Solutions to Dummit & Foote's Abstract Algebra 3rd Edition

JR

October 27th, 2025

Contents

Preface

This is a collection of solutions to the exercises in Dummit and Foote's *Abstract Algebra*, 3rd edition. These solutions were written by me as I worked through the book, and are intended to serve as a reference for myself and others who are studying abstract algebra. I have made every effort to ensure the correctness of these solutions, but I cannot guarantee that they are free of errors. If you find any mistakes or have suggestions for improvement, please feel free to contact me.

I've attempted to format the solutions in a clear and consistent manner, using LaTeX for typesetting. Each chapter's exercises are included in separate files for better organization if viewing on GitHub. Moreover, solutions to exercises only utilize techniques that are available to an advanced undergraduate student or beginning graduate student, in line with the intended audience of the textbook. As an aside, I've graduated from a bachelor's program in mathematics but have not pursued graduate studies, so my background is primarily at the undergraduate level.

Some suggestions I've been given to improve the guide are citing particularly important exercises that will prove useful in reading subsequent chapters, and providing writeups/discussions for why I choose a particular method of solution (such as functions/homomorphisms that may appear out of nowhere). Most problems are enclosed in the following environment:

Exercise 0.0.1

Example exercise.

However, there are some exercises that I found to be either challenging, interesting, or useful for the development of later material. These exercises are enclosed in a special environment:

(∗) **Exercise 0.0.2**

Example special exercise.

This is to highlight these exercises for future readers who may want to focus on them.

Many thanks to the authors, David S. Dummit and Richard M. Foote, for writing such an excellent textbook that has been a valuable resource for my recreational studies in abstract algebra. I've received requests on Reddit for individuals to assist me in completing this project, but at this time I prefer to work on it independently. However, I welcome feedback and suggestions from anyone who is interested in contributing to the project in the future.

2 Subgroups

2.1 Definitions and Examples

Exercise 2.1.1

In each of (a)-(e) prove that the specified subset is a subgroup of the given group:

(a) the set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition)

(b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)

(c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)

(d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)

(e) the set of nonzero real numbers whose square is a rational number (under multiplication)

Solution. Let G be the group and H be the subset in equestion.

(a) Since $0 + 0i \in H$, then H is nonempty. For $a + ai, b + bi \in H$,

$$(a + ai) - (b + bi) = (a - b) + (a - b)i \in H$$

so that $H \leq G$.

(b) Since $|1| = 1$, then $1 \in H$ so that it is nonempty. For $z, w \in H$, we first note that $|w^{-1}| = |\overline{w}|/|w|^2 = 1/1 = 1$, where $\overline{w}$ is the complex conjugate of w. Then

$$|zw^{-1}| = |z||w^{-1}| = 1 \cdot 1 = 1$$

so that $zw^{-1} \in H$, hence $H \leq G$.

(c) Fix $n \in \mathbb{Z}^+$. Since $0 = 0/k$ for some k such that $k \mid n$, then $0 \in H$ so that H is nonempty. Let $a/b, c/d \in H$ such that $(a, c) = (b, d) = 1$, and $b \mid n$ and $d \mid n$. Then there exists $x, y \in \mathbb{Z}^+$ such that $bx = n$ and $dy = n$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ax - cy}{n}$$

where reducing this fraction still yields a denominator that divides n. Then $H \leq G$.

(d) Fix $n \in \mathbb{Z}^+$. Since $0 = 0/k$ for some k such that $(k, n) = 1$, then $0 \in H$ so that H is nonempty. Let $a/b, c/d \in H$ such that $(a, c) = 1$, $(b, n) = 1$, and $(d, n) = 1$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$

Assume, by way of contradiction, that $(bd, n) \neq 1$. Then there exists some prime p such that $p \mid bd$ and $p \mid n$. Then $p \mid b$ or $p \mid d$, contradicting our assumption. Then $(bd, n) = 1$ so that $H \leq G$.

(e) Since $1 = 1^1 = 1/1$, then $1 \in H$ so that H is nonempty. For $x, y \in H$, then $x^2, y^2 \in \mathbb{Q}$. Then

$$\left(\frac{x}{y}\right)^2 = \frac{x^2}{y^2} \in \mathbb{Q}$$

so that $x/y \in H$, hence $H \leq G$. ■

Exercise 2.1.2

In each of (a)–(e) prove that the specified subset is *not* a subgroup of the given group:

(a) the set of 2-cycles in S_n for $n \geq 3$

(b) the set of reflections in D_{2n} for $n \geq 3$

(c) for n a composite integer > 1 and G a group containing an element of order n, the set $\{x \in G \mid |x| = n\} \cup \{1\}$

(d) the set of (positive and negative) odd integers in $\mathbb{Z}$ together with 0

(e) the set of real numbers whose square is a rational number (under addition)

Solution. Let G be the group and H be the subset in question.

