equation (10) isolates $c_1$:

$$c_1^2 = \frac{-3}{\frac{4a^3+27b^2}{27b^2}} = \frac{81b^2}{-4a^3 - 27b^2} = \frac{81b^2}{\Delta} \implies c_1 = \frac{9b}{\sqrt{\Delta}} \tag{7.92}$$

Back-substituting to solve for $c_2$ and $c_0$ yields the full explicit solution:

$$c_0 = \frac{-4a^2}{\sqrt{\Delta}}, \quad c_1 = \frac{9b}{\sqrt{\Delta}}, \quad c_2 = \frac{-6a}{\sqrt{\Delta}} \tag{7.93}$$

For $c_0, c_1, c_2$ to be rational numbers, the scalar factor $\sqrt{\Delta} = \sqrt{-4a^3 - 27b^2}$ must be a rational number. Thus, $\Delta$ must be a perfect square in $\mathbb{Q}$.

**($\Rightarrow$)** Assume $f(x)$ is irreducible over $\mathbb{Q}$ and $\Delta = d^2$ for some $d \in \mathbb{Q}$.

Because $f(x)$ is irreducible, the base step of the tower is $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. We look at the explicit

element constructed from our algebraic solution in equation (7.93):

$$\theta = \frac{1}{d}\left(-4a^2 + 9b\alpha - 6a\alpha^2\right) \tag{7.94}$$

Since $a, b, d \in \mathbb{Q}$ and $\alpha \in \mathbb{Q}(\alpha)$, it follows that $\theta \in \mathbb{Q}(\alpha)$. Squaring $\theta$ yields exactly $-3\alpha^2 - 4a$.

Because $\theta^2 = -3\alpha^2 - 4a$, we know that $\theta$ matches the root difference $(\beta - \gamma)$ up to sign. Therefore, $(\beta - \gamma) \in \mathbb{Q}(\alpha)$. From the quadratic quotient $Q(x)$, Vieta's formulas dictate that the sum of the remaining roots is $(\beta + \gamma) = -\alpha \in \mathbb{Q}(\alpha)$.

We isolate the remaining roots using linear combinations inside the field:

$$\beta = \frac{(\beta+\gamma) + (\beta-\gamma)}{2} \in \mathbb{Q}(\alpha), \quad \gamma = \frac{(\beta+\gamma) - (\beta-\gamma)}{2} \in \mathbb{Q}(\alpha) \tag{7.95}$$

Because all three roots $\alpha, \beta, \gamma$ reside entirely within $\mathbb{Q}(\alpha)$, the splitting field collapses down to the base extension: $K = \mathbb{Q}(\alpha)$. Therefore, the total degree of the splitting field is exactly $[K : \mathbb{Q}] = 3$. ■

**Exercise 7.24.** Let $k$ be a field, and let $K/k$ be a field extension. Let $f \in k[x]$ and let $\varphi$ be an automorphism of $K$ with $\varphi|_k = \mathrm{id}_k$. Show that $\varphi$ maps a zero of $f \in K$ to a zero of $f \in K$.

*Solution.* Suppose $f = \sum_{i=0}^{n} a_i x^i \in k[x]$, and $r \in K$ is a root of $f$. Then

$$0 = \varphi\left(\sum_{i=0}^{n} a_i r^i\right) = \sum_{i=0}^{n} \varphi(a_i)\,\varphi(r)^i = \sum_{i=0}^{n} a_i \varphi(r)^i. \tag{7.96}$$

Therefore, $\varphi(r) \in K$ is a root of $f$. ■

**Exercise 7.25.** Show that $\mathbb{Q}\left(\sqrt[3]{2}\right)$ has no automorphism except for the identity.

*Solution.* Let $\varphi : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(\sqrt[3]{2}\right)$ be an automorphism. Since an automorphism maps 1 to itself, $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. $f = x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$. So $\varphi$ maps $\sqrt[3]{2}$ to one of the roots of $f$ in $\mathbb{Q}\left(\sqrt[3]{2}\right)$ (by Exercise 7.24). But the other roots of $f$ are not real, so we must have that $\sqrt[3]{2} \mapsto \sqrt[3]{2}$.

Let $\alpha = \sqrt[3]{2}$. Then a general element of $\mathbb{Q}(\alpha)$ is $a + b\alpha + c\alpha^2$ for $a, b, c \in \mathbb{Q}$. Since $\varphi$ maps rationals to themselves, and $\alpha$ to itself, it maps $a + b\alpha + c\alpha^2$ to itself. Therefore, $\varphi = \mathrm{id}_{\mathbb{Q}(\alpha)}$. ■

**Exercise 7.26.** Let $f \in \mathbb{R}[x]$. If $\alpha \in \mathbb{C}$ is a zero of $f$, then also the complex conjugate $\overline{\alpha}$.

*Solution.* $\varphi : \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ is a field automorphism, with $\varphi|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$. By Exercise 7.24, it maps a root of $f$ to a root of $f$, i.e. $\overline{\alpha}$ is a root of $f$. ■

**Exercise 7.27.** Let $k$ be a field and let $f \in k[x]$ be irreducible of degree 6. Let $K/k$ be an extension of degree 2. Prove or disprove: Either $f$ is irreducible over $K$ or $f$ is the product of two irreducible polynomials of degree 3 over $K$.

*Solution.* Let $\alpha$ be a root of $f$. Then $f$ (upto scaling) is the minimal polynomial of $\alpha$ over $k$. Consider $[K(\alpha) : k]$, and apply the tower law in two different ways:

$$[K(\alpha) : k] = [K(\alpha) : k(\alpha)]\,[k(\alpha) : k] = [K(\alpha) : k(\alpha)] \cdot 6 \tag{7.97}$$

$$[K(\alpha) : k] = [K(\alpha) : K]\,[K : k] = [K(\alpha) : K] \cdot 2 \leq 12, \tag{7.98}$$

because the degree of the minimal polynomial of $\alpha$ over $K$ has degree at most 6 (since $\deg f = 6$). Therefore, $[K(\alpha) : k]$ is divisible by 6, and at most 12.

**Case 1:** $[K(\alpha) : k] = 12$. Then $[K(\alpha) : K] = 6$. Hence, $f$ is the minimal polynomial of $\alpha$ over $K$. In other words, $f$ is irreducible over $K$.

**Case 2:** $[K(\alpha) : k] = 6$. Then $[K(\alpha) : K] = 3$. Hence, if $g$ is the minimal polynomial of $\alpha$ over $K$, we have $\deg g = 3$.

> **Claim 7.2:** If $g$ is the minimal polynomial of $\alpha$ over $K$, and $f \in K[x]$ with $f(\alpha) = 0$, then $g \mid f$.
>
> *Proof.* By Euclidean algorithm, $f = gq + r$ where $r = 0$ or $\deg r < \deg g$. Suppose $r \neq 0$. Then
>
> $$r(\alpha) = f(\alpha) - g(\alpha)\,q(\alpha) = 0 - 0 = 0. \tag{7.99}$$
>
> But since $g$ is the minimal polynomial of $\alpha$, it's the least-degree polynomial in $K[x]$ with $\alpha$ as a root, and now we have found another polynomial with strictly smaller degree. Hence, $r \neq 0$ is not possible. □

Then $g \mid f$, and $g$ is irreducible with $\deg g = 3$. Now, consider the polynomial $q = f/g$. If $\beta$ is another root of $f$ which is not a root of $g$, then by the similar construction as before, the degree of the minimal polynomial $h$ of $\beta$ over $K$ is 3, and $h \mid f$. In other words, $h = q$. So $f$ is the product of two irreducible degree-3 polynomials. ■

**Exercise 7.28.** Find a primitive element for the extension $\mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right)/\mathbb{Q}$.

*Solution.* Let $\alpha = \sqrt[3]{2}$ and $\omega = e^{\frac{2\pi i}{3}}$. We'll show that $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha + \omega)$. Clearly, $\mathbb{Q}(\alpha, \omega) \supseteq \mathbb{Q}(\alpha + \omega)$.

Suppose $\beta = \alpha + \omega$. We'll first show that $\omega \in \mathbb{Q}(\beta)$.

$$2 = (\beta - \omega)^3 = \beta^3 - 1 - 3\beta^2\omega + 3\beta\omega^2 = \beta^3 - 1 - 3\beta^2\omega + 3\beta(-\omega - 1). \tag{7.100}$$

Rearranging, we get

$$\omega = \frac{\beta^3 - 3\beta - 3}{3\beta(\beta + 1)} \in \mathbb{Q}(\beta). \tag{7.101}$$

Then $\alpha = \beta - \omega \in \mathbb{Q}(\beta)$. Therefore, $\mathbb{Q}(\alpha, \omega) \subseteq \mathbb{Q}(\beta)$. ■

**Exercise 7.29.** Let $k$ be a field of characteristic $p \neq 0$ and let $f \in k[x]$ with $f' = 0$. Show that $f = g(x^p)$ for some polynomial $g \in k[x]$.

*Solution.* Let $f = \sum_{i=0}^{n} a_i x^i$, then $f' = \sum_{i=1}^{n} i a_i x^{i-1}$. $f' = 0$ implies each $ia_i = 0$. This gives either $a_i = 0$ or $i = 0$ in $k$.

We consider the terms $a_i \neq 0$. For those terms, $p \mid i$, and as a result, $f$ is

$$\sum_{i=0}^{d} a_{pi} x^{pi} = \sum_{i=0}^{d} a_{pi} (x^p)^i = g(x^p) \tag{7.102}$$

for $g = \sum_{i=0}^{d} a_{pi} x^i$. ■

**Exercise 7.30.** Let $K/L/k$ be field extensions. Show that if $K$ is normal over $L$ and $L$ is normal over $k$ then $K$ need not be normal over $k$.

*Solution.* Consider

$$k = \mathbb{Q}, \quad L = \mathbb{Q}\left(\sqrt{2}\right), \quad K = \mathbb{Q}\left(\sqrt[4]{2}\right). \tag{7.103}$$

Then $[L : k] = [K : L] = 2$, so these extensions are normal (by Exercise 7.31). But the extension $\mathbb{Q} \leq \mathbb{Q}\left(\sqrt[4]{2}\right)$ is not normal. Because the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $x^4 - 2$ (irreducible by Eisenstein), and it doesn't split over $\mathbb{Q}\left(\sqrt[4]{2}\right)$, as the roots

$$\sqrt[4]{2}, \quad i\sqrt[4]{2}, \quad -\sqrt[4]{2}, \quad -i\sqrt[4]{2} \tag{7.104}$$

are not all in $\mathbb{Q}\left(\sqrt[4]{2}\right)$, because $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is a subfield of $\mathbb{R}$. ■

**Exercise 7.31.** Let $K/k$ be a field extension with $[K : k] = 2$. Show that $K/k$ is normal.

*Solution.* Let $\alpha \in K \setminus k$. Then $\alpha$ is algebraic over $k$, so its minimal polynomial over $k$ has degree 2. In other words, $K = k(\alpha)$.

Let the minimal polynomial of $\alpha$ over $k$ is $f = x^2 + ax + b$. Then the other root $\beta$ is

$$\beta = -a - \alpha \in k(\alpha). \tag{7.105}$$

Therefore, both the roots of $f$ are in $K$, so $K$ is the splitting root of $f$. Hence, the extension $k \leq K$ is normal. ■

**Exercise 7.32.** Let $k$ be a field of characteristic 0. Let $f \in k[x]$. Let $g \in k[x]$ be an irreducible polynomial that divides $f$ and $f'$. Show $g^2$ divides $f$.

*Solution.* Since $g \mid f$,

$$f = g^m h \text{ for some } m \geq 1, \text{ and } g \nmid h. \tag{7.106}$$

Suppose $g^2 \nmid f$, i.e. $m = 1$. Then

$$f' = gh' + g'h. \tag{7.107}$$

Since $g \mid f'$, we have $g \mid g'h$. Since $g$ is irreducible (and hence prime, since $k[x]$ is a PID), $g \mid g'h$ implies $g \mid g'$ (since $g \nmid h$).

But $\deg g > \deg g'$. Furthermore, since $\operatorname{char} k = 0$, the leading term of $g'$ is $na_n \neq 0$ ($n = \deg g$, $a_n \neq 0$ is the leading term of $g$). Since $na_n \neq 0$, $\deg g' = n - 1$, which can't be divisible by $g$. Contradiction! ■

**Exercise 7.33.** For which fields and which primes $p$ does $f = x^p - x$ have a multiple root?

*Solution.* We claim that $x^p - x$ has a multiple root if $\operatorname{char} k =: q \mid p - 1$. If $\operatorname{char} k = p$, then

$$f' = px^{p-1} - 1 = -1, \tag{7.108}$$

which is never 0. So $f$ doesn't have a multiple root in this case. Now, consider the case $\operatorname{char} k = 0$ or $\operatorname{char} k = q \nmid p - 1$. Let $\alpha$ be a root of $f$. Then $\alpha = 0$ or $\alpha^{p-1} = 1$.

$$f'(\alpha) = p\alpha^{p-1} - 1 = \begin{cases} -1 & \text{if } \alpha = 0, \\ p - 1 & \text{otherwise;} \end{cases} \tag{7.109}$$

which is never 0. Now consider the remaining case $\operatorname{char} k = q \mid p - 1$. Then for nonzero roots of $x^p - x$, $f'(\alpha) = p - 1 = 0$ since $q \mid p - 1$. Therefore, every nonzero root is a multiple root of $f$. ■

**Exercise 7.34.** Identify the additive group of $\mathbb{F}_4$.

*Solution.* $\operatorname{char} \mathbb{F}_4 = 2$, so it contains elements $0, 1$ with $1 + 1 = 0$. Let the other elements are $a, b$. Then $a + a = b + b = 0$ since $\operatorname{char} \mathbb{F}_4 = 2$. Then $a + 1 = b$ and $b + 1 = a$. Furthermore, $a + b = a + a + 1 = 1$. So the addition table is

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\boldsymbol{a}$ | $\boldsymbol{b}$ |
|---|---|---|---|---|
| $\mathbf{0}$ | 0 | 1 | $a$ | $b$ |
| $\mathbf{1}$ | 1 | 0 | $b$ | $a$ |
| $\boldsymbol{a}$ | $a$ | $b$ | 0 | 1 |
| $\boldsymbol{b}$ | $b$ | $a$ | 1 | 0 |

This coincides with the addition table of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

| $+$ | $\mathbf{(0,0)}$ | $\mathbf{(0,1)}$ | $\mathbf{(1,0)}$ | $\mathbf{(1,1)}$ |
|---|---|---|---|---|
| $\mathbf{(0,0)}$ | $(0,0)$ | $(0,1)$ | $(1,0)$ | $(1,1)$ |
| $\mathbf{(0,1)}$ | $(0,1)$ | $(0,0)$ | $(1,1)$ | $(1,0)$ |
| $\mathbf{(1,0)}$ | $(1,0)$ | $(1,1)$ | $(0,0)$ | $(0,1)$ |
| $\mathbf{(1,1)}$ | $(1,1)$ | $(1,0)$ | $(0,1)$ | $(0,0)$ |

Therefore, $\mathbb{F}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ as additive groups. ■

**Exercise 7.35.** Determine the number of irreducible polynomials of degree 3 over $\mathbb{F}_2$.

*Solution.* By (6.65), the number of irreducible polynomials of degree 3 over $\mathbb{F}_2$ is

$$\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d = \frac{1}{3}\left[\mu(3)\,2 + \mu(1)\,2^3\right] = \frac{1}{3}\left[-2+8\right] = 2. \tag{7.110}$$

■

**Exercise 7.36.** Determine all polynomials $f \in \mathbb{F}_q[x]$ such that $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$.

*Solution.* $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$ if and only if

$$\prod_{\alpha\in\mathbb{F}_q}(x-\alpha) \mid f. \tag{7.111}$$

Now, we claim that

$$\prod_{\alpha\in\mathbb{F}_q}(x-\alpha) = x^q - x. \tag{7.112}$$

For $\alpha \in \mathbb{F}_q$, if $\alpha = 0$, then clearly it's a root of $x^q - x = x\left(x^{q-1}-1\right)$. If $\alpha \neq 0$, then $\alpha^{q-1} = 1$ since $\mathbb{F}_q^\times$ is a finite group. Therefore, $\prod_{\alpha\in\mathbb{F}_q}(x-\alpha) \mid x^q - x$. Since the degrees are the same and the leading coefficients are the same, we can say that $\prod_{\alpha\in\mathbb{F}_q}(x-\alpha) = x^q - x$. Therefore, $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$ if and only if $x^q - x \mid f$. ■

**Exercise 7.37.** Prove that every element in $\mathbb{F}_p$ has exactly one $p$-th root.

*Solution.* Since $a^p = a$, we always have that $a$ is its own $p$-th root. Now, if $b$ is another $p$-th root of $a$, then $b^p = a = a^p$, which gives us

$$a = b^p = b, \tag{7.113}$$

by Fermat's little theorem. Therefore, $a$ is its unique $p$-th root in $\mathbb{F}_p$. ■

**Exercise 7.38.** Give an example of a simple algebraic extension $K/k$, such that $\mathrm{Gal}(K/k) = \{1\}$, but $K \neq k$.

*Solution.* $\mathbb{Q} \leq \mathbb{Q}\left(\sqrt[3]{2}\right)$ is a simple algebraic extension. But the only field automorphism $\mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(\sqrt[3]{2}\right)$ is identity (Exercise 7.25). ■

**Exercise 7.39.** Find the Galois group of $x^3 - 2x + 4$ over $\mathbb{Q}$.

*Solution.* The roots of $x^3 - 2x + 4$ are

$$-2, \quad 1+i, \quad 1-i. \tag{7.114}$$

Therefore, the splitting field is $\mathbb{Q}(i)$. This is a Galois extension of degree 2. So $|\mathrm{Gal}(\mathbb{Q}(i) : \mathbb{Q})| = 2$. There is only one group of order 2, namely $\mathbb{Z}_2$. So $\mathrm{Gal}(\mathbb{Q}(i) : \mathbb{Q}) \cong \mathbb{Z}_2$.

The elements of $\mathrm{Gal}(\mathbb{Q}(i) : \mathbb{Q})$ are id and $i \mapsto -i$ (i.e. complex conjugation). ■

**Exercise 7.40.** Determine the Galois group of $x^4 - 5$ over $\mathbb{Q}$. Determine the diagram of all subgroups and the diagram of all intermediate fields.

*Solution.* The roots are $\pm\sqrt[4]{5}, \pm i\sqrt[4]{5}$. So the splitting field is

$$K := \mathbb{Q}\left(\pm\sqrt[4]{5}, \pm i\sqrt[4]{5}\right) = \mathbb{Q}\left(\sqrt[4]{5}, i\right). \tag{7.115}$$

The degree of this extension is

$$[K : \mathbb{Q}] = \left[\mathbb{Q}\left(\sqrt[4]{5}, i\right) : \mathbb{Q}\left(\sqrt[4]{5}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{5}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8. \tag{7.116}$$

So the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ will have order 8. Consider the field automorphisms $K \to K$

$$\sigma : \sqrt[4]{5} \mapsto i\sqrt[4]{5}, \quad i \mapsto i, \tag{7.117}$$

$$\tau : \sqrt[4]{5} \mapsto \sqrt[4]{5}, \quad i \mapsto -i. \tag{7.118}$$

Then $\mathrm{ord}\,\sigma = 4$ and $\mathrm{ord}\,\tau = 2$. Furthermore,

$$\tau\sigma\tau(i) = \tau\sigma(-i) = \tau(-i) = i\sigma^{-1}(i); \tag{7.119}$$

$$\tau\sigma\tau\left(\sqrt[4]{5}\right) = \tau\sigma\left(\sqrt[4]{5}\right) = \tau\left(i\sqrt[4]{5}\right) = -i\sqrt[4]{5} = \sigma^{-1}\left(\sqrt[4]{5}\right). \tag{7.120}$$

Therefore, we have $\tau\sigma\tau = \sigma^{-1}$, so $\langle\sigma, \tau\rangle$ is isomorphic to $D_4$, which has order 8. But we already know that $\mathrm{Gal}(K/\mathbb{Q})$ has order 8. Hence,

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma, \tau\rangle \cong D_4. \tag{7.121}$$

Now, the subgroups $H$ of $\langle\sigma, \tau\rangle \cong D_4$ are:

- $|H| = 1$: so $H = \{\mathrm{id}_K\}$, and hence $\mathrm{Fix}\, H = K$.
- $|H| = 2$: the only elements of order 2 (aka, involutions) are $\sigma^j\tau$ and $\sigma^2$.
  - $H = \langle\sigma^2\rangle$. Then $\sigma^2$ fixes $i$ and $\sqrt{5}$. So $\mathrm{Fix}\, H \supseteq \mathbb{Q}(\sqrt{5}, i)$. Since $[\mathrm{Fix}\, H : \mathbb{Q}] = [G : H] = 4$, and $\left[\mathbb{Q}\left(\sqrt{5}, i\right) : \mathbb{Q}\right] = 4$, we have that $\mathrm{Fix}\, H = \mathbb{Q}\left(\sqrt{5}, i\right)$.
  - $H = \langle\tau\rangle$. Then $\tau$ fixes $\sqrt[4]{5}$, so $\mathrm{Fix}\, H \supseteq \mathbb{Q}\left(\sqrt[4]{5}\right)$. Since $\left[\mathbb{Q}\left(\sqrt[4]{5}\right) : \mathbb{Q}\right] = 4 = [\mathrm{Fix}\, H : \mathbb{Q}]$, we have $\mathrm{Fix}\, H = \mathbb{Q}\left(\sqrt[4]{5}\right)$.

- $H = \langle \sigma^2\tau \rangle$. One can check that $\sigma^2\tau$ fixes $i\sqrt[4]{5}$, as

$$\sigma^2\tau\left(i\sqrt[4]{5}\right) = \sigma^2\left(-i\sqrt[4]{5}\right) = -i\sigma^2\left(\sqrt[4]{5}\right) = -i\left(-\sqrt[4]{5}\right) = i\sqrt[4]{5}. \tag{7.122}$$

  So $\operatorname{Fix} H \supseteq \mathbb{Q}\left(i\sqrt[4]{5}\right)$. Since $\left[\mathbb{Q}\left(i\sqrt[4]{5}\right) : \mathbb{Q}\right] = 4$ (as $i\sqrt[4]{5}$ is a root of the irreducible polynomial $x^4 - 5 \in \mathbb{Q}[x]$), we have $\operatorname{Fix} H = \mathbb{Q}\left(i\sqrt[4]{5}\right)$.

- $H = \langle \sigma\tau \rangle$. After acting $\sigma\tau$ on the basis elements, we find that $\sigma\tau$ fixes $(1+i)\sqrt[4]{5}$, as

$$\sigma\tau\left((1+i)\sqrt[4]{5}\right) = \sigma\left((1-i)\sqrt[4]{5}\right) = (1-i)i\sqrt[4]{5} = (1+i)\sqrt[4]{5}. \tag{7.123}$$

  So $\operatorname{Fix} H \supseteq \mathbb{Q}\left((1+i)\sqrt[4]{5}\right)$. Since $\left[\mathbb{Q}\left((1+i)\sqrt[4]{5}\right) : \mathbb{Q}\right] = 4$ (as $(1+i)\sqrt[4]{5}$ is a root of the irreducible polynomial $x^4 + 20 \in \mathbb{Q}[x]$), we have $\operatorname{Fix} H = \mathbb{Q}\left((1+i)\sqrt[4]{5}\right)$.

- $H = \langle \sigma^3\tau \rangle$. After acting $\sigma\tau$ on the basis elements, we find that $\sigma\tau$ fixes $(1-i)\sqrt[4]{5}$, as

$$\sigma^3\tau\left((1-i)\sqrt[4]{5}\right) = \sigma^3\left((1+i)\sqrt[4]{5}\right) = -(1+i)i\sqrt[4]{5} = (1-i)\sqrt[4]{5}. \tag{7.124}$$

  So $\operatorname{Fix} H \supseteq \mathbb{Q}\left((1-i)\sqrt[4]{5}\right)$. Since $\left[\mathbb{Q}\left((1-i)\sqrt[4]{5}\right) : \mathbb{Q}\right] = 4$ (as $(1-i)\sqrt[4]{5}$ is a root of the irreducible polynomial $x^4 + 20 \in \mathbb{Q}[x]$), we have $\operatorname{Fix} H = \mathbb{Q}\left((1-i)\sqrt[4]{5}\right)$.

- $|H| = 4$: either $H$ is $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. In the latter case, it must be $\langle \sigma^2, \tau \rangle = \{\mathrm{id}, \sigma^2, \tau, \sigma^2\tau\}$ or $\langle \sigma^2, \sigma\tau \rangle = \{\mathrm{id}, \sigma^2, \sigma\tau, \sigma^3\tau\}$.

  - $H = \langle \sigma \rangle$. Then $\sigma$ fixes $i$, so $\operatorname{Fix} H \supseteq \mathbb{Q}(i)$. Since $[\operatorname{Fix} H : \mathbb{Q}] = [G : H] = 2$, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, we have that $\operatorname{Fix} H = \mathbb{Q}(i)$.

  - $H = \langle \sigma^2, \tau \rangle = \{\mathrm{id}, \sigma^2, \tau, \sigma^2\tau\}$. We can check that both $\sigma^2$ and $\tau$ fix $\sqrt{5}$, so $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\sqrt{5}\right)$. Since $\left[\mathbb{Q}\left(\sqrt{5}\right) : \mathbb{Q}\right] = 2 = [\operatorname{Fix} H : \mathbb{Q}]$, we have $\operatorname{Fix} H = \mathbb{Q}\left(\sqrt{5}\right)$.

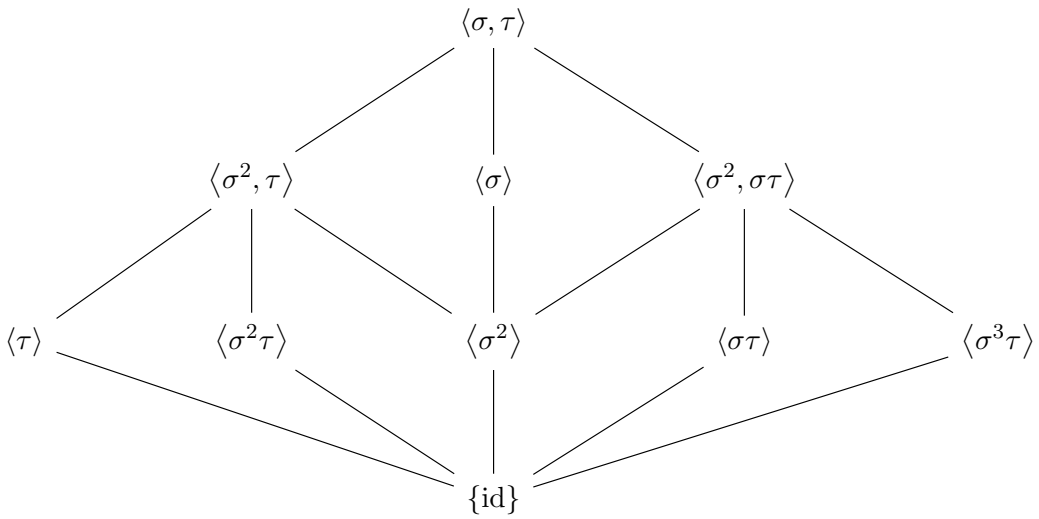
  - $H = \langle \sigma^2, \sigma\tau \rangle = \{\mathrm{id}, \sigma^2, \sigma\tau, \sigma^3\tau\}$. We can check that both $\sigma^2$ and $\sigma\tau$ fix $i\sqrt{5}$, as

$$\sigma\tau\left(i\sqrt{5}\right) = \sigma\left(-i\sqrt{5}\right) = \sigma\left(-i\sqrt[4]{5}\sqrt[4]{5}\right) = -i\ i\sqrt[4]{5}\ i\sqrt[4]{5} = i\sqrt{5}. \tag{7.125}$$

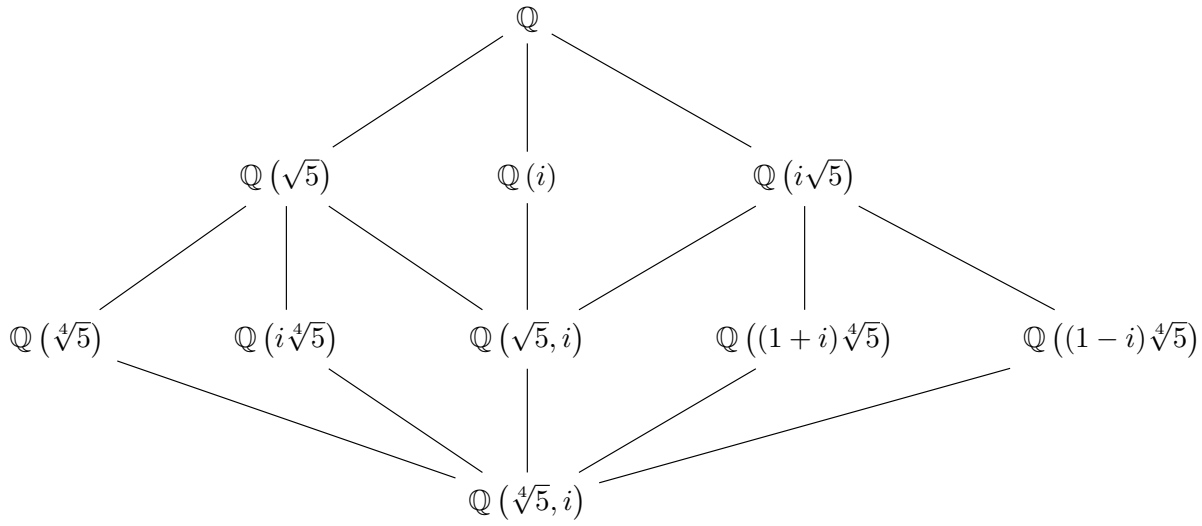
    So $\operatorname{Fix} H \supseteq \mathbb{Q}\left(i\sqrt{5}\right)$. Since $\left[\mathbb{Q}\left(i\sqrt{5}\right) : \mathbb{Q}\right] = 2 = [\operatorname{Fix} H : \mathbb{Q}]$, we have $\operatorname{Fix} H = \mathbb{Q}\left(i\sqrt{5}\right)$.

- $|H| = 8$: so $H = \langle \sigma, \tau \rangle$, and hence $\operatorname{Fix} H = \mathbb{Q}$.

The subgroup lattice is: (top is larger, bottom is smaller)




And the field lattice is: (top is smaller, bottom is larger)




■

**Exercise 7.41.** (a) Let $a \in \mathbb{Z}$. Prove that $x^3 + ax - 1$ is irreducible in $\mathbb{Q}[x]$ if and only if $a \neq 0$ and $a \neq -2$.

(b) Let $s$ be a zero of $x^3 - 3x - 1$ in $\mathbb{C}$. Show that $-(1+s)^{-1}$ is also a zero of $x^3 - 3x - 1$.

(c) Let $s$ as in part (b). Show that $\mathbb{Q}(s)/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

*Solution.* (a) $f(x) = x^3 + ax - 1$ is irreducible in $\mathbb{Q}[x]$ if and only if it doesn't have a rational root if and only if it doesn't have any integer root if and only if $\pm 1$ are not roots of $f$.

$$f(1) = a \text{ and } f(-1) = -2 - a. \tag{7.126}$$

So $\pm 1$ are not roots of $f$ if and only if $a \neq 0$ and $a \neq -2$.

(b) Let $f(x) = x^3 - 3x - 1$, which is irreducible by (a). Then

$$f\left(-\frac{1}{1+s}\right) = \left(-\frac{1}{1+s}\right)^3 + 3\left(\frac{1}{1+s}\right) - 1 = \frac{-1+3\left(1+s^2\right)-(1+s)^3}{(1+s)^3}. \tag{7.127}$$

The numerator is

$$-1+3\left(1+s^2\right)-(1+s)^3 = -1+3+3s^2+6s-1-s^3-3s-3s^2 \tag{7.128}$$

$$= -s^3+3s+1 = -f(s) = 0. \tag{7.129}$$

So $-\frac{1}{1+s}$ is also a root of $f$.

(c) By (b), $-\frac{1}{1+s} \in \mathbb{Q}(s)$. The sum of the three roots is 0, so the other root is also in $\mathbb{Q}(s)$. Hence, $\mathbb{Q}(s)$ is the splitting field of $f(x) = x^3 - 3x - 1$. Since $f$ is normal and separable, $\mathbb{Q} \leq \mathbb{Q}(s)$ is a Galois extension (by Exercise 8.4).

Since it's Galois, $|\mathrm{Gal}\left(\mathbb{Q}(s)/\mathbb{Q}\right)| = [\mathbb{Q}(s) : \mathbb{Q}] = 3$. The only group (upto isomorphism) of order 3 is $\mathbb{Z}_3$, so $\mathrm{Gal}\left(\mathbb{Q}(s)/\mathbb{Q}\right) \cong \mathbb{Z}_3$.

■

**Exercise 7.42.** Determine the minimal polynomial for $i + \sqrt{2}$ over $\mathbb{Q}$.

*Solution.* Let $\alpha = i + \sqrt{2}$. Then

$$\alpha - i = \sqrt{2} \implies 2 = (\alpha - i)^2 = \alpha^2 - 1 - 2\alpha i \tag{7.130}$$

$$\implies -4\alpha^2 = (2\alpha i)^2 = \left(\alpha^2 - 3\right)^2 = \alpha^4 + 9 - 6\alpha^2 \tag{7.131}$$

$$\implies \alpha^4 - 2\alpha^2 + 9 = 0. \tag{7.132}$$

So $\alpha$ is a root of the degree-4 polynomial $x^4 - 2x^2 + 9$. Furthermore, one can check that

$$\mathbb{Q}(\alpha) = \mathbb{Q}\left(i, \sqrt{2}\right). \tag{7.133}$$

$\subseteq$ is obvious. We'll show that $i \in \mathbb{Q}(\alpha)$. Consider

$$\alpha^2 = 1 + 2\sqrt{2}i \implies \alpha^2 - 1 = 2\sqrt{2}i \implies \alpha^3 - \alpha = 2\sqrt{2}i\left(\sqrt{2} + i\right) = 4i - 2\sqrt{2}. \tag{7.134}$$

Then $\alpha^3 + \alpha$ is

$$\alpha^3 - \alpha + \alpha = \left(4i - 2\sqrt{2}\right) + \left(2\sqrt{2} + 2i\right) = 6i. \tag{7.135}$$

So $i \in \mathbb{Q}(\alpha)$, and thus, $\sqrt{2} \in \mathbb{Q}(\alpha)$, and as a result, $\mathbb{Q}\left(i, \sqrt{2}\right) \subseteq \mathbb{Q}(\alpha)$. Then,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4. \tag{7.136}$$

So the minimal polynomial of $\alpha$ over $\mathbb{Q}$ will have degree-4. Hence, the monic polynomial that we found earlier, $x^4 - 2x^2 + 9$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$. ■

**Exercise 7.43.** Determine the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$.

*Solution.* $K := \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ is the splitting field of $\left(x^2-2\right)\left(x^2-3\right)$, so it's a Galois extension (by Exercise 8.4). By Exercise 7.7, $\left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\right]=4$. So $\left|\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)\right|=4$. Now, consider the field automorphisms $K\to K$

$$\sigma_1:\sqrt{2}\mapsto-\sqrt{2},\quad \sqrt{3}\mapsto\sqrt{3}; \tag{7.137}$$

$$\sigma_2:\sqrt{2}\mapsto\sqrt{2},\quad \sqrt{3}\mapsto-\sqrt{3}. \tag{7.138}$$

They also commute, so they generate a subgroup of order 4. But since $\left|\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)\right|=4$, we have that $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)$ consists of all these elements, i.e.

$$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)=\left\{\mathrm{id},\sigma_1,\sigma_2,\sigma_1\sigma_2\right\}. \tag{7.139}$$

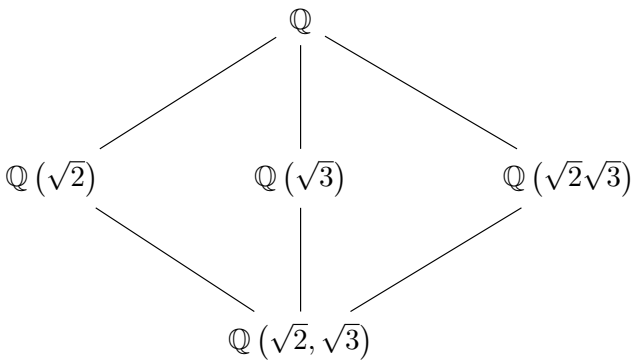
Its subgroups are:

- $H=\{\mathrm{id}\}$. Then $\mathrm{Fix}\,H=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$.
- $|H|=2$.
  - $H=\{\mathrm{id},\sigma_1\}$. Since $\sigma_1$ fixes $\sqrt{3}$, we have that $\mathrm{Fix}\,H\supseteq\mathbb{Q}\left(\sqrt{3}\right)$. The index of $H$ is 2, so $[\mathrm{Fix}\,H:\mathbb{Q}]=2=\left[\mathbb{Q}\left(\sqrt{3}\right):\mathbb{Q}\right]$, so $\mathrm{Fix}\,H=\mathbb{Q}\left(\sqrt{3}\right)$.
  - $H=\{\mathrm{id},\sigma_2\}$. Since $\sigma_2$ fixes $\sqrt{2}$, we have that $\mathrm{Fix}\,H\supseteq\mathbb{Q}\left(\sqrt{3}\right)$. The index of $H$ is 2, so $[\mathrm{Fix}\,H:\mathbb{Q}]=2=\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]$, so $\mathrm{Fix}\,H=\mathbb{Q}\left(\sqrt{2}\right)$.
  - $H=\{\mathrm{id},\sigma_1\sigma_2\}$. Since $\sigma_1\sigma_2$ fixes $\sqrt{6}$, as

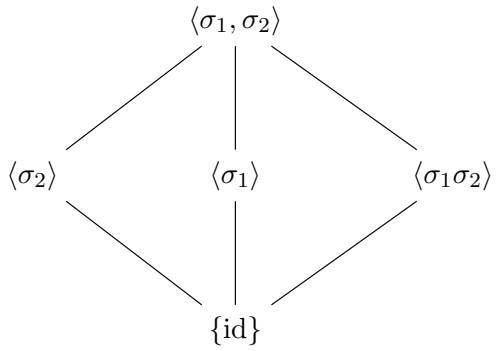
    $$\sigma_1\sigma_2\left(\sqrt{6}\right)=\sigma_1\sigma_2\left(\sqrt{2}\sqrt{3}\right)=\sigma_1\left(-\sqrt{2}\sqrt{3}\right)=\sqrt{2}\sqrt{3}=\sqrt{6}, \tag{7.140}$$

    so we have that $\mathrm{Fix}\,H\supseteq\mathbb{Q}\left(\sqrt{3}\right)$. The index of $H$ is 2, so $[\mathrm{Fix}\,H:\mathbb{Q}]=2=\left[\mathbb{Q}\left(\sqrt{6}\right):\mathbb{Q}\right]$, so $\mathrm{Fix}\,H=\mathbb{Q}\left(\sqrt{6}\right)$.
- $H=\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)$. Then $\mathrm{Fix}\,H=\mathbb{Q}$.

Therefore, the intermediate fields are (top is small, bottom is large)




corresponding to the subgroup lattice (top is large, bottom is small)




■

**Exercise 7.44.** Let $\sqrt[4]{2}$ be the positive real fourth root of 2. Factor the polynomial $x^4-2$ into irreducible factors over each of the fields $\mathbb{Q}$, $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}\left(\sqrt{2},i\right)$, $\mathbb{Q}\left(\sqrt[4]{2}\right)$, $\mathbb{Q}\left(\sqrt[4]{2},i\right)$.

*Solution.* Over $\mathbb{Q}$, it's irreducible by Eisenstein. Over $\mathbb{Q}\left(\sqrt{2}\right)$, we can factorize it

$$x^4-2=\left(x^2-\sqrt{2}\right)\left(x^2+\sqrt{2}\right). \tag{7.141}$$

This cannot be factorized further, because the roots of the factors $\pm\sqrt[4]{2},\pm i\sqrt[4]{2}$ are not in $\mathbb{Q}\left(\sqrt{2}\right)$. Over $\mathbb{Q}\left(\sqrt{2},i\right)$, the factorization remains the same.

Over $\mathbb{Q}\left(\sqrt[4]{2}\right)$,we can factorize it

$$x^4-2=\left(x-\sqrt[4]{2}\right)\left(x+\sqrt[4]{2}\right)\left(x^2+\sqrt{2}\right). \tag{7.142}$$

This cannot be factorized further, because the roots of the quadratic factors $\pm i\sqrt[4]{2}$ are not in $\mathbb{Q}\left(\sqrt[4]{2}\right)$.

$\mathbb{Q}\left(\sqrt[4]{2},i\right)$ is the splitting field of $x^4-2$, as shown in Exercise 7.40 (although it was for $x^4-5$, but all the arguments work by replacing 5 with 2). So it splits into linear factors:

$$x^4-2=\left(x-\sqrt[4]{2}\right)\left(x-i\sqrt[4]{2}\right)\left(x+\sqrt[4]{2}\right)\left(x+i\sqrt[4]{2}\right). \tag{7.143}$$

■

**Exercise 7.45.** Let $k$ be a field, let $K:=k(\alpha)$ be a field extension of $k$ with $\alpha^2=a\in k$. Determine all elements of $K$ whose squares are in $k$.

*Solution.* Given any $\beta\in k(\alpha)$, we can write it as $\beta=x+y\alpha$ for $x,y\in k$. Then

$$\beta^2=(x+y\alpha)^2=x^2+y^2\alpha^2+2xy\alpha. \tag{7.144}$$

$x^2+y^2\alpha^2\in k$. So $\beta^2\in k$ if and only if $2xy\alpha\in k$.

- if $\operatorname{char}k=2$, $2xy\alpha=0\in k$, so all $\beta^2\in k$.

- if $\operatorname{char} k \neq 2$, $\alpha \in k$, $2xy\alpha \in k$, so all $\beta^2 \in k$.
- if $\operatorname{char} k \neq 2$, $\alpha \notin k$, $2xy\alpha \in k$ can happen if and only if either $x = 0$ or $y = 0$, i.e. $\beta \in k$ or $\beta = y\alpha$ for $y \in k$.

■

**Exercise 7.46.** Let $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)$. Determine $[K : \mathbb{Q}]$, prove that $K/\mathbb{Q}$ is a Galois extension and determine its Galois group.