(a) For $n = 3$, then $(1\ 2), (1\ 3) \in H$, but $(1\ 2)(1\ 3) = (1\ 3\ 2) \notin H$.

(b) For $n = 3$, then $s, sr \in H$, but $s(sr) = r \notin H$.

(c) Let $n = ab$ for some $a, b \in \mathbb{Z}^+$ with $1 < a, b < n$. Let $x \in G$ with $|x| = n$. Then $x \in H$ so that $x^a \in H$, but $(x^a)^b = x^n = 1$ implies that $|x^a| \leq b$ so that $x^a \notin H$.

(d) Observe that $1 \in H$, but $1 + 1 = 2 \notin H$.

(e) Observe that $\sqrt{2}, \sqrt{3} \in H$, but

$$(\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{6} + 3 \notin \mathbb{Q}$$

so that $\sqrt{2} + \sqrt{3} \notin H$. ■

Exercise 2.1.3

Show that the following subsets of the dihedral group D_8 are actually subgroups:

(a) $\{1, r^2, s, sr^2\}$

(b) $\{1, r^2, sr, sr^3\}$

Solution.

(a)

$\circ$	1	r^2	s	sr^2
1	1	r^2	s	sr^2
r^2	r^2	1	sr^2	s
s	s	sr^2	1	r^2
sr^2	sr^2	s	r^2	1

(b)

$\circ$	1	r^2	sr	sr^3
1	1	r^2	sr	sr^3
r^2	r^2	1	sr^3	sr
sr	sr	sr^3	1	r^2
sr^3	sr^3	sr	r^2	1

Both tables show closure, since no product is an element outside of the subset. ■

Exercise 2.1.4

Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.

Solution. Let $G = \mathbb{Z}$ and $H = \mathbb{Z}^+$. Then for any $m, n \in \mathbb{Z}^+$, we have $m + n \in \mathbb{Z}^+$ but $m - n \notin \mathbb{Z}^+$ when $m < n$. Hence, H is not a subgroup of G. ■

Exercise 2.1.5

Prove that G cannot have a subgroup H with $|H| = n-1$, where $n = |G| > 2$.

Solution. Assume, by way of contradiction, that G has a subgroup H where $|H| = n-1$. By Lagrange's Theorem, $|H|$ divides $|G|$, so there exists some $k \in \mathbb{Z}^+$ such that $k(n-1) = kn - k = n$, Equivalently, $n = k/(k-1)$. Since $n > 2$, then $k > 2$. Then $k/(k-1)$ is not an integer, a contradiction. Hence, no such subgroup H exists. ■

(∗) Exercise 2.1.6

Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G). Give an explicit example where this set is not a subgroup when G is non-abelian.

Solution. Denote the set as $\mathrm{Tor}(G)$. Since $|1| = 1$, then $1 \in \mathrm{Tor}(G)$ so that $\mathrm{Tor}(G)$ is nonempty. Suppose $g, h \in \mathrm{Tor}(G)$ where $|g| = m$ and $|h| = n$ for $m, n \in \mathbb{Z}^+$. Then

$$(gh^{-1})^{mn} = g^{mn}(h^{-1})^{mn} = (g^m)^n((h^n)^{-1})^m = 1^n(1^{-1})^m = 1$$

where we use the fact that G is abelian to rearrange the terms. Then $|gh^{-1}| \leq mn < \infty$ so that $gh^{-1} \in \mathrm{Tor}(G)$, hence $\mathrm{Tor}(G) \leq G$.

For a non-abelian example, let $G = \mathrm{Aut}(\mathbb{R})$. Consider the elements $f, g \in G$ defined as $f(x) = -x$ and $g(x) = 1 - x$. Note that $|f| = 2$ and $|g| = 2$, but

$$(fg)(x) = f(g(x)) = f(1-x) = x - 1$$

It is easy to show by induction that $(fg)^n(x) = x - n$ for all $n \in \mathbb{Z}^+$, so that $|fg| = \infty$. Then $fg \notin \mathrm{Tor}(G)$, hence $\mathrm{Tor}(G)$ is not a subgroup of G. ■

Exercise 2.1.7

Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup (cf. the previous exercise) of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements of infinite order together with the identity is *not* a subgroup of this direct product.