*Solution.* We know that $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 4$ (by Exercise 7.7). Now, one can check that $\sqrt{5} \notin \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Assume the contrary, then

$$\sqrt{5} = x + y\sqrt{3} \text{ for some } x, y \in \mathbb{Q}\left(\sqrt{2}\right). \tag{7.145}$$

By Exercise 7.45, $x = 0$ or $y = 0$. If $y = 0$, we have that $\sqrt{5} \in \mathbb{Q}\left(\sqrt{2}\right)$, which is a contradiction to Exercise 7.7! If $x = 0$, then

$$\sqrt{5} = y\sqrt{3} \implies 5 = 3y^2 \implies y^2 \in \mathbb{Q}. \tag{7.146}$$

But $y = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. By Exercise 7.45, we have $b = 0$ (in which case $y \in \mathbb{Q}$, i.e. $\sqrt{5} \in \mathbb{Q}\left(\sqrt{3}\right)$) or $a = 0$ (in which case we get $\sqrt{5} = b\sqrt{6}$ for some $b \in \mathbb{Q}$), both of which lead to contradiction! Therefore, $\sqrt{5} \notin \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Hence,

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right) : \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)\right] \left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8. \tag{7.147}$$

$K$ is the splitting field of $\left(x^2 - 2\right)\left(x^2 - 3\right)\left(x^2 - 5\right)$, so it's a Galois extension (by Exercise 8.4), and

$$|\operatorname{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 8. \tag{7.148}$$

Now, consider the field automorphisms $K \to K$

$$\sigma_1 : \sqrt{2} \mapsto -\sqrt{2}, \quad \sqrt{3} \mapsto \sqrt{3}, \quad \sqrt{5} \mapsto \sqrt{5}; \tag{7.149}$$

$$\sigma_2 : \sqrt{2} \mapsto \sqrt{2}, \quad \sqrt{3} \mapsto -\sqrt{3}, \quad \sqrt{5} \mapsto \sqrt{5}; \tag{7.150}$$

$$\sigma_3 : \sqrt{2} \mapsto \sqrt{2}, \quad \sqrt{3} \mapsto \sqrt{3}, \quad \sqrt{5} \mapsto -\sqrt{5}. \tag{7.151}$$

Each of them have order 2, and they commute, so they generate a subgroup of order 8, which is isomorphic to $\mathbb{Z}_2^3$. But since $|\operatorname{Gal}(K/\mathbb{Q})| = 8$, these are all the elements of the Galois group.

$$\operatorname{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2, \sigma_2\sigma_3, \sigma_3\sigma_1, \sigma_1\sigma_2\sigma_3\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2. \tag{7.152}$$

■

**Exercise 7.47.** Prove or disprove: Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 3, with one real 0. The other roots are a pair $\beta, \overline{\beta}$ of complex conjugates, so that $L = \mathbb{Q}(\beta)$ has an automorphism, which exchanges $\beta$ and $\overline{\beta}$.

*Solution.* Assume WLOG $f$ is monic. We claim that $\overline{\beta} \notin \mathbb{Q}(\beta)$. If $\overline{\beta} \in \mathbb{Q}(\beta)$, then the real root $\alpha$ is also in $\mathbb{Q}(\beta)$, since

$$\alpha + \beta + \overline{\beta} = -\left(\text{coefficient of } x^2 \text{ in } f\right) \in \mathbb{Q}. \tag{7.153}$$

Then $\mathbb{Q}(\beta)$ is the splitting field of $f$ since it's generated by the roots of $f$. Also,

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = 3, \tag{7.154}$$

since $f$ (irreducible, by hypothesis) is the minimal polynomial of $\beta$ over $\mathbb{Q}$.

**Claim 7.3:** If $f \in \mathbb{Q}[x]$ is an irreducible monic cubic with exactly one real root, and $K$ is the splitting field of $f$, then $[K : \mathbb{Q}] = 6$.

*Proof.* Let $\alpha$ be the real root, and $\beta, \overline{\beta}$ be the other roots. Then the splitting field is $\mathbb{Q}\left(\alpha, \beta, \overline{\beta}\right) = \mathbb{Q}(\alpha, \beta)$. It's easy to see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, since $f$ (irreducible, by hypothesis) is the minimal polynomial of $\alpha$ over $\mathbb{Q}$. Now, over $\mathbb{Q}(\alpha)$, we can factorize $f$ in $\mathbb{Q}(\alpha)$:

$$f(x) = (x - \alpha)\, g(x). \tag{7.155}$$

Then $g(x)$ is the minimal polynomial of $\beta$ over $\mathbb{Q}(\alpha)$. Indeed, since $\mathbb{Q}(\alpha) \leq \mathbb{R}$, $\beta \notin \mathbb{Q}(\alpha)$, and hence the minimal polynomial of $\beta$ has degree at least 2, and $g$ is a degree-2 polynomial with root $\beta$. Hence, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$. So

$$[K : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]\, [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6. \tag{7.156}$$

□

If $\overline{\beta} \in \mathbb{Q}(\beta)$, then $\mathbb{Q}(\beta)$ is the splitting field of $f$, which must have extension degree (over $\mathbb{Q}$) 6 by Claim 7.3. But $\mathbb{Q}(\beta)$ has extension degree 3. So $\overline{\beta} \notin \mathbb{Q}(\beta)$, so there's no automorphism $\mathbb{Q}(\beta) \to \mathbb{Q}(\beta)$ that exchanges $\beta$ and $\overline{\beta}$. ■

**Exercise 7.48.** Let $K/k$ be a Galois extension. Let $f \in k[x]$ be an irreducible polynomial. Show: All irreducible factors of $f$ in $K[x]$ have the same degree.

*Solution.* WLOG $f$ is monic. Let

$$f = \prod_{j=1}^{n} g_j, \qquad \text{where } g_j \in K[x] \text{ are monic irreducible.} \tag{7.157}$$

Let $\varphi \in \mathrm{Gal}(K/k)$. Then $\varphi_* : K[x] \to K[x]$ maps each coefficient under $\varphi$. Since $\varphi$ fixes $k$, $\varphi_*(f) = f$. As a result,

$$f = \prod_{j=1}^{n} \varphi_*(g_j). \tag{7.158}$$

Now, $\varphi_* g_j$ also has to be irreducible, since $\varphi_* g_j = PQ$ implies

$$g_j = \left(\varphi^{-1}\right)_* P \ \left(\varphi^{-1}\right)_* Q, \tag{7.159}$$

and since $g_j$ is monic irreducible, it must be the case that either $P$ or $Q$ has degree 0. That would mean $\varphi_* g_j$ is irreducible.

Fix some $g$ among the $g_j$'s, and consider the $\operatorname{Orb} g$ under the action of $\varphi_*$'s, and consider their product:

$$P := \prod_{h \in \operatorname{Orb} g} h. \tag{7.160}$$

Each $h$ is an irreducible factor of $f$, so $P \mid f$. Also, for every $\varphi \in \operatorname{Gal}(K/k)$, $\varphi_*$ permutes the $h$'s, so

$$\varphi_* P = P, \tag{7.161}$$

so that all the coefficients of $P$ are in $\operatorname{Fix} \operatorname{Gal}(K/k) = k$. Hence, $P \in k[x]$ divides $f$, so $f = P$.

Therefore, $\operatorname{Orb} g$ are all the irreducible factors of $f$. Furthermore, each $h \in \operatorname{Orb} g$ has the same degree as $g$. Hence, all the irreducible factors of $f$ have the same degree! ■

**Exercise 7.49.** Let $f := x^4 + x^3 + x^2 + x + 1$, $\omega = e^{2\pi i/5}$. Put $K := \mathbb{Q}(\omega)$.

(a) Using the Eisenstein criterion show that $f$ is irreducible over $\mathbb{Q}$ and thus $[K : \mathbb{Q}] = 4$.

(b) Show that $K/\mathbb{Q}$ is a Galois extension.

(c) Show that an element of $\operatorname{Gal}(K/\mathbb{Q})$ is determined by its value on $\omega$.

(d) Show that $\operatorname{Gal}(K/\mathbb{Q})$ is a cyclic group of 4 elements.

(e) Determine all the intermediate fields of $K/\mathbb{Q}$.

*Solution.* (a) Exercise 7.22.

(b) $K$ has all the roots of $x^5 - 1$, which are $1, \omega, \omega^2, \omega^3, \omega^4$, so the splitting field of the separable polynomial $x^5 - 1$ is

$$\mathbb{Q}\left(\omega, \omega^2, \omega^3, \omega^4\right) = \mathbb{Q}(\omega) = K. \tag{7.162}$$

Therefore, by Exercise 8.4, $\mathbb{Q} \leq K$ is Galois.

(c) A basis for $K$ over $\mathbb{Q}$ is

$$1, \omega, \omega^2, \omega^3. \tag{7.163}$$

So any automorphism $K \to K$ is determined by its value on $\omega$.

(d) For each $j \in \mathbb{Z}_5^\times$, we define an automorphism $K \to K$

$$\sigma_j : \omega \mapsto \omega^j. \tag{7.164}$$

Since $[K:\mathbb{Q}]=4$, $|\mathrm{Gal}\,(K/Q)|=4$, and we have found 4 elements, so

$$\mathrm{Gal}\,(K/Q)=\{\sigma_1=\mathrm{id},\sigma_2,\sigma_3,\sigma_4\}\,, \tag{7.165}$$

which is isomorphic to $\mathbb{Z}_5^\times\cong\mathbb{Z}_4$ since 2 generates the multiplicative group mod 5.

(e) The subgroups of $\mathrm{Gal}\,(K/Q)$ are:

- $H=\{\mathrm{id}\}$. Then $\mathrm{Fix}\,H=K$.
- $H=\{\sigma_1,\sigma_4\}$. Then $H$ fixes $\omega+\frac{1}{\omega}$. So $\mathrm{Fix}\,H\supseteq\mathbb{Q}\left(\omega+\frac{1}{\omega}\right)$. Now,

$$\omega+\frac{1}{\omega}=2\cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{2}. \tag{7.166}$$

  So $\mathbb{Q}\left(\omega+\frac{1}{\omega}\right)=\mathbb{Q}\left(\sqrt{5}\right)$. Then we have

$$\left[\mathbb{Q}\left(\sqrt{5}\right):\mathbb{Q}\right]=2=[G:H]=[\mathrm{Fix}\,H:\mathbb{Q}]\,, \tag{7.167}$$

  so $\mathrm{Fix}\,H=\mathbb{Q}\left(\sqrt{5}\right)$.
- $H=\mathrm{Gal}\,(K/Q)$. Then $\mathrm{Fix}\,H=\mathbb{Q}$.

Therefore, the subgroup lattice (where top is larger and bottom is smaller) and the subfield lattice (where top is smaller and bottom is larger) are

$$\begin{array}{ccc}
\{\sigma_1=\mathrm{id},\sigma_2,\sigma_3,\sigma_4\} & & \mathbb{Q} \\
\Big| & & \Big| \\
\{\sigma_1,\sigma_4\} & & \mathbb{Q}\left(\sqrt{5}\right) \\
\Big| & & \Big| \\
\{\mathrm{id}\} & & \mathbb{Q}\left(\omega\right)
\end{array}$$

So the only intermediate field in the extension $\mathbb{Q}\leq\mathbb{Q}\left(\omega\right)$ is $\mathbb{Q}\left(\sqrt{5}\right)$.

■

**Exercise 7.50.** Let $f=x^n-1\in\mathbb{Q}\left[x\right]$. Show that the Galois group of $f$ over $\mathbb{Q}$ is abelian.

*Solution.* Let $\zeta=e^{\frac{2\pi i}{n}}$ be a primitive $n$-th root of unity. The Galois group of $x^n-1$ is

$$\mathbb{Q}\left(\text{roots of } x^n-1\right)=\mathbb{Q}\left(\zeta,\zeta^2,\ldots,\zeta^{n-1}\right)=\mathbb{Q}\left(\zeta\right). \tag{7.168}$$

Any element of $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta\right)/\mathbb{Q}\right)=:G$ is completely determined by where it sends $\zeta$. Since $x^n-1$ is a rational polynomial (whose coefficients are fixed by $G$), an element of $G$ sends $\zeta$ to another root of $x^n-1$.

Let $\sigma, \tau \in G$ that sends $\zeta$ to $\zeta^j$ and $\zeta^k$, respectively. Then

$$\sigma\tau(\zeta) = \sigma\left(\zeta^k\right) = \left(\zeta^k\right)^j = \zeta^{kj} = \left(\zeta^j\right)^k = \tau\left(\zeta^j\right) = \tau\sigma(\zeta). \tag{7.169}$$

Hence, $\sigma\tau = \tau\sigma$, i.e. $G$ is abelian. ■

**Exercise 7.51.** (a) Prove that the Galois group of $x^3 - 2$ over $\mathbb{Q}$ is $S_3$, the symmetric group in 3 letters.

(b) Find the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

(c) Write the diagram of subgroups of the Galois group and the corresponding diagram of intermediate fields of the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

*Solution.* Let $K$ be the splitting field of $x^3 - 2$. By Claim 7.3, $[K : \mathbb{Q}] = 6$. The splitting field is

$$K = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\right) = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right). \tag{7.170}$$

If $\mathrm{Gal}(K/\mathbb{Q}) =: G$ is the Galois group, then $|G| = 6$ since $[K : \mathbb{Q}] = 6$. Consider the field automorphisms $K \to K$

$$\sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \quad \omega \mapsto \omega, \tag{7.171}$$

$$\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad \omega \mapsto \omega^2. \tag{7.172}$$

Then $\operatorname{ord}\sigma = 3$ and $\operatorname{ord}\tau = 2$. Then $\sigma$ is a 3-cycle on the set of roots $R := \left\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\right\}$, and $\tau$ is a transposition on $R$ that swaps $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$. Therefore, $\langle\sigma, \tau\rangle \cong S_3$. Since $|G| = 6$, and $\langle\sigma, \tau\rangle \leq G$, we have

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma, \tau\rangle = \left\{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\right\} \cong S_3. \tag{7.173}$$

Now, the subgroups of $G$ and their fixed fields are:

- $H = \{\mathrm{id}\}$, then $\operatorname{Fix} H = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$.
- $H = \langle\tau\rangle$. Then $\tau$ fixes $\sqrt[3]{2}$, so $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\sqrt[3]{2}\right)$. Also, $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]$, so $\operatorname{Fix} H = \mathbb{Q}\left(\sqrt[3]{2}\right)$.
- $H = \langle\sigma\tau\rangle$. Then $\sigma\tau$ fixes $\sqrt[3]{2}\omega^2$, since

$$\sigma\tau\left(\sqrt[3]{2}\omega^2\right) = \sigma\left(\sqrt[3]{2}\omega^4\right) = \sigma\left(\sqrt[3]{2}\omega\right) = \sqrt[3]{2}\omega^2; \tag{7.174}$$

so $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\sqrt[3]{2}\omega^2\right)$. Also,

$$\left[\mathbb{Q}\left(\sqrt[3]{2}\omega^2\right) : \mathbb{Q}\right] = 3 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}], \tag{7.175}$$

so $\operatorname{Fix} H = \mathbb{Q}\left(\sqrt[3]{2}\omega^2\right)$.

- $H = \left\langle \sigma^2\tau \right\rangle$. Then $\sigma^2\tau$ fixes $\sqrt[3]{2}\omega$, since

$$\sigma^2\tau\left(\sqrt[3]{2}\omega\right) = \sigma^2\left(\sqrt[3]{2}\omega^2\right) = \sqrt[3]{2}\omega^2\ \omega^2 = \sqrt[3]{2}\omega; \tag{7.176}$$

  so $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\sqrt[3]{2}\omega\right)$. Also,

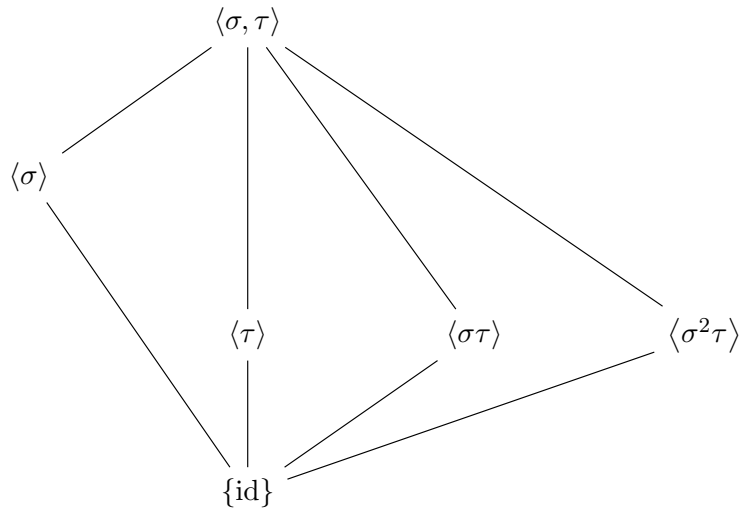
$$\left[\mathbb{Q}\left(\sqrt[3]{2}\omega\right) : \mathbb{Q}\right] = 3 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}], \tag{7.177}$$

  so $\operatorname{Fix} H = \mathbb{Q}\left(\sqrt[3]{2}\omega\right)$.

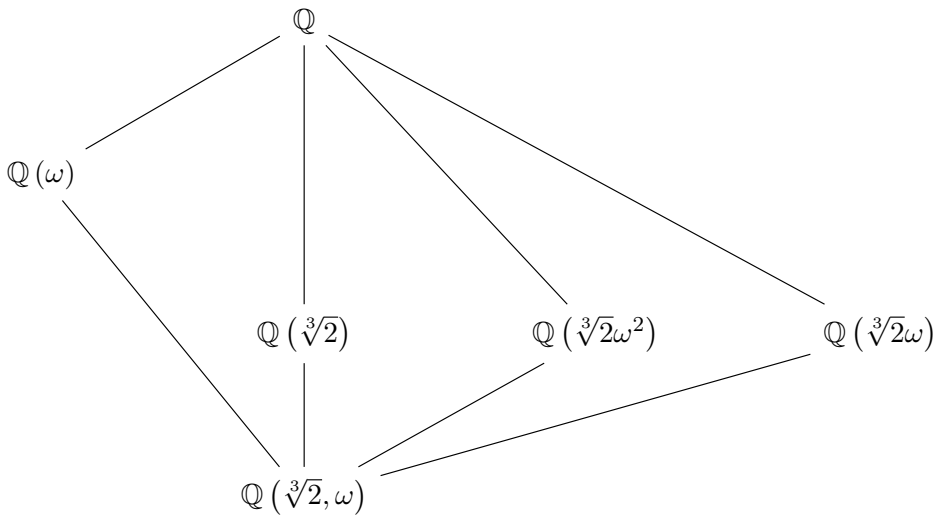
- $H = \langle\sigma\rangle$. Then $\sigma$ fixes $\omega$, so $\operatorname{Fix} H \supseteq \mathbb{Q}(\omega)$. Also, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]$, so $\operatorname{Fix} H = \mathbb{Q}(\omega)$.

- $H = G$, so $\operatorname{Fix} H = \mathbb{Q}$.

The subgroup lattice is (top $\supset$ bottom)




The subfield lattice is (top $\subset$ bottom)




■

**Exercise 7.52.** Determine the Galois group of the following polynomials over $\mathbb{Q}$.

(a) $x^4 - 10x^2 + 5$.

(b) $x^4 - x^2 - 6$.

*Solution.* (a) $f$ is irreducible, by Eisenstein. The roots are

$$\pm\sqrt{5 \pm \sqrt{20}} = \pm\sqrt{5 \pm 2\sqrt{5}} \qquad \text{(all four combinations)}. \tag{7.178}$$

We write

$$\alpha_1 = \sqrt{5+2\sqrt{5}},\ \alpha_2 = -\sqrt{5+2\sqrt{5}},\ \alpha_3 = \sqrt{5-2\sqrt{5}},\ \alpha_4 = -\sqrt{5-2\sqrt{5}}. \tag{7.179}$$

Notice that

$$\alpha_1\alpha_3 = \sqrt{\left(5+2\sqrt{5}\right)\left(5-2\sqrt{5}\right)} = \sqrt{25-20} = \sqrt{5}. \tag{7.180}$$

Squaring $\alpha_1$ gives

$$\alpha_1^2 = 5 + 2\sqrt{5} \implies \sqrt{5} = \frac{\alpha_1^2 - 5}{2} \in \mathbb{Q}(\alpha_1). \tag{7.181}$$

Consequently,

$$\alpha_3 = \frac{\sqrt{5}}{\alpha_1} \in \mathbb{Q}(\alpha_1). \tag{7.182}$$

The splitting field is exactly

$$K = \mathbb{Q}(\alpha_1, -\alpha_1, \alpha_3, -\alpha_3) = \mathbb{Q}(\alpha_1). \tag{7.183}$$

Since $f$ is irreducible and $\alpha_1$ is a root of $f$, we must have $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4$. So $\mathrm{Gal}(K/\mathbb{Q})$ has order 4.

Since $f$ is irreducible, $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the set $R = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of roots of $f$. So there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ mapping $\alpha_1 \mapsto \alpha_3$ yields $\sigma\left(\sqrt{5}\right) = -\sqrt{5}$, which leads to:

$$\sigma(\alpha_3) = \sigma\left(\frac{\sqrt{5}}{\alpha_1}\right) = \frac{-\sqrt{5}}{\alpha_3} = -\alpha_1 = \alpha_2. \tag{7.184}$$

Thus, $\sigma^2(\alpha_1) = \alpha_2 \neq \alpha_1$, proving $\sigma$ has order 4. Since $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, we have

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}_4. \tag{7.185}$$

(b) We can factorize $f$ as

$$x^4 - x^2 - 6 = \left(x^2 - 3\right)\left(x^2 + 2\right). \tag{7.186}$$

So the roots are $\pm\sqrt{3}, \pm i\sqrt{2}$. The splitting field is

$$K := \mathbb{Q}\left(\pm\sqrt{3}, \pm i\sqrt{2}\right) = \mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right), \tag{7.187}$$

and we have $\left[\mathbb{Q}\left(\sqrt{3},\sqrt{2}\right):\mathbb{Q}\right]=2\cdot 2=4$. Therefore, $|\mathrm{Gal}\left(K/\mathbb{Q}\right)|=4$. Consider the automorphisms $K\to K$

$$\sigma_1:\sqrt{3}\mapsto-\sqrt{3},\quad i\sqrt{2}\mapsto i\sqrt{2}; \tag{7.188}$$

$$\sigma_2:\sqrt{3}\mapsto\sqrt{3},\quad i\sqrt{2}\mapsto -i\sqrt{2}. \tag{7.189}$$

They commute, both has order 2, and they generate a subgroup of order 4 (isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2$). Since $|\mathrm{Gal}\left(K/\mathbb{Q}\right)|=4$, this is the whole group, i.e.

$$\mathrm{Gal}\left(K/\mathbb{Q}\right)=\langle\sigma_1,\sigma_2\rangle\cong\mathbb{Z}_2\times\mathbb{Z}_2. \tag{7.190}$$

■

**Exercise 7.53.** Let $p$ be a prime number, $\omega=e^{2\pi i/5}$. Determine the Galois group of $K=\mathbb{Q}\left(\sqrt[5]{p},\omega\right)$ over $\mathbb{Q}$.

*Solution.* $\sqrt[5]{p}$ is a root of $x^5-p$, which is irreducible by Eisenstein. Therefore, $\left[\mathbb{Q}\left(\sqrt[5]{p}\right):\mathbb{Q}\right]=5$. $\left[\mathbb{Q}\left(\omega\right):\mathbb{Q}\right]=4$, as $\omega$ is a root of the irreducible polynomial $x^4+x^3+x^2+x+1$. Since $\gcd(5,4)=1$, we have (by Claim 6.1)

$$\left[\mathbb{Q}\left(\sqrt[5]{p},\omega\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt[5]{p}\right):\mathbb{Q}\right]\left[\mathbb{Q}\left(\omega\right):\mathbb{Q}\right]=5\cdot 4=20. \tag{7.191}$$

Furthermore, the extension $\mathbb{Q}\leq\mathbb{Q}\left(\sqrt[5]{p},\omega\right)$ is Galois since it's the splitting field of $x^5-p$. So $\mathrm{Gal}\left(K/\mathbb{Q}\right)$ has size 20.

Now, any automorphism $K\to K$ is completely determined by where it sends $\sqrt[5]{p}$ and $\omega$. For an element of $\mathrm{Gal}\left(K/\mathbb{Q}\right)$, it sends $\sqrt[5]{p}$ to one of $\sqrt[5]{p}\,\omega^j$; and it sends $\omega$ to one of $\omega^j$'s. So in total there are $5\cdot 4=20$ possiblities. Since there are exactly 20 elements of $\mathrm{Gal}\left(K/\mathbb{Q}\right)$, each of them defines a unique element of $\mathrm{Gal}\left(K/\mathbb{Q}\right)$. So we consider the automorphisms

$$\sigma:\sqrt[5]{p}\mapsto\sqrt[5]{p}\,\omega,\quad\omega\mapsto\omega, \tag{7.192}$$

$$\tau:\sqrt[5]{p}\mapsto\sqrt[5]{p},\quad\omega\mapsto\omega^2. \tag{7.193}$$

Then $\mathrm{ord}\,\sigma=5$ and $\mathrm{ord}\,\tau=4$. So they generate a subgroup of order 20. Since $|\mathrm{Gal}\left(K/\mathbb{Q}\right)|=[K:\mathbb{Q}]=20$, they generate the whole $\mathrm{Gal}\left(K/\mathbb{Q}\right)$, i.e.

$$\mathrm{Gal}\left(K/\mathbb{Q}\right)=\langle\sigma,\tau\rangle. \tag{7.194}$$

Now, consider $\tau\sigma\tau^{-1}$. It fixes $\omega$, so it must be one of the $\sigma^j$. Now,

$$\tau\sigma\tau^{-1}\left(\sqrt[5]{p}\right)=\tau\sigma\left(\sqrt[5]{p}\right)=\tau\left(\sqrt[5]{p}\omega\right)=\sqrt[5]{p}\omega^2=\sigma^2\left(\sqrt[5]{p}\right). \tag{7.195}$$

Therefore,

$$\mathrm{Gal}\left(K/\mathbb{Q}\right)=\langle\sigma,\tau\rangle=\langle\sigma\rangle\rtimes\langle\tau\rangle\cong\mathbb{Z}_5\rtimes\mathbb{Z}_4\cong\mathbb{Z}_5\rtimes\mathbb{Z}_5^\times. \tag{7.196}$$

We can realize it using matrices:

$$\mathbb{Z}_5 \rtimes \mathbb{Z}_5^\times \cong \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{Z}_5^\times, b \in \mathbb{Z} \right\}, \tag{7.197}$$

as

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}. \tag{7.198}$$

Here, we are identifying $\sigma$ with $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\tau$ with $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$. ■

**Exercise 7.54.** What are the degrees of the following fields over $\mathbb{Q}$?

(a) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.

(b) $\mathbb{Q}\left(\sqrt{2}, \sqrt{-2}\right)$.

(c) $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$.

(d) $\mathbb{Q}\left(\sqrt[3]{2} - \sqrt{3}\right)$.

*Solution.* (a) $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 4$, by Exercise 7.7.

(b) Since $\mathbb{Q}\left(\sqrt{2}\right) \leq \mathbb{R}$, it doesn't contain $\sqrt{2}i$, so

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{-2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, \sqrt{-2}\right) : \mathbb{Q}\mathbb{Q}\left(\sqrt{2}\right)\right] \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4. \tag{7.199}$$

(c) $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$ and $\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2$, and they are coprime, so by Claim 6.1,

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] \left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 3 \cdot 2 = 6. \tag{7.200}$$

(d) Let $\alpha = \sqrt[3]{2} - \sqrt{3}$. We claim that $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$. Clearly, $\sqrt[3]{2} - \sqrt{3} \in \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$, so $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$. Now,

$$2 = \left(\alpha + \sqrt{3}\right)^3 = \alpha^3 + 3\alpha^2\sqrt{3} + 9\alpha + 3\sqrt{3} = \alpha^3 + 9\alpha + \sqrt{3}\left(3\alpha^2 + 3\right) \tag{7.201}$$

So we have

$$\sqrt{3} = \frac{2 - \alpha^3 - 9\alpha}{3\alpha^2 + 3} \in \mathbb{Q}(\alpha). \tag{7.202}$$

Therefore, $\sqrt[3]{2} \in \mathbb{Q}(\alpha)$, and as a result $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) \subseteq \mathbb{Q}(\alpha)$.

So we have $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$, and hence,

$$\left[\mathbb{Q}\left(\sqrt[3]{2} - \sqrt{3}\right)\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 6. \tag{7.203}$$

■

**Exercise 7.55.** Which of the extensions of $\mathbb{Q}$ in the previous exercise are Galois extensions?

*Solution.* (c) and (d) are the same fields, and they are NOT Galois extensions, since the irreducible polynomial $x^3-2$ has a root in $\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right)$, but it doesn't split. So the extension $\mathbb{Q}\leq\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right)$ is not normal.

(a) is the splitting field of $\left(x^2-2\right)\left(x^2-3\right)$, as

$$\mathbb{Q}\left(\text{roots of }\left(x^2-2\right)\left(x^2-3\right)\right)=\mathbb{Q}\left(\pm\sqrt{2},\pm\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right). \tag{7.204}$$

(b) is the splitting field of $\left(x^2-2\right)\left(x^2+2\right)$, as

$$\mathbb{Q}\left(\text{roots of }\left(x^2-2\right)\left(x^2+2\right)\right)=\mathbb{Q}\left(\pm\sqrt{2},\pm\sqrt{2}i\right)=\mathbb{Q}\left(\sqrt{2},\sqrt{2}i\right). \tag{7.205}$$

Therefore, $\mathbb{Q}\leq\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ and $\mathbb{Q}\leq\mathbb{Q}\left(\sqrt{2},\sqrt{2}i\right)$ are Galois extensions, by Exercise 8.4. ■

**Exercise 7.56.** Determine the Galois group of the splitting field over $\mathbb{Q}$ of $\left(x^3-2\right)\left(x^3+3\right)$.

*Solution.* The roots are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ and $-\sqrt[3]{3}$, $-\sqrt[3]{3}\omega$, $-\sqrt[3]{3}\omega^2$. The splitting field is

$$K:=\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2,-\sqrt[3]{3},-\sqrt[3]{3}\omega,-\sqrt[3]{3}\omega^2\right)=\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{3},\omega\right). \tag{7.206}$$

First, notice that $\sqrt[3]{3}\notin\mathbb{Q}\left(\sqrt[3]{2}\right)$ by the solution of Exercise 7.14. Therefore, $x^3-3$ is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$, since none of the roots are $\mathbb{Q}\left(\sqrt[3]{2}\right)$. Therefore,

$$\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{3}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{3}\right):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3\cdot3=9. \tag{7.207}$$

Then $\omega$ is the root of the irreducible degree-2 polynomial $x^2+x+1$, and since $\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{3}\right)\subseteq\mathbb{R}$, we have

$$[K:\mathbb{Q}]=\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{3},\omega\right):\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{3}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{3}\right):\mathbb{Q}\right]=2\cdot9.=18. \tag{7.208}$$

Note that any field automorphism $K\to K$ is completely determined by where it sends $\sqrt[3]{2}$, $\sqrt[3]{3}$, $\omega$. For an element of $\mathrm{Gal}\,(K/\mathbb{Q})$, it sends $\sqrt[3]{2}$ to one of $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ (since all of them are roots of $x^3-2$); it sends $\sqrt[3]{3}$ to one of $\sqrt[3]{3}$, $\sqrt[3]{3}\omega$, $\sqrt[3]{3}\omega^2$; it sends $\omega$ to one of $\omega,\omega^2$. So in total there are $3\cdot3\cdot2=18$ possiblities. Since there are exactly 18 elements of $\mathrm{Gal}\,(K/\mathbb{Q})$, each of them defines a unique element of $\mathrm{Gal}\,(K/\mathbb{Q})$. So we consider the automorphisms

$$\sigma:\sqrt[3]{2}\mapsto\sqrt[3]{2}\omega,\quad\sqrt[3]{3}\mapsto\sqrt[3]{3},\quad\omega\mapsto\omega, \tag{7.209}$$

$$\tau:\sqrt[3]{2}\mapsto\sqrt[3]{2},\quad\sqrt[3]{3}\mapsto\sqrt[3]{3}\omega,\quad\omega\mapsto\omega, \tag{7.210}$$

$$\mu:\sqrt[3]{2}\mapsto\sqrt[3]{2},\quad\sqrt[3]{3}\mapsto\sqrt[3]{3},\quad\omega\mapsto\omega^2. \tag{7.211}$$

We have $\mathrm{ord}\,\sigma=\mathrm{ord}\,\tau=3$ and $\mathrm{ord}\,\mu=2$. And

$$\mathrm{Gal}\,(K/\mathbb{Q})=\langle\sigma,\tau,\mu\rangle. \tag{7.212}$$

Since $\sigma$ and $\tau$ commute, they generate a subgroup of order 9 which is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. Now, consider the element $\mu\left(\sigma^j\tau^k\right)\mu$. It fixes $\omega$ since $\sigma^j\tau^k$ doesn't touch $\omega$. Then

$$\mu\sigma^j\tau^k\mu\left(\sqrt[3]{2}\right) = \mu\sigma^j\tau^k\left(\sqrt[3]{2}\right) = \mu\sigma^j\left(\sqrt[3]{2}\right) = \mu\left(\sqrt[3]{2}\omega^j\right) = \sqrt[3]{2}\omega^{-j} = \sigma^{-j}\tau^{-k}\left(\sqrt[3]{2}\right). \quad (7.213)$$

Similarly, on $\sqrt[3]{3}$,

$$\mu\sigma^j\tau^k\mu\left(\sqrt[3]{3}\right) = \sigma^{-j}\tau^{-k}\left(\sqrt[3]{3}\right). \quad (7.214)$$

Therefore, we have

$$\mu\left(\sigma^j\tau^k\right)\mu = \left(\sigma^j\tau^k\right)^{-1}. \quad (7.215)$$

So we have

$$\mathrm{Gal}\left(K/\mathbb{Q}\right) = \langle\sigma,\tau,\mu\rangle \cong \mathrm{Dih}\left(\langle\sigma,\tau\rangle\right) \cong \mathrm{Dih}\left(\mathbb{Z}_3\times\mathbb{Z}_3\right) \cong \left(\mathbb{Z}_3\times\mathbb{Z}_3\right)\rtimes\mathbb{Z}_2. \quad (7.216)$$

■

**Exercise 7.57.** Let $\alpha$ be a complex root of the polynomial $x^3+x+1$ over $\mathbb{Q}$ and let $K$ be the splitting field of this polynomial over $\mathbb{Q}$.

(a) Is $\sqrt{-3}$ in $\mathbb{Q}(\alpha)$? Is it in $K$?

(b) Prove that $\mathbb{Q}(\alpha)$ has no automorphism over $\mathbb{Q}$ except the identity.

*Solution.* (a) First, notice that $f = x^3+x+1$ is irreducible over $\mathbb{Q}$, since $\pm1$ are not roots of $f$. Now, if $\sqrt{3}i \in \mathbb{Q}(\alpha)$, then we would have that

$$\mathbb{Q} \le \mathbb{Q}\left(\sqrt{3}i\right) \le \mathbb{Q}(\alpha), \quad (7.217)$$

so $\left[\mathbb{Q}\left(\sqrt{3}i\right):\mathbb{Q}\right]$ divides $[\mathbb{Q}(\alpha):\mathbb{Q}]$, which is absurd, as $f$ is the minimal polynomial of $\alpha$, and hence $[\mathbb{Q}(\alpha):\mathbb{Q}] = \deg f = 3$.

For the latter part, we first show that $\sqrt{\Delta} \in K$.

> **Claim 7.4:** Let $K$ be the splitting field of a cubic $x^3+px+q$. Then $\sqrt{\Delta} \in K$.
>
> *Proof.* If $a,b,c$ are roots of $x^3+px+q$, then
>
> $$\sqrt{\Delta} = (a-b)(b-c)(c-a) \in \mathbb{Q}(a,b,c) = K. \quad (7.218)$$
>
> □

The discriminant of the polynomial $x^3+x+1$ is (Exercise 7.69) $-4p^3-27q^2 = -31$. So $\sqrt{31}i \in K$. If $\sqrt{3}i \in \mathbb{Q}$, then

$$\mathbb{Q}\left(\sqrt{31}i, \sqrt{3}i\right) \le K. \quad (7.219)$$

Since $f$ is strictly increasing (as $f' > 0$), so it has exactly one real root. Thus, $[K : \mathbb{Q}] = 6$ by Claim 7.3. By tower law,

$$\left[\mathbb{Q}\left(\sqrt{31}i, \sqrt{3}i\right) : \mathbb{Q}\right] \Big| [K : \mathbb{Q}] = 6. \tag{7.220}$$

**Claim 7.5:** If $p, q$ are distinct primes, then $\left[\mathbb{Q}\left(\sqrt{p}i, \sqrt{q}i\right) : \mathbb{Q}\right] = 4$.

*Proof.* By tower law,

$$[\mathbb{Q}(\sqrt{p}i, \sqrt{q}i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}i, \sqrt{q}i) : \mathbb{Q}(\sqrt{p}i)]\,[\mathbb{Q}(\sqrt{p}i) : \mathbb{Q}] \tag{7.221}$$

$\left[\mathbb{Q}\left(\sqrt{p}i\right) : \mathbb{Q}\right] = 2$, because $\left\{1, \sqrt{p}i\right\}$ is a basis of $\mathbb{Q}\left(\sqrt{p}i\right)$ over $\mathbb{Q}$.

$\left[\mathbb{Q}\left(\sqrt{p}i, \sqrt{q}i\right) : \mathbb{Q}\left(\sqrt{p}i\right)\right]$ is either 1 or 2, because $\sqrt{q}i$ is a root of $x^2 + q$. If it's 1, then $\sqrt{q}i \in \mathbb{Q}\left(\sqrt{p}i\right)$. But in that case,

$$a + b\sqrt{p}i = \sqrt{q}i \text{ for some } a, b \in \mathbb{Q}. \tag{7.222}$$

Squaring and simplifying, we have

$$2ab\sqrt{p}i = -q - a^2 + b^2 p. \tag{7.223}$$

If $ab \neq 0$, then LHS is purely imaginary and RHS is real, which can't be true. If $a = 0$, then $q = b^2 p$. Say $b = \frac{m}{n}$ with $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. Then

$$pm^2 = qn^2. \tag{7.224}$$

But then $p \mid qn^2$ implies $p \mid n^2$. This gives $p^2 \mid n^2$. But that implies $p^2 \mid pm^2$, i.e. $p \mid m^2$. This contradicts $\gcd(m, n) = 1$.

If $b = 0$, then $\sqrt{q}i = a$, which is not possible since $\sqrt{q}i \notin \mathbb{Q}$. Therefore,

$$[\mathbb{Q}(\sqrt{p}i, \sqrt{q}i) : \mathbb{Q}(\sqrt{p}i)] = 2. \tag{7.225}$$

Hence,

$$[\mathbb{Q}(\sqrt{p}i, \sqrt{q}i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}i, \sqrt{q}i) : \mathbb{Q}(\sqrt{p}i)]\,[\mathbb{Q}(\sqrt{p}i) : \mathbb{Q}] = 2 \cdot 2 = 4. \tag{7.226}$$

□

So we have $\left[\mathbb{Q}\left(\sqrt{31}i, \sqrt{3}i\right) : \mathbb{Q}\right] = 4$, which doesn't divide 6. Thus we arrive at a contradiction, so $\sqrt{3}i \notin K$.

(b) First, notice that $[K : \mathbb{Q}] = 6$. In other words, $\mathbb{Q}(\alpha)$ doesn't contain any other root of $f$, since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

An automorphism of $\mathbb{Q}(\alpha)$ would map a root of $f$ to another root of $f$ (because such an automorphism would fix $\mathbb{Q}$, and $f \in \mathbb{Q}[x]$). Therefore, an automorphism must map $\alpha \mapsto \alpha$. So the only automorphism of $\mathbb{Q}(\alpha)$ is $\mathrm{id}_{\mathbb{Q}(\alpha)}$.

■

**Exercise 7.58.** Let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of $f = x^3 + 2x + 1$ and let $g = x^3 + x + 1$. Does $g$ have a root in $K$?

*Solution.* Assume for the sake of contradiction that $g$ has a root $\beta \in \mathbb{Q}(\alpha)$. Then $\mathbb{Q}(\beta) \leq \mathbb{Q}(\alpha)$. But

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg g = \deg f = [\mathbb{Q}(\alpha) : \mathbb{Q}], \tag{7.227}$$

since $f, g$ are irreducibles. Therefore, $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$. Let $L_f, L_g$ be the splitting fields of $f, g$, respectively. Then $L_f$ (respectively, $L_g$) is the smallest Galois extension of $\mathbb{Q}$ that contains $\mathbb{Q}(\alpha)$ (respectively, $\mathbb{Q}(\beta)$). Since $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$, we have $L_f = L_g =: L$.

By Claim 7.4, $\sqrt{\Delta_f} = \sqrt{-59}, \sqrt{\Delta_g} = \sqrt{-31} \in L$. Since $f$ has only one real root (since $f' > 0$, so $f$ is increasing everywhere), $[L : \mathbb{Q}] = 6$, by Claim 7.3. Therefore,

$$\mathbb{Q} \leq \mathbb{Q}\left(\sqrt{-31}, \sqrt{-59}\right) \leq L, \tag{7.228}$$

so $\left[\mathbb{Q} \leq \mathbb{Q}\left(\sqrt{-31}, \sqrt{-59}\right) : \mathbb{Q}\right]$ divides $[L : \mathbb{Q}] = 6$. But $\left[\mathbb{Q} \leq \mathbb{Q}\left(\sqrt{-31}, \sqrt{-59}\right) : \mathbb{Q}\right] = 4$ by Claim 7.5. This is a contradiction! ■

**Exercise 7.59.** Let $f \in k[x]$ be a polynomial of degree $n$, and let $K$ be a splitting field for $f$ over $k$. Prove that $[K : k]$ divides $n!$.

*Solution.* We prove it by induction on $n$. The base case $n = 1$ is trivial. By induction hypothesis, suppose for any polynomial of degree $d \leq n - 1$, the degree of its splitting field divides $d!$.

Now, let $f \in k[x]$ with $\deg f = n$. If $f$ is not irreducible, $f = gh$ with $\deg g = n_1, \deg h = n_2$, both of which strictly smaller than $n$. Let $K'$ be the splitting field of $g$ over $k$. Then by induction hypothesis,

$$\left[K' : k\right] \,\middle|\, n_1! \tag{7.229}$$

Let $K$ be the splitting field of $h$ over $K'$. Then by induction hypothesis,

$$\left[K : K'\right] \,\middle|\, n_2! \tag{7.230}$$

Then $K$ is the splitting field of $f$ over $k$. So

$$[K : k] = \left[K : K'\right]\left[K' : k\right] \,\middle|\, n_2! n_1! \,\middle|\, (n_1 + n_2)! = n! \tag{7.231}$$

Now, consider the case $f$ is irreducible. Now, let $\alpha$ be a root of $f$, so we write

$$f = (x - \alpha)\, g, \tag{7.232}$$

where $g \in k(\alpha)[x]$ with $\deg g = n-1$. Then by induction hypothesis, since $K$ is the splitting field of $g$ over $k(\alpha)$,

$$[K : k(\alpha)] \,\Big|\, (n-1)! \tag{7.233}$$

Also, the minimal polynomial of $\alpha$ over $k$ is $f$ (upto scaling), so $[k(\alpha) : k] = \deg f = n$. Therefore,

$$[K : k] = [K : k(\alpha)]\,[k(\alpha) : k] \,\Big|\, (n-1)!\, n = n! \tag{7.234}$$

and we are done. ■

**Exercise 7.60.** Let $G$ be a finite group. Prove that there exists a field $k$ and a Galois extension $K$ of $k$ whose Galois group is $G$.

*Solution.* Since $G$ is finite, by Cayley's theorem, $G$ is (isomorphic to) a subgroup of some $S_n$. Let $K$ be any field, and consider

$$L := K(x_1, \ldots, x_n), \tag{7.235}$$

be the field of rational functions with coefficients in $K$ and variables $x_1, \ldots, x_n$. Then $K \leq L$ is a field extension, and $S_n$ acts on $L$ by permuting the variables:

$$\sigma \cdot f(x_1, \ldots, x_n) := f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right), \qquad \text{for } \sigma \in S_n, f \in L. \tag{7.236}$$

So $S_n \leq \mathrm{Aut}(L/K)$ (actually, $S_n$ is isormorphic to a subgroup of $\mathrm{Aut}(L/K)$). Since $G \leq S_n$, $G$ is a finite subgroup of $\mathrm{Aut}(L/K)$. Therefore, by Artin's theorem,

$$\mathrm{Fix}\, G \leq L \text{ is Galois, and } \mathrm{Gal}(L/\mathrm{Fix}\, G) = G. \tag{7.237}$$

■

**Exercise 7.61.** Let $K/L/k$ be fields. Prove or disprove:

(a) If $K/k$ is Galois, then $K/L$ is Galois.

(b) If $K/k$ is Galois, then $L/k$ is Galois.

(c) If $L/k$ and $K/L$ are Galois, then $K/k$ is Galois.

*Solution.* (a) True. If $k \leq K$ is Galois, then an intermediate field $L$ is going to be $L = \mathrm{Fix}(H)$ for some $H \leq \mathrm{Gal}(K/k)$. By Artin's theorem, $\mathrm{Fix}\, H \leq K$ is Galois.

(b) False. If $k \leq K$ is Galois, then an intermediate field $L$ is going to be $L = \mathrm{Fix}(H)$ for some $H \leq G := \mathrm{Gal}(K/k)$. $k \leq \mathrm{Fix}\, H$ is normal if and only if $H \trianglelefteq G$. So this is false when $\mathrm{Gal}(K/k)$ has non-normal subgroups. For example, consider the field extension

$$\mathbb{Q} \leq \mathbb{Q}\left(\sqrt[3]{2}\right) \leq \mathbb{Q}\left(\sqrt[3]{2}, \omega\right). \tag{7.238}$$

$\mathbb{Q} \leq \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$ is Galois (since it's the splitting field of a separable polynomial $x^3 - 2$, by Exercise 8.4), but $\mathbb{Q} \leq \mathbb{Q}\left(\sqrt[3]{2}\right)$ is not Galois, because it's not normal. Because the polynomial $x^3 - 2$ has one root in $\mathbb{Q}\left(\sqrt[3]{2}\right)$, but it doesn't split as the other (complex) roots are not in $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

(c) False. Consider the field extension

$$\mathbb{Q} \leq \mathbb{Q}\left(\sqrt{2}\right) \leq \mathbb{Q}\left(\sqrt[4]{2}\right). \tag{7.239}$$

$\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$, so they are normal by Exercise 7.31. Since we are in characteristic 0, every algebraic extension is separable. In particular, every finite extension is separable. So the extensions $\mathbb{Q} \leq \mathbb{Q}\left(\sqrt{2}\right)$ and $\mathbb{Q}\left(\sqrt{2}\right) \leq \mathbb{Q}\left(\sqrt[4]{2}\right)$ are Galois.

But $\mathbb{Q} \leq \mathbb{Q}\left(\sqrt[4]{2}\right)$ is not Galois, because it's not normal by Exercise 7.30.

■

**Exercise 7.62.** Let $K/k$ be a Galois extension whose Galois group is the symmmetric group $S_3$. Is it true that $K$ is the splitting field of an irreducible cubic polynomial over $k$?

*Solution.* Let $G = \mathrm{Gal}\,(K/k) \cong S_3$. Then $G$ has a subgroup $H$ isomorphic to $\langle (1\ 2) \rangle$. Then

$$[\mathrm{Fix}\, H : k] = [G : H] = [S_3 : \langle (1\ 2) \rangle] = 3. \tag{7.240}$$

$k \leq \mathrm{Fix}\, H$ is a finite separable extension, so by primitive element theorem, $\mathrm{Fix}\, H = k(\alpha)$ for some $\alpha \in K$. Since $[k(\alpha) : k] = 3$, the minimal polynomial $f$ of $\alpha$ over $k$ has degree-3.

Since $k \leq K$ is Galois, in particular, normal, and $f \in k[x]$ has one root $\alpha \in K$. So the other roots $r_1, r_2 \in K$. Therefore, the splitting field $E$ of $f$ satisfies

$$E = k(\alpha, r_1, r_2) = k(\alpha, r_1) \leq K. \tag{7.241}$$

Now, notice that if $r_1 \in k(\alpha)$, that would mean $E = k(\alpha)$, so $k \leq k(\alpha) = \mathrm{Fix}\, H$ is a Galois extension. But that's not true since $H$ is not a normal subgroup of $G$. Therefore, $[k(\alpha, r_1) : k(\alpha)] \geq 2$. In fact, it is 2, since $r_1$ is a root of the degree-2 polynomial $g \in k(\alpha)[x]$, where

$$f(x) = (x - a)\, g(x). \tag{7.242}$$

Therefore, $[k(\alpha, r_1) : k(\alpha)] = 2$. As a result,

$$[E : k] = [k(\alpha, r_1) : k(\alpha)]\, [k(\alpha) : k] = 2 \cdot 3 = 6 = [K : k]. \tag{7.243}$$

So $K = E$, which is the splitting field of irreducible $f \in k[x]$ with $\deg f = 3$. ■

**Exercise 7.63.** Let $K/k$ be a Galois extension with Galois group $G$ and let $H \leq G$. Prove that there exists an element $\beta \in K$ whose stabilizer is $H$.

*Solution.* $k \leq K$ is Galois, in particular, finite separable. Then $k \leq \operatorname{Fix} H$ is a separable extension by the following claim.

> **Claim 7.6:** If $K \leq L \leq M$ are finite field extensions such that $K \leq M$ is separable, then $K \leq L$ is separable.
>
> *Proof.* Let $\alpha \in L$, then $\alpha \in M$. Since $K \leq M$ is separable, the minimal polynomial $f$ of $\alpha$ over $K$ has simple roots in its splitting field. Therefore, any element of $L$ has this property that its minimal polynomial over $L$ has simple roots in its splitting field. So $K \leq L$ is separable. □

Since $k \leq \operatorname{Fix} H$ is finite separable, $\operatorname{Fix} H = k(\beta)$ for some $\beta \in \operatorname{Fix} H$. We claim that $\operatorname{Stab} \beta = H$.

Since $H$ fixes all elements of $k(\beta)$, in particular, $\beta$, $\operatorname{Stab} \beta \supseteq H$. On the other hand, for $\sigma \in \operatorname{Stab} \beta$, $\sigma$ fixes any element of $k(\beta) = \operatorname{Fix} H$, so $\sigma \in H$, proving $\operatorname{Stab} \beta \subseteq H$. ■

**Exercise 7.64.** Let $K$ be a subfield of $\mathbb{C}$ which is a Galois extension of $\mathbb{Q}$. Prove or disprove: Complex conjugation carries $K$ to itself, and thus it defines an automorphism of $K$.

*Solution.* If $K \leq \mathbb{R}$, then complex conjugation is identity, which is an automorphism of $K$. Let $\alpha \in K$, which is not real. Then $\alpha$ is a root of some irreducible polynomial $f \in \mathbb{Q}[x]$. Since $\mathbb{Q} \leq K$ is a normal extension, and one of the roots of $f$ is in $K$, all the roots of $f$ are in $K$. In particular, $\overline{\alpha} \in K$.

So we have proved that for every $\alpha \in K$, $\overline{\alpha} \in K$. Now we can define the field automorphism $\alpha \mapsto \overline{\alpha}$, which fixes $\mathbb{Q}$ (so it's an element of $\operatorname{Gal}(K/\mathbb{Q})$). ■

**Exercise 7.65.** Prove that the discriminant of a cubic $f \in \mathbb{R}[x]$ is positive if all the roots are real and negative if not.

*Solution.* Let $a, b, c$ be the roots of $f$. If $a, b, c \in \mathbb{R}$, then the discriminant

$$\Delta = (a-b)^2 (b-c)^2 (c-a)^2 \geq 0 \tag{7.244}$$

since all the terms are individually non-negative. Suppose not all roots are real. Then there is one real root and two complex roots (which are complex-conjugates of each other). Say the roots are

$$a, \quad b = \quad u + iv, \quad c = \quad u - iv, \tag{7.245}$$

where $a, u, v \in \mathbb{R}$ with $v \neq 0$. Then

$$(b-c)^2 = (2iv)^2 = -4v^2 < 0. \tag{7.246}$$

On the other hand,

$$(a-b)^2 (c-a)^2 = (a-b)^2 \left(a-\overline{b}\right)^2 = |a-b|^2 = (a-u)^2 + v^2 > 0. \tag{7.247}$$

Therefore,

$$\Delta = (a-b)^2 (b-c)^2 (c-a)^2 < 0. \tag{7.248}$$

■

**Exercise 7.66.** Determine the Galois groups of the following polynomials over $\mathbb{Q}$.

(a) $x^3 + 27x - 4$.

(b) $x^3 + x + 1$.

(c) $x^3 + x^2 - 2x + 1$.

(d) $x^3 + x^2 - 2x - 1$.

*Solution.* We're gonna use the following fact:

If $f \in \mathbb{Q}[x]$ with $\deg f = 3$, then $\mathrm{Gal}(f)$ is either $A_3$ (if $\sqrt{\Delta} \in \mathbb{Q}$) or $S_3$ (if $\sqrt{\Delta} \notin \mathbb{Q}$).

**Claim 7.7:** If $f = x^3 + bx^2 + cx + d$, then $\Delta = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd$.

*Proof.* We do the transformation $x = y - \frac{b}{3}$. This transforms $f(x)$ into a depressed cubic:

$$g(y) = y^3 + py + q. \tag{7.249}$$

Equating coefficients shows that:

$$p = c - \frac{b^2}{3} \quad \text{and} \quad q = d - \frac{bc}{3} + \frac{2b^3}{27}. \tag{7.250}$$

Because a linear shift shifts all roots equally $y_i = \alpha_i + \frac{b}{3}$, the differences between the roots remain invariant $y_i - y_j = \alpha_i - \alpha_j$. Consequently, the discriminant of $f(x)$ is identical to the discriminant of $g(y)$. The discriminant of the depressed cubic is (by Exercise 7.69)

$$\Delta = -4p^3 - 27q^2 \tag{7.251}$$

Finally, we substitute the expressions for $p$ and $q$ back into the formula:

$$\Delta = -4\left(c - \frac{b^2}{3}\right)^3 - 27\left(d - \frac{bc}{3} + \frac{2b^3}{27}\right)^2 \tag{7.252}$$

Expanding the two parts explicitly:

$$-4\left(c - \frac{b^2}{3}\right)^3 = -4c^3 + 4b^2c^2 - \frac{4b^4c}{3} + \frac{4b^6}{27}, \tag{7.253}$$

$$-27\left(d - \frac{bc}{3} + \frac{2b^3}{27}\right)^2 = -27d^2 + 18bcd - 4b^3d - 3b^2c^2 + \frac{4b^4c}{3} - \frac{4b^6}{27}. \tag{7.254}$$

Summing these expressions cancels out the fractional $\frac{4b^4c}{3}$ and $\frac{4b^6}{27}$ terms. So we have

$$\Delta = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd \tag{7.255}$$

□

(a) First $f$ is irreducible since $f(\pm 2) \neq 0$. $f' > 0$, so $f$ has exactly one real root. If $K$ is the splitting field of $f$ over $\mathbb{Q}$, then $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 6$, by Claim 7.3. Therefore, $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

(b) First $f$ is irreducible since $f(\pm 1) \neq 0$. $f' > 0$, so $f$ has exactly one real root. If $K$ is the splitting field of $f$ over $\mathbb{Q}$, then $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 6$, by Claim 7.3. Therefore, $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

(c) In this case, the discriminant is $\Delta = -31$, so $\sqrt{\Delta} \notin \mathbb{Q}$. Hence, $\mathrm{Gal}(f) \cong S_3$.

(d) In this case, the discriminant is $\Delta = 49$, so $\sqrt{\Delta} \in \mathbb{Q}$. Hence, $\mathrm{Gal}(f) \cong A_3$.

■

**Exercise 7.67.** Let $f$ be an irreducible cubic polynomial over $k$ and let $\delta$ be the square root of the discriminant. Show that $f$ remains irreducible over $k(\delta)$.

*Solution.* Assume for the sake of contradiction that $f$ is not irreducible over $k(\delta)$. Then $f$ has a root $\alpha \in k(\delta)$. Then, consider the field extensions $k \leq k(\alpha) \leq k(\delta)$,

$$[k(\delta) : k] = [k(\delta) : k(\alpha)]\,[k(\alpha) : k] = [k(\delta) : k(\alpha)] \cdot 3 \geq 3. \tag{7.256}$$

Here, $[k(\alpha) : k] = 3$ since $f$ (upto scaling) is the minimal polynomial of $\alpha$ over $k$. But, $\delta$ is a root of $x^2 - \Delta \in k[x]$. So $[k(\delta) : k] \leq 2$. Thus we arrive at a contradiction! ■

**Exercise 7.68.** Let $f \in \mathbb{Q}[x]$ be an irreducible cubic polynomials which has precisely one real root, and let $K$ be the splitting field of $f$ over $\mathbb{Q}$. Show that $[K : \mathbb{Q}] = 6$.

*Solution.* Claim 7.3. ■

**Exercise 7.69.** Prove that the discriminant of the cubic $x^3 + px + q$ is $-4p^3 - 27q^2$.

*Solution.* Let $a, b, c$ be roots of $x^3 + px + q$. Then

$$a + b + c = 0, \quad ab + bc + ca = p, \quad abc = -q. \tag{7.257}$$

Writing $f(x) = (x - a)(x - b)(x - c)$, we have

$$f'(a) = (a - b)(a - c), \quad f'(b) = (b - a)(b - c), \quad f'(c) = (c - a)(c - b). \tag{7.258}$$

Then

$$\Delta = [(a-b)(b-c)(c-a)]^2 = -f'(a)f'(b)f'(c). \tag{7.259}$$

Writing $f'(x) = 3x^2 + p$, we get

$$-\Delta = \left(3a^2+p\right)\left(3b^2+p\right)\left(3c^2+p\right) \tag{7.260}$$

$$= 27a^2b^2c^2 + 9p\left(a^2b^2+b^2c^2+c^2a^2\right) + 3p^2\left(a^2+b^2+c^2\right) + p^3 \tag{7.261}$$

Now, $a^2b^2c^2 = q^2$, and

$$a^2+b^2+c^2 = (a+b+c)^2 - 2(ab+bc+ca) = -2p. \tag{7.262}$$

On the other hand,

$$a^2b^2+b^2c^2+c^2a^2 = (ab+bc+ca)^2 - 2abc(a+b+c) = p^2. \tag{7.263}$$

Assembling everything back into (7.261), we have

$$-\Delta = 27q^2 + 9p\cdot p^2 + 3p^2(-2p) + p^3 = 4p^3 + 27q^2. \tag{7.264}$$

■

**Exercise 7.70.** Let $k$ be a field of characteristic 0.

(a) Let $k(\alpha_1,\ldots,\alpha_n)/k$ be a finite field extension. Let $L/K$ be a field extension, such that $L/k$ is a finite Galois extension (e.g. let $L$ be the splitting field of the product of the minimal polynomials of the $\alpha_i$). Assume $K/k$ is not normal. We put

$$K' = k\left(g(\alpha_i) \mid i = 1,\ldots,n,\ g \in \mathrm{Gal}(L/k)\right). \tag{7.265}$$

Show that $K'/k$ is a normal extension.

(b) Now assume that each $\alpha_i$ satisfies an equation $X^{r_i} - a_i = 0$ with $a_i \in k(\alpha_1,\ldots,\alpha_{i-1})$. Then we have for all $g \in \mathrm{Gal}(L/k)$ that $g(\alpha_i)$ satisfies the equation $X^{r_i} - g(a_i) = 0$, with $g(a_i) \in k(g(\alpha_1),\ldots,g(\alpha_{i-1}))$. Conclude that $K'/k$ is a radical Galois extension.

*Solution.* (a) Let $\sigma \in \mathrm{Gal}(L/k)$, and

$$S = \{g(\alpha_i) \mid 1 \le i \le n \text{ and } g \in \mathrm{Gal}(L/k)\} = \bigcup_{i=1}^{n} \mathrm{Orb}(\alpha_i). \tag{7.266}$$

Then $\sigma$ just permutes each orbit, and hence, we have $\sigma(S) = S$. Therefore, we have that $\sigma(K') = K'$, as $K' = k(S)$ and $\sigma$ maps the generating set $S$ onto itself.

> **Claim 7.8:** Let $k \le K \le L$ be field extensions such that $k \le L$ is Galois. Then $k \le K$ is normal if and only if for all $\sigma \in \mathrm{Gal}(L/k)$, $\sigma(K) = K$.

*Proof.* Take any $\varphi : K \to \overline{K}$ with $\varphi|_k = \mathrm{id}_k$. Then $\varphi$ can be extended to $\varphi' : L \to \overline{K}$. Since $k \leq L$ is Galois, in particular normal, $\varphi'(L) = L$, by Exercise 8.2. So $\varphi'$ is an element of $\mathrm{Gal}\,(L/k)$. Conversely, any $\varphi' \in \mathrm{Gal}\,(L/k)$, restricting it to $K$ and extending the codomain, we get a homomorphism $\varphi : K \to \overline{K}$. Then we have

$$\begin{aligned} k \leq K \text{ normal} &\iff \varphi(K) = K \text{ for all } \varphi : K \to K' \\ &\iff \varphi'(K) = K \text{ for all } \varphi' \in \mathrm{Gal}\,(L/k)\,. \end{aligned}$$

□

Therefore, $k \leq K'$ is normal.

(b) In characteristic 0, any algebraic extension is separable. Since $k \leq K'$ is normal, it is Galois. Since $k \leq L$ is Galois, $\mathrm{Gal}\,(L/k)$ is finite, so we can list the elements

$$\mathrm{Gal}\,(L/k) = \{g_1, g_2, \ldots, g_m\}\,. \tag{7.267}$$

By definition,

$$K' = k\left(g_1(\alpha_1), \ldots, g_1(\alpha_n), g_2(\alpha_1), \ldots, g_2(\alpha_n), \ldots, g_m(\alpha_1), \ldots, g_m(\alpha_n)\right). \tag{7.268}$$

We are given that for each $i$, the element $\alpha_i$ satisfies the radical relation

$$(\alpha_i)^{r_i} = a_i, \tag{7.269}$$

where $a_i$ is an element belonging to the subfield generated by the prior elements in the initial chain, namely $a_i \in k(\alpha_1, \ldots, \alpha_{i-1})$. This means there exists a rational function expression $P_i$ with coefficients in $k$ such that

$$a_i = P_i(\alpha_1, \ldots, \alpha_{i-1})\,. \tag{7.270}$$

Now, let us apply the field automorphism $g_j \in \mathrm{Gal}\,(L/k)$ to both sides of the radical relation.

$$(g_j(\alpha_i))^{r_i} = g_j(a_i)\,. \tag{7.271}$$

Because $g_j$, fixes every element of $k$, applying $g_j$ to the rational expression for $a_i$ transforms the arguments while leaving the coefficients in $k$ unchanged:

$$g_j(a_i) = P_i(g_j(\alpha_1), \ldots, g_j(\alpha_{i-1}))\,. \tag{7.272}$$

Therefore,

$$g_j(a_i) \in k(g_j(\alpha_1), \ldots, g_j(\alpha_{i-1})) \tag{7.273}$$

Therefore, $g_j(\alpha_i)$ is a root of the polynomial $x^n - A$ ($n$ and $A$ depends on $i, j$), for

$$A \in k\left(g_1(\alpha_1), \ldots, g_1(\alpha_n), \ldots, g_j(\alpha_1), \ldots, g_j(\alpha_{i-1})\right). \tag{7.274}$$

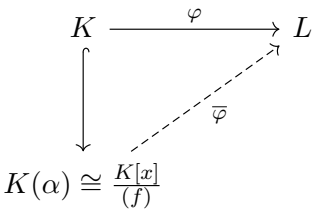
Therefore, at each step, we are addjoining an element, namely $g_j(\alpha_i)$, which is the $n$-th root of some element in the previous field. Hence, $k \leq K'$ is a radical extension.

■

# §8 Problem Set 5

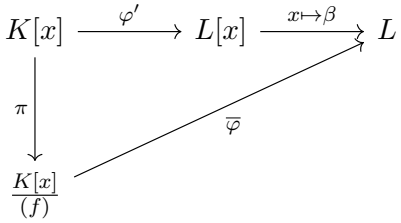
**Exercise 8.1.** Let $\varphi\colon K \to L$ be a homomorphism of fields such that $L$ is algebraically closed. Let $i\colon K \hookrightarrow F$ be a finite algebraic extension. Show that there exists a homomorphism $\overline{\varphi}\colon F \to L$ extending $\varphi$, i.e. $\varphi = \overline{\varphi} \circ i$.

*Solution.* Consider the special case $F = K(\alpha)$ first. Let $f$ be the minimal polynomial of $\alpha$ over $K$, with $\deg f = n$. Then $F \cong K[x]/(f)$.




(8.1)

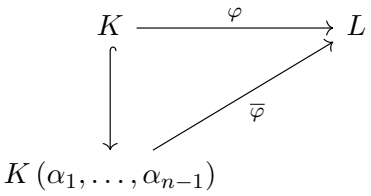
We can define $\varphi' : K[x] \to L[x]$ that maps each coefficient under $\varphi$. Under this homomorphism, $\varphi'(f)$ is a polynomial in $L[x]$. Since $L$ is algebraically closed, it has a root, say $\beta$.




(8.2)

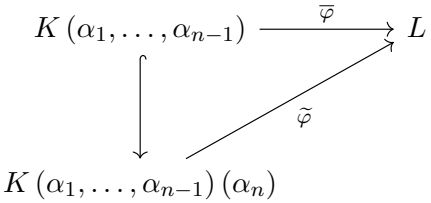
Since the kernel of the top composition $(x \mapsto \beta) \circ \varphi'$ contains $(f)$, which is the kernel of $\pi$, there exists a homomorphism $\overline{\varphi}$ such that the (8.2) commutes. This is precisely the map $\overline{\varphi}$ that we need in (8.1).

Now, we consider the general case $F = K(\alpha_1, \ldots, \alpha_n)$. We approach by induction. The base case is already done. By inductive hypothesis, $\overline{\varphi}$ exists such that the following diagram commutes:



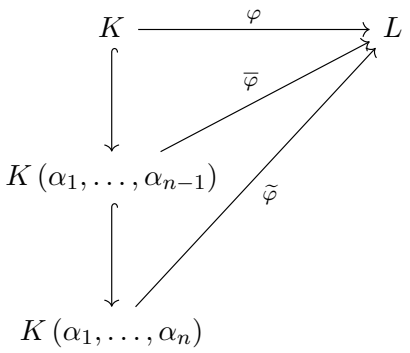

(8.3)

By the base case, $\widetilde{\varphi}$ exists such that the following diagram commutes:



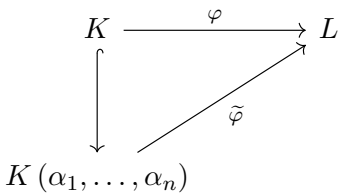

(8.4)

Stacking these commutative diagrams, we get




(8.5)

Therefore, we have the commutative diagram




(8.6)

which is what we wanted! ■

**Exercise 8.2.** Show that the following are equivalent for a finite algebraic extension $K \subseteq F$:

1. $K \subseteq F$ is normal;
2. for all $\varphi\colon F \to \overline{F}$ such that $\varphi|_K = \mathrm{Id}_K$, we have $\varphi(F) = F$;
3. $F$ is the splitting field of a finite family of polynomials in $K[x]$.

*Solution.* **(1⇒2)** Let $\varphi : F \to \overline{F}$ such that $\varphi|_K = \mathrm{id}_K$. Let $\alpha \in F$ with minimal polynomial $f$ over $K$. Then $f$ splits in $F$ by normality. $\varphi(\alpha)$ is a root of $\varphi(f) = f$, because

$$\sum_{i=0}^{n} a_i \alpha^i = 0 \implies 0 = \varphi\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} a_i \varphi(\alpha)^i . \tag{8.7}$$

So $\varphi(\alpha) \in F$. Hence $\varphi(F) \subseteq F$. Since $\varphi$ is an injective $K$-linear map between $K$-vector spaces of the same finite dimension, $\varphi(F) = F$.

**(2⇒1)** Let $\alpha \in F$ and let $\beta \in \overline{F}$ be any root of the minimal polynomial $f$ of alpha. The map

$$\begin{aligned} K(\alpha) \cong K[x]/(f) &\to \overline{F} \\ \alpha &\mapsto \beta \end{aligned} \tag{8.8}$$

extends to $\varphi : F \to \overline{F}$ by Exercise 8.1. By 2, $\beta = \varphi(\alpha) \in \varphi(F) = F$. So $f$ splits in $F$.

**(2⇒3)** Let $F = K(\alpha_1, \ldots, \alpha_n)$, with minimal polynomials $f_1, \ldots, f_n$, respectively. As above, every root of $f_i$ is in $F$. So $\prod f_i$ splits in $F$, and $F$ is generated by the roots of $f_i$'s. Hence, $f$ is the splitting field of $\prod f_i$.

**(3⇒2)** Let $F$ be the splitting field of $f$ and let $\varphi\colon F \to \overline{F}$ fix $K$. Then $\varphi$ maps roots of $f$ to roots of $f$, and all of these lie in $F$. Since $F$ is generated by these roots, $\varphi(F) \subseteq F$, and equality holds by dimension. ■

**Exercise 8.3.** Let $K \subseteq E$ be a field extension. Let $K \subseteq L \subseteq E$ and $K \subseteq F \subseteq E$ be intermediate extensions such that $K \subseteq L$ and $K \subseteq F$ are finite and algebraic. Denote with $LF$ the smallest subfield of $E$ containing both $L$ and $F$ (called the **composite** field of $L$ and $F$). Show that if $K \subseteq L$ and $K \subseteq F$ are normal, then $K \subseteq LF$ is again normal.

*Solution.* By Exercise 8.2, $L$ and $F$ are splitting fields of $f, g \in K[x]$, respectively. Then

$$L = K(r_1, \ldots, r_n) \text{ and } F = K(s_1, \ldots, s_m), \tag{8.9}$$

where $r_i$ are the roots of $f$ and $s_j$ are roots of $g$. Then we claim that

$$LF = K(r_1, \ldots, r_n, s_1, \ldots, s_m). \tag{8.10}$$

Indeed, $L, F \subseteq K(r_1, \ldots, r_n, s_1, \ldots, s_m)$, so we have $LF \subseteq K(r_1, \ldots, r_n, s_1, \ldots, s_m)$. Furthermore, $r_i, s_j \in LF$ implies $LF \supseteq K(r_1, \ldots, r_n, s_1, \ldots, s_m)$. So $LF = K(r_1, \ldots, r_n, s_1, \ldots, s_m)$ is the splitting field of $fg \in K[x]$. Hence, $K \subseteq LF$ is a normal extension. ■

**Exercise 8.4.** Show that the following are equivalent for a finite algebraic extension $K \subseteq F$:

1. $K \subseteq F$ is Galois;
2. The fixed field of $\mathrm{Aut}(F/K) := \{\varphi \in \mathrm{Aut}(F) \mid \varphi|_K = \mathrm{id}_K\}$ is precisely $K$.
3. $F$ is the splitting field of a separable polynomial in $K[x]$.

*Solution.* **(1⇒2)** Clearly $K \subseteq \mathrm{Fix}(\mathrm{Aut}(F/K))$. Let $a \in \mathrm{Fix}(\mathrm{Aut}(F/K))$, and let $f$ be the minimal polynomial of $a$ over $K$. Since $K \leq F$ is normal and separable, $f$ has $n := \deg f$ distinct roots in $F$.

Let $b$ be a root of $f$. Then the map $K(a) \to \overline{F}$, $a \mapsto b$, extends to a field homomorphism $F \to \overline{F}$ by Exercise 8.1.

$$\begin{array}{ccccc} K(a) & \xrightarrow{a\mapsto b} & F & \hookrightarrow & \overline{F} \\ \downarrow & & & \nearrow_{\varphi} & \\ F & & & & \end{array} \tag{8.11}$$

By Exercise 8.2(2), $\varphi(F) = F$, so $\varphi$ is an automorphism of $F$, and it fixes $K$. So there exists $\varphi \in \mathrm{Aut}(F/K)$ such that $\varphi(a) = b$. Since $a \in \mathrm{Fix}(\mathrm{Aut}(F/K))$,

$$a = \varphi(a) = b. \tag{8.12}$$

Therefore, all the roots of $f$ are $a$ only. Hence, $f = x - a$, i.e. $a \in K$.

**Claim 8.1** (Artin's theorem)**:** Let $K \leq L$ be a field extension and $H \leq \operatorname{Aut}(L/K)$ be a finite subgroup. Then $M = \operatorname{Fix}(H) \leq L$ is a finite Galois extension and $H = \operatorname{Gal}(L/M)$.

*Proof.* Let $\alpha \in L$. First, we claim that $[M(\alpha) : M] \leq |H|$. Let

$$R = \{\alpha_1, \ldots, \alpha_n\} = \{\varphi(\alpha) \mid \varphi \in H\} = \operatorname{Orb}_H(\alpha). \tag{8.13}$$

Then $|R| = n \leq |H|$. We define a polynomial

$$g(x) = \prod_{i=1}^{n} (x - \alpha_i) \in L[x]. \tag{8.14}$$

Each $\varphi$ induces a homomorphism $\varphi_* : L[x] \to L[x]$. Since $R$ is the orbit of $\alpha$ under $H$, any element $\varphi \in H$ permutes $R$. In other words, after applying $\varphi_*$ on $g$, it stays invariant. In other words, every coefficient of $g$ stays invariant under the action of $\varphi$, i.e. the coefficients are in $\operatorname{Fix}(H) = M$.

If $f$ is the minimal polynomial of $\alpha$ over $M$, then $f \mid g$. Then

$$[M(\alpha) : M] = \deg f \leq \deg g = n \leq |H|. \tag{8.15}$$

Since $g$ doesn't have repeated roots, $f$ also doesn't have repeated roots. So every element of $L$ is separable over $M$. Also $g$ splits over $L$, so $f$ splits over $L$. This implies the extension $M \leq L$ is also normal.

Next, we'll show that $L = M(\alpha)$ for some $\alpha$. Choose $\alpha$ such that $[M(\alpha) : M]$ is maximal (we can do this because $[M(\alpha) : M] \leq |H|$). We'll show that $L = M(\alpha)$. Suppose $\beta \in L$. Consider the extension $M \leq M(\alpha, \beta)$. Since every element of $L$ is separable over $M$, this is a separable extension. Furthermore, it's finite, because

$$[M(\alpha, \beta) : M] \leq [M(\beta) : M][M(\alpha) : M] \leq |H|^2. \tag{8.16}$$

A finite separable extension is simple, i.e. $M(\alpha, \beta) = M(\gamma)$ for some $\gamma \in L$. Then

$$[M(\gamma) : M] = [M(\gamma) : M(\alpha)][M(\alpha) : M] \geq [M(\alpha) : M]. \tag{8.17}$$

By the maximality of $[M(\alpha) : M]$, we have $[M(\gamma) : M] = [M(\alpha) : M]$, i.e. $M(\gamma) = M(\alpha)$, so that $\beta \in M(\alpha)$. Therefore, $L = M(\alpha)$.

Therefore, $M \leq L$ is a finite extension, which is normal and separable as shown earlier. Therefore, $M \leq L$ is Galois. It's clear that $\operatorname{Gal}(L/M) \subseteq H$. Now,

$$[L : M] = [M(\alpha) : M] \leq |H| \leq |\operatorname{Gal}(L/M)| = [L : M]. \tag{8.18}$$

Hence, $\operatorname{Gal}(L/M) = H$. □

**(2⇒1)** Let $G = \mathrm{Aut}(F/K)$, which is finite since $|\mathrm{Aut}(F/K)| \leq [F : K]$, and $\mathrm{Fix}(G) = K$. By Artin's theorem, $K \leq F$ is Galois.

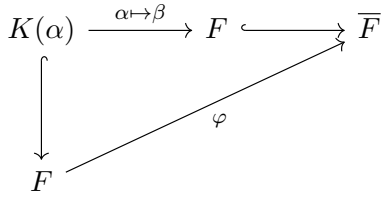
**(2⇒3)** Let $F = K(\alpha_1, \ldots, \alpha_n)$. As in (8.14), let $\mathrm{Orb}_{\mathrm{Aut}(F/K)}(\alpha_i) =: G\alpha_i$ be the orbit of $\alpha_i$ under $\mathrm{Aut}(F/K) =: G$; and we define the polynomials

$$h_i(x) = \prod_{\beta \in G\alpha_i} (x - \beta) \in F[x]. \tag{8.19}$$

This is actually in $K[x]$, that can be proven using the same arguments as in Artin's theorem. Let $f$ be the product of distinct irreducible factors of $h_1 \cdots h_r$. Then $f \in K[x]$ is separable, $F$ is generated by its roots. So $F$ is the splitting field of $f$.

**(3⇒2)** Let $F$ be the splitting field of a separable $f \in K[x]$. We'll show $|\mathrm{Aut}(F : K)| = [F : K]$ by induction on $[F : K]$. The base case $[F : K] = 1$ ic clearly true. Assume the claim holds for all extensions of degree less than $[F : K]$.

Take an irreducible factor $g \in K[x]$ of $f$, with $\deg g = d > 1$ (if all irreducible factors have degree 1, then $f$ splits over $K$, so $F = K$). Since $f$ is separable, $g$ has $d$ distinct roots in $F$. Let $\alpha$ be a root of $g$. Let $\beta$ be another root of $g$. Then the map $K(\alpha) \to \overline{F}$, $\alpha \mapsto \beta$, extends to a field homomorphism $F \to \overline{F}$ by Exercise 8.1.




(8.20)

By Exercise 8.2(2), $\varphi(F) = F$, so $\varphi$ is an automorphism of $F$, and it fixes $K$. This gives $d$ many automorphisms $F \to F$ that fixes $K$, each of which is an extension of $K(\alpha) \to K(\beta)$ to $F \to F$.

An automorphism $F \to F$ that fixes $K$ must take $\alpha$ to another root $\beta$. In order to get that we have to compose a field automorphism that fixes $K(\alpha)$ with $\alpha \mapsto \beta$. Therefore,

$$|\mathrm{Aut}(F/K)| = d\,|\mathrm{Aut}(F/K(\alpha))| = [K(\alpha) : K]\,[F : K(\alpha)] = [F : K]. \tag{8.21}$$

Now, by Artin's theorem,

$$|\mathrm{Aut}(F/K)| = [F : \mathrm{Fix}(\mathrm{Aut}(F/K))] \tag{8.22}$$

Therefore,

$$[F : \mathrm{Fix}(\mathrm{Aut}(F/K))] = [F : K], \tag{8.23}$$

proving $K = \mathrm{Fix}(\mathrm{Aut}(F/K))$. ■

**Exercise 8.5.** Let $K, E, L, F$ be as in Exercise 8.3. Assume, moreover, that $K \subseteq L$ and $K \subseteq F$ are Galois extensions. Show that $K \subseteq LF$ is Galois.

*Solution.* By Exercise 8.4, $L$ and $F$ are splitting fields of separable polynomials $f, g \in K[x]$, respectively. Let

$$h = \prod_{\substack{p \mid fg, \\ p \text{ monic irreducible}}} p. \tag{8.24}$$

We take each $p$ exactly once. (Irreducible and prime are the same, since we're in a PID.) Since $p \mid fg$, it means $p \mid f$ or $p \mid g$. Since $f, g$ are separable, it implies $p$ is also separable (i.e. doesn't have repeated roots in any extension).

Furthermore, $p$ and $q$ can't have a common root. If they have a common root, then the minimal polynomial of that common root divides both $p$ and $q$.But since they are irreducible, their only factors are themselves. So the minimal polynomial of that common root is $p = q$.

Hence, $h$ is separable. Now, we claim that $LF$ is the splitting field of $h$. The roots of $h$ are the roots of $f$ or the roots of $g$. Therefore,

$$LF = K\left((\text{roots of } f) \cup (\text{roots of } g)\right) = K\left(\text{roots of } h\right). \tag{8.25}$$

Hence, $K \leq LF$ is a Galois extension, as it's the splitting field of a separable polynomial $h$. ■

**Exercise 8.6.** Let $K, E, L, F$ be as in Exercise 8.5. Show that $F \subseteq LF$ and $L \cap F \subseteq L$ are Galois extension and the following is an isomorphism:

$$\begin{aligned} \psi' \colon \operatorname{Gal}(LF/F) &\longrightarrow \operatorname{Gal}(L/L \cap F) \\ \sigma &\longmapsto \sigma|_L. \end{aligned} \tag{8.26}$$

*Solution.* By (8.25),

$$LF = K\left((\text{roots of } f) \cup (\text{roots of } g)\right) = \left[K\left(\text{roots of } g\right)\right]\left(\text{roots of } f\right) \tag{8.27}$$

$$= F\left(\text{roots of } f\right). \tag{8.28}$$

So $LF$ is the splitting field of the separable polynomial $f \in F[x]$. Therefore, $F \leq LF$ is Galois. Similarly,

$$L = K\left(\text{roots of } f\right) = \left(L \cap F\right)\left(\text{roots of } f\right). \tag{8.29}$$

So $L$ is the splitting field of the separable polynomial $f \in (L \cap F)[x]$. Therefore, $L \cap F \leq L$ is Galois.

Let $\sigma \in \operatorname{Gal}(LF/F)$. Since $K \leq L$ is normal, and $\sigma|_L : L \to LF \hookrightarrow \overline{L}$ fixes $L \cap F \supseteq K$, by Exercise 8.2(2), $\sigma(L) = L$. Therefore, $\psi'$ indeed maps from $\operatorname{Gal}(LF/F)$ to $\operatorname{Gal}(L/L \cap F)$.

Now, we'll show that $\psi'$ is injective. Indeed, if $\sigma \in \operatorname{Ker} \psi'$, i.e. $\sigma|_L = \mathrm{id}_L$, $\sigma$ fixes both $L$ and $F$. In particular, it fixes roots of $f$ and $g$. $\sigma$ also fixes $L \cap F \supseteq K$. So $\sigma$ fixes the whole $LF$, since

$$LF = K\left((\text{roots of } f) \cup (\text{roots of } g)\right). \tag{8.30}$$

Therefore, $\sigma = \mathrm{id}_{LF}$, i.e. $\operatorname{Ker} \psi' = \{\mathrm{id}_{LF}\}$.

Now, we'll show that $\psi'$ is surjective. Let $H = \operatorname{im}\psi'$. If $x \in L$ is fixed by $H$, then $x$ is fixed by the whole $\operatorname{Gal}(LF/F)$, so $x \in F$. Therefore, by Artin's theorem,

$$L \cap F = \operatorname{Fix}(H) = \operatorname{Fix}\left(\operatorname{im}\psi'\right), \tag{8.31}$$

and hence, $\operatorname{Gal}(L/L \cap F) = H$, proving the surjectivity of $\psi'$. ■

**Exercise 8.7.** Let $K, E, L, F$ be as in Exercise 8.5. Show that if $K \subseteq L$ and $K \subseteq F$ are Galois, then $K \subseteq LF$ is again Galois and there is an **injective** homomorphism:

$$\begin{aligned} \operatorname{Gal}(LF/K) &\xrightarrow{\psi} \operatorname{Gal}(L/K) \times \operatorname{Gal}(F/K) \\ \sigma &\longmapsto (\sigma|_L, \sigma|_F). \end{aligned} \tag{8.32}$$

Show that $\psi$ defined above is an isomorphism iff $L \cap F = K$.

*Solution.* $K \leq LF$ is Galois, by Exercise 8.5. Since $K \leq L$ is normal, and $\sigma|_L : L \to LF \hookrightarrow \overline{L}$ fixes $K$, by Exercise 8.2(2), $\sigma(L) = L$. Similarly, $\sigma(F) = F$. Hence,

$$(\sigma|_L, \sigma|_F) \in \operatorname{Gal}(L/K) \times \operatorname{Gal}(F/K), \tag{8.33}$$

i.e. $\psi$ is a well-defined homomorphism. If $\sigma \in \operatorname{Ker}\psi$, then $\sigma|_L = \mathrm{id}_L$ and $\sigma|_F = \mathrm{id}_F$. Using the similar argument as the previous question (Exercise 8.6), we get $\sigma = \mathrm{id}_{LF}$. Hence, $\psi$ is injective.

Now, we have

$$\begin{aligned} |\operatorname{Gal}(LF/K)| &= [LF : K] = [LF : F]\,[F : K] && (8.34)\\ &= |\operatorname{Gal}(LF/F)|\,|\operatorname{Gal}(F/K)| && (8.35)\\ &= |\operatorname{Gal}(L/L \cap F)|\,|\operatorname{Gal}(F/K)| && (8.36) \end{aligned}$$

Now,

$$|\operatorname{Gal}(L/L \cap F)| = [L : L \cap F] = \frac{[L : K]}{[L \cap F : K]} = \frac{|\operatorname{Gal}(L/K)|}{[L \cap F : K]}. \tag{8.37}$$

So we have

$$|\operatorname{Gal}(LF/K)| = \frac{1}{[L \cap F : K]}\ |\operatorname{Gal}(L/K) \times \operatorname{Gal}(F/K)|. \tag{8.38}$$

$\psi$ is an injective map. If $L \cap F = K$, then the domain and codomain of $\psi$ are of the same (finite) size, so $\psi$ is surjective as well, and hence $\psi$ is an isomorphism. If $L \cap F \neq K$, then the domain has strictly less elements than the codomain, so $\psi$ can't be an isomorphism. ■

**Exercise 8.8.** Let $E$ be the splitting field of $(x^3 - 7)(x^2 - 3)$ over $\mathbb{Q}$.

(a) Compute $\operatorname{Gal}(E/\mathbb{Q})$.

(b) Find all proper intermediate fields of the extension which are not normal over $\mathbb{Q}$.

*Solution.* **(a)** The roots are $\sqrt[3]{7}\omega^j$ for $j = 0, 1, 2$ and $\pm\sqrt{3}$. So the splitting field is

$$E = \mathbb{Q}\left(\sqrt[3]{7}, \sqrt[3]{7}\omega, \sqrt[3]{7}\omega^2, \sqrt{3}, -\sqrt{3}\right) = \mathbb{Q}\left(\sqrt[3]{7}, \omega, \sqrt{3}\right). \tag{8.39}$$

Then

$$\left[\mathbb{Q}\left(\sqrt[3]{7}, \sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{7}\right) : \mathbb{Q}\right]\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 3 \cdot 2 = 6, \tag{8.40}$$

since they are coprime. $\mathbb{Q}\left(\sqrt[3]{7}, \sqrt{3}\right) \subseteq \mathbb{R}$, so $\omega \notin \mathbb{Q}\left(\sqrt[3]{7}, \sqrt{3}\right)$. Therefore, $\left[E : \mathbb{Q}\left(\sqrt[3]{7}, \sqrt{3}\right)\right] \geq 2$. Also $\omega$ is a root of the polynomial $x^2 + x + 1$, so we have $\left[E : \mathbb{Q}\left(\sqrt[3]{7}, \sqrt{3}\right)\right] = 2$. Now,

$$[E : \mathbb{Q}] = \left[E : \mathbb{Q}\left(\sqrt[3]{7}, \sqrt{3}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{7}, \sqrt{3}\right) : \mathbb{Q}\right] = 2 \cdot 6 = 12. \tag{8.41}$$

Let $L = \mathbb{Q}\left(\sqrt[3]{7}, \omega\right)$ be the splitting field of $x^3 - 7$, and $F = \mathbb{Q}\left(\sqrt{3}\right)$ be the splitting field of $x^2 - 3$. Then $LF = E$, and $E = L\left(\sqrt{3}\right)$. Now, since $K \leq L$ and $K \leq F$ are Galois extensions, and

$$L \cap F = \mathbb{Q}\left(\sqrt[3]{7}, \omega\right) \cap \mathbb{Q}\left(\sqrt{3}\right) \supseteq \mathbb{Q}. \tag{8.42}$$

The intersection will be a subfield of $\mathbb{R}$, so it will be a subfield of $\mathbb{Q}\left(\sqrt[3]{7}\right)$. And it's a subfield of $\mathbb{Q}\left(\sqrt{3}\right)$. Therefore, by tower law,

$$[L \cap F : \mathbb{Q}] \mid \left[\mathbb{Q}\left(\sqrt[3]{7}\right) : \mathbb{Q}\right] = 3 \text{ and } [L \cap F : \mathbb{Q}] \mid \left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2. \tag{8.43}$$

Therefore, $[L \cap F : \mathbb{Q}] = 1$, i.e.

$$L \cap F = \mathbb{Q}. \tag{8.44}$$

Hence, by Exercise 8.7,

$$\mathrm{Gal}\left(E/\mathbb{Q}\right) \cong \mathrm{Gal}\left(L/\mathbb{Q}\right) \times \mathrm{Gal}\left(F/\mathbb{Q}\right). \tag{8.45}$$

Using the same procedure as Exercise 7.51, we find that $\mathrm{Gal}\left(L/\mathbb{Q}\right) \cong S_3 \cong D_3$, and $\mathrm{Gal}\left(F/\mathbb{Q}\right)$ is isomorphic to $\mathbb{Z}_2$ (its two elements are id and $\sqrt{3} \mapsto -\sqrt{3}$). Therefore,

$$\mathrm{Gal}\left(E/\mathbb{Q}\right) \cong D_3 \times \mathbb{Z}_2 \cong D_6. \tag{8.46}$$

The generators are

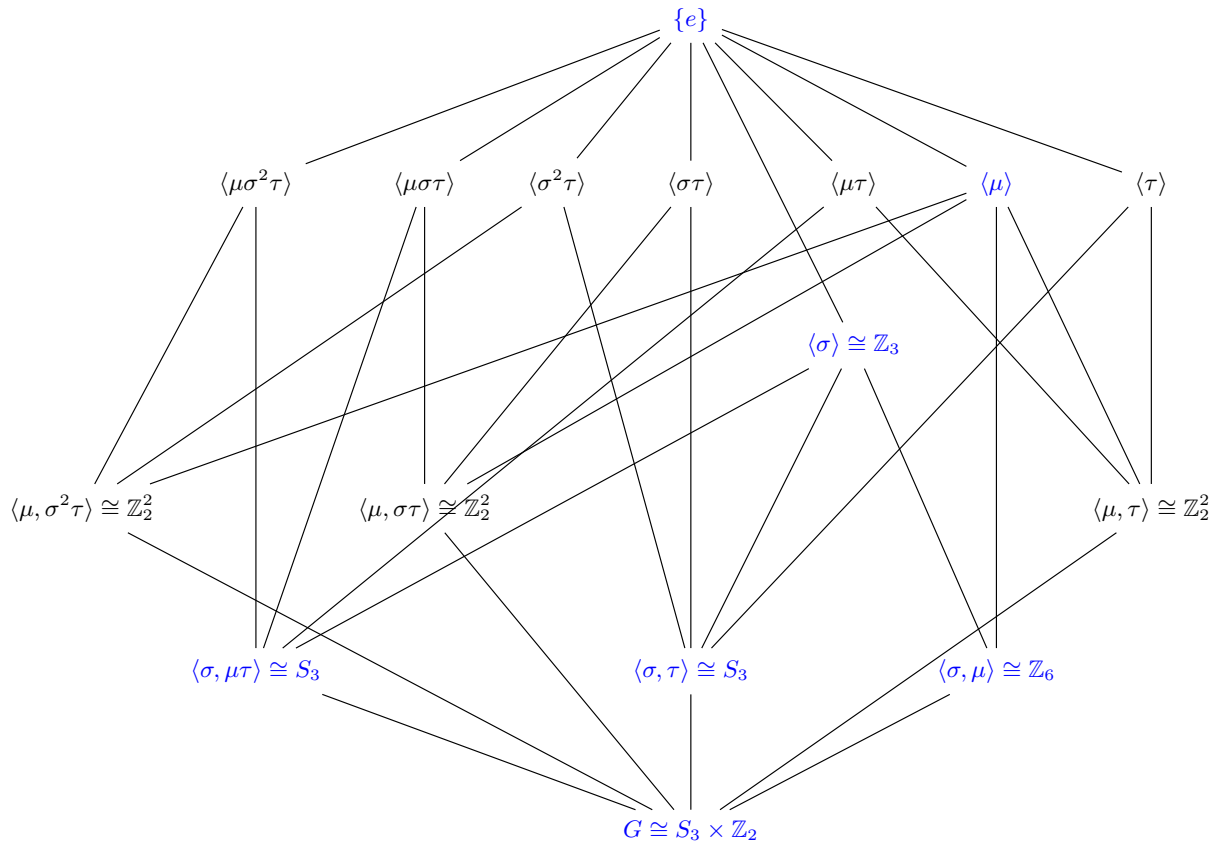
$$\sigma : \sqrt[3]{7} \mapsto \omega\sqrt[3]{7}, \quad \omega \mapsto \omega, \quad \sqrt{3} \mapsto \sqrt{3}, \tag{8.47}$$

$$\tau : \sqrt[3]{7} \mapsto \sqrt[3]{7}, \quad \omega \mapsto \omega^2, \quad \sqrt{3} \mapsto \sqrt{3}, \tag{8.48}$$

$$\mu : \sqrt[3]{7} \mapsto \sqrt[3]{7}, \quad \omega \mapsto \omega, \quad \sqrt{3} \mapsto -\sqrt{3}. \tag{8.49}$$

Here, $\langle \sigma, \tau \rangle$ generates a subgroup isomorphic to $D_3$, and $\mu$ commutes with elements of $\langle \sigma, \tau \rangle$.

**(b)** The subgroup lattice of $G := \mathrm{Gal}\left(E/\mathbb{Q}\right) \cong S_3 \times \mathbb{Z}_2$ is (the normal subgroups are marked blue)




As we can see, there are 9 non-normal subgroups, each corresponding to a non-normal extension. They are:

- $H = \left\langle \sigma^j\tau \right\rangle$ for $j = 0, 1, 2$. $\sigma^j\tau$ fixes $\sqrt{3}$. Also it fixes $\omega^{-j}\sqrt[3]{7}$, since

$$\sigma^j\tau\left(\omega^{-j}\sqrt[3]{7}\right) = \sigma^j\left(\omega^j\sqrt[3]{7}\right) = \omega^j\omega^j\sqrt[3]{7} = \omega^{2j}\sqrt[3]{7} = \omega^{-j}\sqrt[3]{7}. \tag{8.50}$$

  Therefore, $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}, \sqrt{3}\right)$. Now,

$$\left[\mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}, \sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}\right) : \mathbb{Q}\right]\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 6, \tag{8.51}$$

  since they are coprime, so we have

$$\left[\mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}, \sqrt{3}\right) : \mathbb{Q}\right] = 6 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.52}$$

  So $\operatorname{Fix} H = \mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}, \sqrt{3}\right)$.

- $H = \left\langle \mu\sigma^j\tau \right\rangle$ for $j = 0, 1, 2$. $\sigma^j\tau$ fixes $\omega^{-j}\sqrt[3]{7}$, which is also fixed by $\mu$. Now, $\mu\sigma^j\tau$ also fixes $i$ since

$$\mu\sigma^j\tau(i) = \mu\sigma^j\tau\left(\frac{2\omega+1}{\sqrt{3}}\right) = \mu\sigma^j\left(\frac{2\omega^2+1}{\sqrt{3}}\right) = \mu\left(\frac{2\omega^2+1}{\sqrt{3}}\right) = \frac{2\omega^2+1}{-\sqrt{3}} = i. \tag{8.53}$$

Therefore, $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}, i\right)$. Now,

$$\left[\mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}\right) : \mathbb{Q}\right][\mathbb{Q}(i) : \mathbb{Q}] = 6, \tag{8.54}$$

since they are coprime, so we have

$$\left[\mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}, i\right) : \mathbb{Q}\right] = 6 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.55}$$

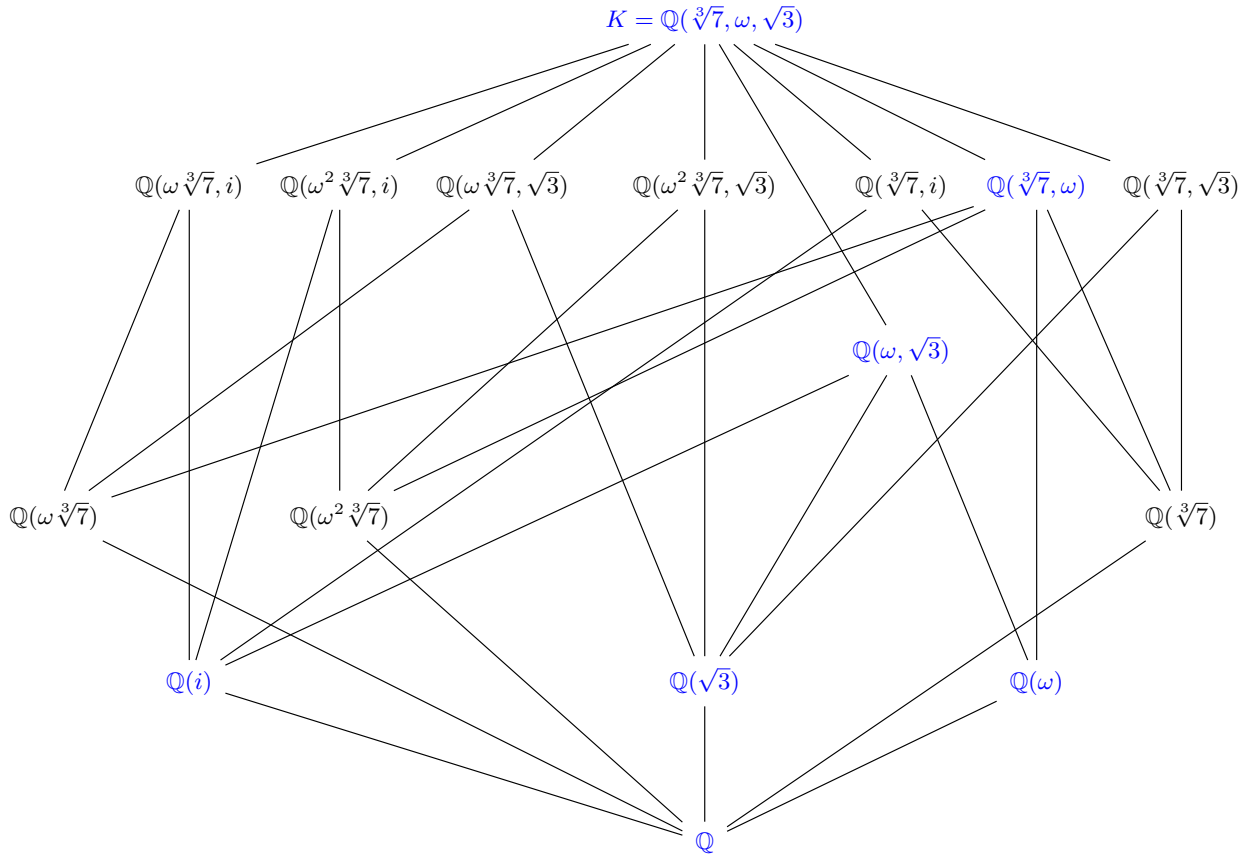
So $\operatorname{Fix} H = \mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}, i\right)$.

- $H = \langle \mu, \sigma^j \tau \rangle$ for $j = 0, 1, 2$. $\mu$ fixes $\sqrt[3]{7}, \omega$. $\sigma^j \tau$ fixes $\omega^{-j}\sqrt[3]{7}$. So $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}\right)$. Now,

$$\left[\mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}\right) : \mathbb{Q}\right] = 3 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.56}$$

So $\operatorname{Fix} H = \mathbb{Q}\left(\omega^{-j}\sqrt[3]{7}\right)$.

In fact, one can compute $\operatorname{Fix} H$ for all $H \leq G$ to find the complete lattice:




■

**Exercise 8.9.** Let $E$ be the splitting field of $x^4 - 2x^2 - 10$ over $\mathbb{Q}$.

(a) Compute $\operatorname{Gal}(E/\mathbb{Q})$.

(b) Compute the number of proper intermediate fields and identify which of them are normal over $\mathbb{Q}$.

*Solution.* **(a)** The roots of $f := x^4 - 2x^2 - 10$ are $\pm\sqrt{1+\sqrt{11}} =: \pm a$ and $\pm i\sqrt{\sqrt{11}-1} =: \pm ib$. Also, notice that $ab = \sqrt{10}$. So we have

$$E = \mathbb{Q}(\pm a, \pm ib) = \mathbb{Q}\left(a, i\frac{\sqrt{10}}{a}\right) = \mathbb{Q}\left(a, i\sqrt{10}\right). \tag{8.57}$$

Now,

$$[E:\mathbb{Q}] = \left[\mathbb{Q}\left(a, i\sqrt{10}\right) : \mathbb{Q}(a)\right][\mathbb{Q}(a):\mathbb{Q}] = 2\cdot 4 = 8, \tag{8.58}$$

since $f$ (irreducible by Eisenstein) is the minimal polynomial of $a$ over $\mathbb{Q}$. So $|\mathrm{Gal}(E/\mathbb{Q})| = [E:\mathbb{Q}] = 8$. Furthermore, since $f$ is irreducible, $\mathrm{Gal}(E/\mathbb{Q})$ acts transitively on $R = \{a, ib, -a, -ib\}$. So there exists an element $\sigma \,\mathrm{Gal}(E/\mathbb{Q})$ that maps $a \mapsto ib$. Since

$$\left(a^2\right) + (ib)^2 = 2, \tag{8.59}$$

$ib \mapsto a$ or $ib \mapsto -a$.

**Case 1:** If $ib \mapsto -a$, then $-a \mapsto -ib$ and $-ib \mapsto a$. So $\sigma$ is a 4-cycle in $\mathrm{Gal}(E/\mathbb{Q})$.

**Case 2:** If $ib \mapsto a$, then we have

$$a \leftrightarrow ib, \quad -a \leftrightarrow -ib. \tag{8.60}$$

So it's like $(1\ 2)(3\ 4)$ seen as an element of $S_4$ acting on $R = \{a, ib, -a, -ib\}$. Now, the complex conjugation map, i.e. $(2\ 4)$, is also in $\mathrm{Gal}(E/\mathbb{Q})$ (Exercise 7.64). Also,

$$(1\ 2)(3\ 4)(2\ 4) = (1\ 2\ 3\ 4). \tag{8.61}$$

Therefore, in both cases there is a 4-cycle in $\mathrm{Gal}(E/\mathbb{Q})$ that acts like

$$a \mapsto ib \mapsto -a \mapsto -ib \mapsto a. \tag{8.62}$$

Let $\sigma$ be this 4-cycle, and let $\tau$ be the complex conjugation that fixes the whole $\mathbb{R}$. Then

$$\tau\sigma\tau(a) = \tau\sigma(a) = \tau(ib) = -ib; \quad \tau\sigma\tau(ib) = \tau\sigma(-ib) = \tau(a) = a. \tag{8.63}$$

So $\tau\sigma\tau$ acts like

$$a \mapsto -ib \mapsto -a \mapsto ib \mapsto a. \tag{8.64}$$

Hence, $\tau\sigma\tau = \sigma^{-1}$. Since $\operatorname{ord}\sigma = 4$ and $\operatorname{ord}\tau = 2$, $\langle\sigma,\tau\rangle \cong D_4$, which has order 8. Since $|\mathrm{Gal}(E/\mathbb{Q})| = [E:\mathbb{Q}] = 8$, we can conclude that

$$\mathrm{Gal}(E/\mathbb{Q}) = \langle\sigma,\tau\rangle = \left\{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\right\} \cong D_4. \tag{8.65}$$

**(b)** The intermediate fields are precisely $\operatorname{Fix} H$ for $H \leq G := \operatorname{Gal}(E/\mathbb{Q}) \cong D_4$.

- $H = \{\mathrm{id}\}$, so $\operatorname{Fix} H = \mathbb{Q}$.
- $H = \langle \sigma^2 \rangle$. $\sigma^2 = (1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$, i.e. it maps $a \leftrightarrow -a$ and $ib \leftrightarrow -ib$. It fixes $a^2 - 1 = \sqrt{11}$ and $iab = i\sqrt{10}$. So $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\sqrt{11}, i\sqrt{10}\right)$. Also,

$$\left[\mathbb{Q}\left(\sqrt{11}, i\sqrt{10}\right) : \mathbb{Q}\right] = 4 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.66}$$

  Hence, $\operatorname{Fix} H = \mathbb{Q}\left(\sqrt{11}, i\sqrt{10}\right)$.

- $H = \langle \tau \rangle$. Then $\tau$ fixes $a$, so $\operatorname{Fix} H \supseteq \mathbb{Q}(a)$. Also,

$$[\mathbb{Q}(a) : \mathbb{Q}] = 4 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.67}$$

  Hence, $\operatorname{Fix} H = \mathbb{Q}(a)$.

- $H = \langle \sigma\tau \rangle$. Since $(1\ 2\ 3\ 4)(2\ 4) = (1\ 2)(3\ 4)$, so $\sigma\tau$ maps $a \leftrightarrow ib$ and $-a \leftrightarrow -ib$. So it fixes $a + ib$, i.e. so $\operatorname{Fix} H \supseteq \mathbb{Q}(a + ib)$.

  **Claim 8.2:** $[\mathbb{Q}(a + ib) : \mathbb{Q}] = 4$.

  *Proof.* Let $\alpha = a + ib$. Then

$$\alpha^2 = a^2 - b^2 + 2iab = 2 + 2i\sqrt{10}. \tag{8.68}$$

  Rearranging and squaring, we get

$$\left(\alpha^2 - 2\right)^2 = \left(2i\sqrt{10}\right)^2 \implies \alpha^4 - 4\alpha^2 + 44 = 0. \tag{8.69}$$

  It remains to show that $x^4 - 4x^2 + 44$ is irreducible. We reduce it to mod 3 to get $x^4 + 2x^2 + 2$. It's clear that it doesn't have any roots in mod 3. The only monic irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$ are $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$. One can easily check that none of these divide $x^4 + 2x^2 + 2$. So it's irreducible over $\mathbb{F}_3$, and hence, it was originally irreducible over $\mathbb{Q}$. □

  Therefore,

$$[\mathbb{Q}(a + ib) : \mathbb{Q}] = 4 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.70}$$

  Hence, $\operatorname{Fix} H = \mathbb{Q}(a + ib)$.

- $H = \langle \sigma^2\tau \rangle$. Since $(1\ 2\ 3\ 4)^2(2\ 4) = (1\ 3)$, so $\sigma^2\tau$ maps $a \leftrightarrow -a$. Then $\tau$ fixes $ib$, so $\operatorname{Fix} H \supseteq \mathbb{Q}(ib)$. Also,

$$[\mathbb{Q}(ib) : \mathbb{Q}] = 4 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.71}$$

  Hence, $\operatorname{Fix} H = \mathbb{Q}(ib)$.

- $H = \langle \sigma^3\tau \rangle$. Since $(1\ 2\ 3\ 4)^3\,(2\ 4) = (1\ 4)\,(2\ 3)$, so $\sigma^3\tau$ maps $a \leftrightarrow -ib$ and $-a \leftrightarrow ib$. So it fixes $a - ib$, i.e. so $\operatorname{Fix} H \supseteq \mathbb{Q}(a - ib)$. Now, $a + ib$ and $a - ib$ has the same minimal polynomial (because $a - ib$ is also a root of the minimal polynomial of $a + ib$, which is irreducible). So
$$[\mathbb{Q}(a - ib) : \mathbb{Q}] = 4 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.72}$$
Hence, $\operatorname{Fix} H = \mathbb{Q}(a - ib)$.

- $H = \langle \sigma \rangle$. Then $\sigma$ negates $\sqrt{11} = a^2 - 1 = b^2 + 1$ and $i\sqrt{10} = iab$, so it fixes their product. In other words, $\operatorname{Fix} H \supseteq \mathbb{Q}\left(i\sqrt{110}\right)$. Now,
$$\left[\mathbb{Q}\left(i\sqrt{110}\right) : \mathbb{Q}\right] = 2 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.73}$$
Hence, $\operatorname{Fix} H = \mathbb{Q}\left(i\sqrt{110}\right)$.

- $H = \langle \sigma^2, \tau \rangle$. $\sigma^2$ fixes $\sqrt{11}$; $\tau$ is complex conjugation so it also fixes $\sqrt{11}$. So $\operatorname{Fix} H \supseteq \mathbb{Q}\left(\sqrt{11}\right)$. Now,
$$\left[\mathbb{Q}\left(\sqrt{11}\right) : \mathbb{Q}\right] = 2 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.74}$$
Hence, $\operatorname{Fix} H = \mathbb{Q}\left(\sqrt{11}\right)$.

- $H = \langle \sigma^2, \sigma\tau \rangle$. $\sigma^2$ fixes $i\sqrt{10}$, $\sigma\tau$ maps $a \leftrightarrow ib$, so it fixes $iab = i\sqrt{10}$. So $\operatorname{Fix} H \supseteq \mathbb{Q}\left(i\sqrt{10}\right)$. Now,
$$\left[\mathbb{Q}\left(i\sqrt{10}\right) : \mathbb{Q}\right] = 2 = [G : H] = [\operatorname{Fix} H : \mathbb{Q}]. \tag{8.75}$$
Hence, $\operatorname{Fix} H = \mathbb{Q}\left(i\sqrt{10}\right)$.

- $H = \langle \sigma, \tau \rangle$. Then $\operatorname{Fix} H = \mathbb{Q}$.

Among these subgroups, the normal ones are all subgroups of size 4 (since they have index 2), and the center $\langle \sigma^2 \rangle = \{\mathrm{id}, \sigma^2\}$. Therefore, the normal proper intermediate fields are
$$\mathbb{Q}\left(i\sqrt{10}\right), \quad \mathbb{Q}\left(\sqrt{11}\right), \quad \mathbb{Q}\left(i\sqrt{110}\right), \quad \mathbb{Q}\left(\sqrt{11}, i\sqrt{10}\right). \tag{8.76}$$

■

**Exercise 8.10.** Let $E$ be the splitting field of the polynomial $x^8 - 2$ over $\mathbb{Q}$.

(a) Find a set of generators for the extension $\mathbb{Q} \subseteq E$ and compute $[E : \mathbb{Q}]$.

(b) Let $\alpha := \sqrt[8]{2}$ and $\zeta := \sqrt{2}(1 + i)/2$. Show that $\mathrm{Gal}(E/\mathbb{Q})$ contains an automorphism $\theta$ such that
$$\sigma(\alpha) = \zeta\alpha, \qquad \sigma(i) = i \tag{8.77}$$
and an automorphism $\sigma$ such that
$$\tau(\alpha) = \alpha, \qquad \tau(i) = -i. \tag{8.78}$$

(c) Show that $\mathrm{Gal}(E/\mathbb{Q})$ is not a dihedral group.

(d) Describe the fields fixed by the following subgroups: $\langle\sigma\rangle$, $\langle\sigma^2\rangle$, $\langle\sigma^4\rangle$, $\langle\tau\rangle$ and $\langle\sigma^4,\tau\rangle$.

*Solution.* **(a)** We claim that $E = \mathbb{Q}(\alpha, i)$ where $\alpha = \sqrt[8]{2}$. The roots of $x^8 - 2$ are $\sqrt[8]{2}\zeta^j$ for $j = 0, 1, \ldots, 7$, where $\zeta$ is a primitive 8-th root of unity:

$$\zeta = e^{\frac{2\pi i}{8}} = \frac{1+i}{\sqrt{2}}. \tag{8.79}$$

Then

$$E = \mathbb{Q}\left(\sqrt[8]{2}, \sqrt[8]{2}\zeta, \ldots, \sqrt[8]{2}\zeta^7\right). \tag{8.80}$$

Indeed, $\alpha \in E$. Furthermore, $\zeta = \frac{\sqrt[8]{2}\zeta}{\sqrt[8]{2}} \in E$. So we have

$$E = \mathbb{Q}\left(\sqrt[8]{2}, \zeta\right). \tag{8.81}$$

Furthermore, $\alpha^4 = \sqrt{2} \in E$, so we have $\sqrt{2}\zeta = 1 + i \in E$. Therefore, $i \in E$. Hence,

$$\mathbb{Q}(\alpha, i) \subseteq E = \mathbb{Q}\left(\sqrt[8]{2}, \zeta\right). \tag{8.82}$$

On the other hand,

$$\zeta = \frac{1+i}{\alpha^4} \in \mathbb{Q}(\alpha, i). \tag{8.83}$$

Therefore,

$$E = \mathbb{Q}(\alpha, i). \tag{8.84}$$

Now,

$$[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 8 = 16. \tag{8.85}$$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ since $x^8 - 2$ is irreducible (by Eisenstein) and its root is $\alpha$. $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$ since $i$ is a root of $x^2 + 1$, and $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$ can't be 1 since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

Therefore, $[E : \mathbb{Q}] = 16$.

**(b)**

$$[\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)] = \frac{[E : \mathbb{Q}]}{[\mathbb{Q}(i) : \mathbb{Q}]} = \frac{16}{2} = 8. \tag{8.86}$$

So the minimal polynomial of $\alpha$ over $\mathbb{Q}(i)$ has degree-8, so the minimal polynomial is $x^8 - 2$. Now, $\mathbb{Q}(i) \leq \mathbb{Q}(i, \alpha)$ is a Galois extension (as it's the splitting field of $x^8 - 2$). So $\mathrm{Gal}(E/\mathbb{Q}(i))$ acts transitively on the set $R := \{\alpha, \alpha\zeta, \ldots, \alpha\zeta^7\}$ of roots of $x^8 - 2$. Hence, there exists an element of $\mathrm{Gal}(E/\mathbb{Q}(i))$ that maps $\alpha \mapsto \alpha\zeta$. This is an element of $\mathrm{Gal}(E/\mathbb{Q})$ such that

$$\alpha \mapsto \alpha\zeta, \quad i \mapsto i. \tag{8.87}$$

That's $\sigma$, and $\tau$ is complex conjugation, which is always in $\mathrm{Gal}(E/\mathbb{Q})$ (Exercise 7.64).

**(c)** Note that $\zeta = \frac{1+i}{\alpha^4}$, so

$$\sigma(\zeta) = \sigma\left(\frac{1+i}{\alpha^4}\right) = \frac{1+i}{\alpha^4\zeta^4} = \zeta\,\frac{1}{\zeta^4} = \zeta^5. \tag{8.88}$$

Since $\gcd(5,8)=1$, $\operatorname{ord}\sigma=8$. Also, $\operatorname{ord}\tau=2$. Furthermore,

$$\tau\sigma\tau(\alpha)=\tau\sigma(\alpha)=\tau(\alpha\zeta)=\alpha\overline{\zeta}=\alpha\zeta^{-1}; \tag{8.89}$$

$$\sigma^3(\alpha)=\sigma^2(\alpha\zeta)=\sigma\left(\alpha\zeta\ \zeta^5\right)=\alpha\zeta\ \left(\zeta^6\right)^5=\alpha\zeta^{-1}. \tag{8.90}$$

$$\tau\sigma\tau(i)=\tau\sigma(-i)=\tau(-i)=i=\sigma^3(i). \tag{8.91}$$

Therefore, $\tau\sigma\tau=\sigma^3\neq\sigma^{-1}$. Therefore, $\operatorname{Gal}(E/\mathbb{Q})$ is **NOT** $D_8$.

**(d)** Let's calculate the fixed fields of the given subgroups.

- $|H|=\langle\sigma\rangle$. Then $\sigma$ fixes $i$, so $\operatorname{Fix}H\supseteq\mathbb{Q}(i)$. Also,

$$[\mathbb{Q}(i):\mathbb{Q}]=2=[G:H]=[\operatorname{Fix}H:\mathbb{Q}], \tag{8.92}$$

  so $\operatorname{Fix}H=\mathbb{Q}(i)$.

- $|H|=\left\langle\sigma^2\right\rangle$. Then $\sigma^2$ fixes $i$, and also $\alpha^4=\sqrt{2}$ as well, since

$$\sigma^2\left(\alpha^4\right)=\sigma\left(\alpha^4\zeta^4\right)=\alpha^4\zeta^4\left(\zeta^4\right)^5=\alpha^4. \tag{8.93}$$

  So $\operatorname{Fix}H\supseteq\mathbb{Q}\left(\sqrt{2},i\right)$. Since

$$\left[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}\right]=4=[G:H]=[\operatorname{Fix}H:\mathbb{Q}], \tag{8.94}$$

  so $\operatorname{Fix}H=\mathbb{Q}(\sqrt{2},i)$.

- $|H|=\left\langle\sigma^4\right\rangle$. Then $\sigma^4$ fixes $i$, and also $\alpha^2=\sqrt[4]{2}$ as well, since

$$\sigma^4\left(\alpha^2\right)=\sigma^3\left(\alpha^2\zeta^2\right)=\sigma^2\left(\alpha^2\zeta^2\ \left(\zeta^2\right)^5\right)=\sigma\left(\alpha^2\zeta^2\ \left(\zeta^{12}\right)^5\right)=\alpha^2\zeta^2\ \left(\zeta^{62}\right)^5=\alpha^2. \tag{8.95}$$

  So $\operatorname{Fix}H\supseteq\mathbb{Q}\left(\sqrt[4]{2},i\right)$. Since

$$\left[\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}\right]=8=[G:H]=[\operatorname{Fix}H:\mathbb{Q}], \tag{8.96}$$

  so $\operatorname{Fix}H=\mathbb{Q}(\sqrt[4]{2},i)$.

- $H=\langle\tau\rangle$. $\tau$ fixes $\alpha$, so so $\operatorname{Fix}H\supseteq\mathbb{Q}(\alpha)$. Also,

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=8=[G:H]=[\operatorname{Fix}H:\mathbb{Q}], \tag{8.97}$$

  so $\operatorname{Fix}H=\mathbb{Q}\left(\sqrt[8]{2}\right)$.

- $H=\left\langle\sigma^4,\tau\right\rangle$. $\sigma^4$ fixes $\alpha^2=\sqrt[4]{2}$. $\tau$ also fixes $\alpha^2$. Now,

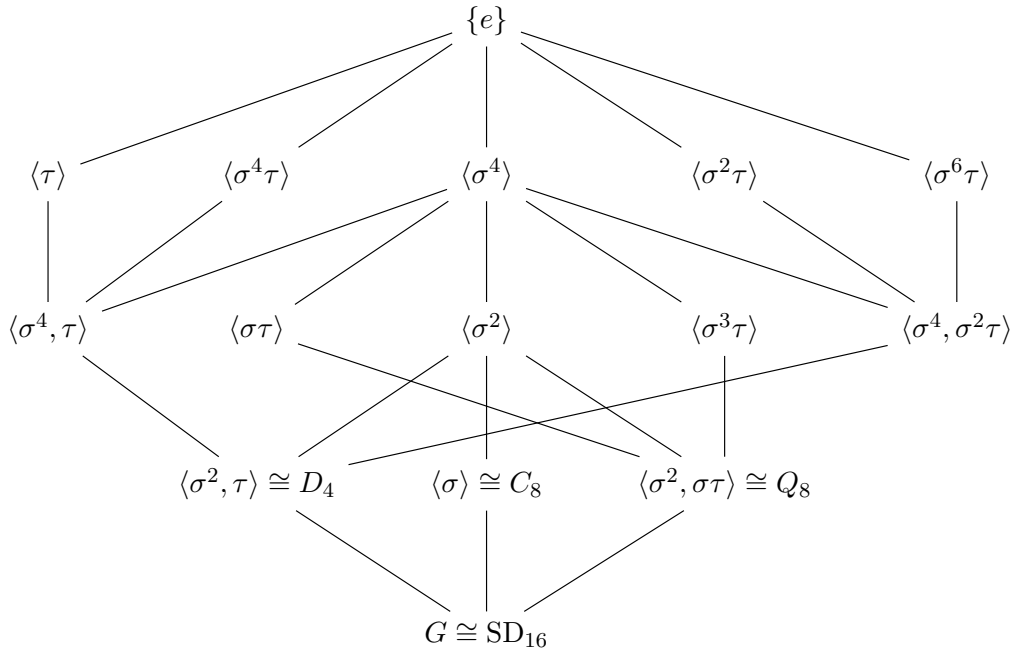
$$H=\left\langle\sigma^4,\tau\right\rangle=\left\{\mathrm{id},\sigma^4,\tau,\sigma^4\tau\right\}. \tag{8.98}$$

  So we have

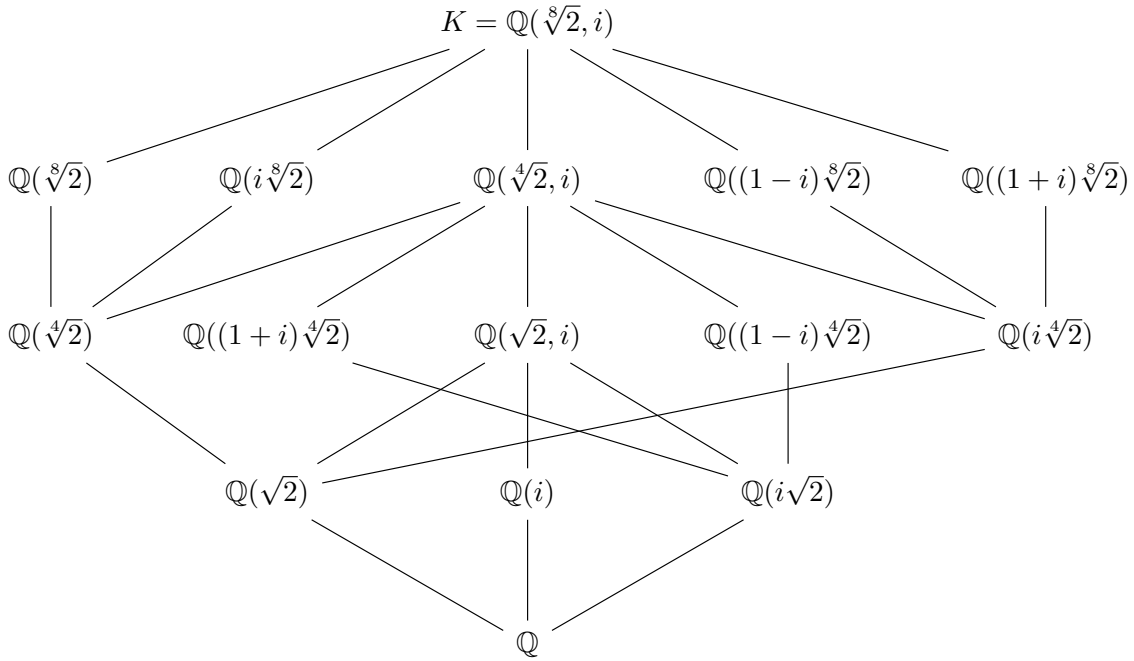
$$\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]=4=[G:H]=[\operatorname{Fix}H:\mathbb{Q}], \tag{8.99}$$

so $\operatorname{Fix} H = \mathbb{Q}\left(\sqrt[4]{2}\right)$.

In fact, the subgroup lattice is




and the corresponding subfield lattice is




■

**Exercise 8.11.** Consider the field extension $\mathbb{C}(t) \subseteq \mathbb{C}(x)$, where $t = x^3 + x^{-3}$.

(a) Determine the degree of the field extension.

(b) Prove that the extension is Galois and compute the Galois group $\mathrm{Gal}(\mathbb{C}(x)/\mathbb{C}(t))$.

(c) Describe all proper intermediate fields of the extension, and for each of them find a primitive element.

*Solution.* **(a)** Note that

$$t = x^3 + \frac{1}{x^3} = \frac{x^6+1}{x^3} \implies x^6 - tx^3 + 1 = 0. \tag{8.100}$$

So $x$ is the root of $P(X) = X^6 - tX^3 + 1 \in \mathbb{C}(t)[X]$. Now, $P(X)$ is irreducible in $\mathbb{C}[X][t]$, since it's a degree-1 polynomial with coprime coefficients. But since $\mathbb{C}[X][t] = \mathbb{C}[t][X]$, so it's irreducible in $\mathbb{C}[t][X]$ as well. Since the field of fraction of $\mathbb{C}[t]$ is $\mathbb{C}(t)$, by Gauss Lemma, $P(X)$ is irreducible in $\mathbb{C}(t)[X]$.

Hence, $x$ is a root of a degree-6 monic irreducible polynomial $P(X)$. Hence, $P(X)$ is the minimal polynomial of $x$ over $\mathbb{C}(t)$. Hence,

$$[\mathbb{C}(x) : \mathbb{C}(t)] = [\mathbb{C}(t)(x) : \mathbb{C}(t)] = \deg P(X) = 6. \tag{8.101}$$

**(b)** Let $\omega = e^{\frac{2\pi i}{3}}$ be a cubic root of unity. The map

$$\begin{aligned} r : \mathbb{C}(x) &\to \mathbb{C}(x) \\ x &\mapsto \omega x \end{aligned} \tag{8.102}$$

is an automorphism of $\mathbb{C}(x)$ that fixes $t$, so it fixes $\mathbb{C}(t)$. Furthermore, the map

$$\begin{aligned} s : \mathbb{C}(x) &\to \mathbb{C}(x) \\ x &\mapsto \frac{1}{x} \end{aligned} \tag{8.103}$$

is also an automorphism of $\mathbb{C}(x)$ fixing $t$. $\operatorname{ord} r = 3$ and $\operatorname{ord} s = 2$. So $r$ and $s$ generate a subgroup of $\operatorname{Aut}(\mathbb{C}(x)/\mathbb{C}(t))$ of order 6. Now,

$$6 \leq |\operatorname{Aut}(\mathbb{C}(x)/\mathbb{C}(t))| \leq [\mathbb{C}(x) : \mathbb{C}(t)] = 6, \tag{8.104}$$

so $\operatorname{Aut}(\mathbb{C}(x)/\mathbb{C}(t)) = \langle r, s\rangle \cong D_3$.

Then $M = \operatorname{Fix}(\operatorname{Aut}(\mathbb{C}(x)/\mathbb{C}(t)))$ is a field extension of $\mathbb{C}(t)$, and $M \leq \mathbb{C}(x)$ is Galois, and $\operatorname{Gal}(\mathbb{C}(x)/M) = \operatorname{Aut}(\mathbb{C}(x)/\mathbb{C}(t))$. But then we have

$$[\mathbb{C}(x) : \mathbb{C}(t)] = [\mathbb{C}(x) : M][M : \mathbb{C}(t)] = |\operatorname{Gal}(\mathbb{C}(x)/M)|[M : \mathbb{C}(t)] \tag{8.105}$$

$$= [\mathbb{C}(x) : \mathbb{C}(t)][M : \mathbb{C}(t)] \tag{8.106}$$

So $M = \mathbb{C}(t)$, i.e. $\mathbb{C}(t) \leq \mathbb{C}(x)$ is Galois, and the Galois group is $\langle r, s\rangle$, isomorphic to $D_3$.

**(c)** The proper subgroups of $D_3$ are cyclic group of order 3, and 2-element subgroups generated by each reflections. In our case, the proper subgroups of $\operatorname{Gal}(\mathbb{C}(x)/\mathbb{C}(t))$ are:

- $\langle r \rangle$. This subgroup has order 3, i.e. index 2. $r$ fixes $x^3$, so the fixed field $M \subseteq \mathbb{C}\left(x^3\right)$. Now,

$$2 = (\text{index of } \langle r \rangle) = [M : \mathbb{C}(t)] = \left[M : \mathbb{C}(x^3)\right] \left[\mathbb{C}\left(x^3\right) : \mathbb{C}(t)\right]. \tag{8.107}$$

  $x^3$ is the root of $X^2 - tX + 1$, and it's irreducible (since it doesn't have any root in $\mathbb{C}(t)$). Therefore, $\left[\mathbb{C}\left(x^3\right) : \mathbb{C}(t)\right] = 2$, so that $M = \mathbb{C}(x^3)$.

- $\left\langle r^j s \right\rangle$, for $j = 0, 1, 2$. This subgroup has order 2, i.e. index 3. It fixes $x + \frac{\omega^{-j}}{x}$, since

$$r^j s\left(x + \frac{\omega^{-j}}{x}\right) = r^j s\left(x\right) + \frac{\omega^{-j}}{r^j s\left(x\right)} = r^j\left(\frac{1}{x}\right) + \frac{\omega^{-j}}{r^j\left(\frac{1}{x}\right)} \tag{8.108}$$

$$= \frac{1}{\omega^j x} + \frac{\omega^j}{\frac{1}{x\omega^j}} = \frac{\omega^{-j}}{x} + x. \tag{8.109}$$

  If $M$ is the fixed field, then $M \subseteq \mathbb{C}\left(x + \frac{\omega^{-j}}{x}\right)$. Now,

$$3 = \left(\text{index of } \left\langle r^j s \right\rangle\right) = [M : \mathbb{C}(t)] = [M : \mathbb{C}\left(y_j\right)] \left[\mathbb{C}\left(y_j\right) : \mathbb{C}(t)\right], \tag{8.110}$$

  where $y_j = x + \frac{\omega^{-j}}{x}$. Then $y_j$ is a root of $X^3 - 3X\omega^{-j} - t$, which is irreducible over $\mathbb{C}(t)$. Hence, $\left[\mathbb{C}\left(y_j\right) : \mathbb{C}(t)\right] = 3$, so that $M = \mathbb{C}\left(y_j\right)$.

■