Solution. Observe that the only element of finite order in $\mathbb{Z}$ is 0. Moreover, every element of $\mathbb{Z}/n\mathbb{Z}$ is of finite order. Then

$$\mathrm{Tor}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \{(0, \bar{x}) \mid \bar{x} \in \mathbb{Z}/n\mathbb{Z}\}$$

Now consider the set of elements of infinite order together with the identity. Denoting this set as H, observe that $(1,1), (-1,0) \in H$, but

$$(1,1)(-1,0) = (0,1) \notin H$$

since $|(0,1)| = n < \infty$. Hence, H is not a subgroup of $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. ■

Exercise 2.1.8

Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Solution.

* ($\Rightarrow$) Suppose $H \cup K$ is a subgroup. If $H \subseteq K$, then we are done. Suppose that $H \not\subseteq K$. Then there exists some $h \in H$ such that $h \notin K$. Since $H \cup K$ is a subgroup, then for any $k \in K$, we have $hk \in H \cup K$.

  Observe that $k^{-1} \in K$ since $K \leq G$. If $hk \in K$, then $h = (hk)k^{-1} \in K$, contradicting our assumption. It must be that $hk \in H$. Since $h \in H$, then $h^{-1}H$ as $H \leq G$. Then $h^{-1}(hk) = k \in H$, hence $K \subseteq H$.
* ($\Leftarrow$) If $H \subseteq K$, then $H \cup K = K \leq G$. Similarly, if $K \subseteq H$, then $H \cup K = H \leq G$. ■

(∗) Exercise 2.1.9

Let $G = \mathrm{GL}_n(F)$, where F is any field. Define

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) \mid \det(A) = 1\}$$

(called the special linear group). Prove that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$.

Solution. Since $\det(I_n) = 1$, then $I_n \in \mathrm{SL}_n(F)$ so that $\mathrm{SL}_n(F)$ is nonempty. Suppose $A, B \in \mathrm{SL}_n(F)$. Then

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \frac{\det(A)}{\det(B)} = \frac{1}{1} = 1$$

so that $AB^{-1} \in \mathrm{SL}_n(F)$. It follows that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$. ■

Exercise 2.1.10

(a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.
(b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

Solution.

(a) Let $L = H \cap K$. Since $1 \in H$ and $1 \in K$ because $H \leq G$ and $K \leq G$, then $1 \in L$ so that L is nonempty. Suppose $a, b \in L$. Then $a, b \in H$ and $a, b \in K$. Since H and K are subgroups of G, then $ab^{-1} \in H$ and $ab^{-1} \in K$. Hence, $ab^{-1} \in L$, and $L \leq G$.

(b) Let I be an indexing set, and consider the collection of subgroups $\{H_i\}_{i \in I}$ of G. Let

$$H = \bigcap_{i \in I} H_i$$

Since $1 \in H_i$ for all $i \in I$, then $1 \in H$. Suppose $a, b \in H$. Then $a, b \in H_i$ for all $i \in I$. Since each H_i is a subgroup of G, then $ab^{-1} \in H_i$ for all $i \in I$. Hence, $ab^{-1} \in H$, and $H \leq G$. ■

Exercise 2.1.11

Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:

(a) $\{(a, 1) \mid a \in A\}$
(b) $\{(1, b) \mid b \in B\}$
(c) $\{(a, a) \mid a \in A\}$, where we assume $B = A$ (called the diagonal subgroup)

Solution. Let C be the set in each part.

(a) Since $1 \in A$, then $(1, 1) \in C$ so that C is nonempty. Suppose $(a_1, 1), (a_2, 1) \in C$. Then

$$(a_1, 1)(a_2, 1)^{-1} = (a_1, 1)(a_2^{-1}, 1) = (a_1 a_2^{-1}, 1) \in C$$

since $a_1 a_2^{-1} \in A$. Hence, $C \leq A \times B$.

(b) Since $1 \in B$, then $(1, 1) \in C$ so that C is nonempty. Suppose $(1, b_1), (1, b_2) \in C$. Then

$$(1, b_1)(1, b_2)^{-1} = (1, b_1)(1, b_2^{-1}) = (1, b_1 b_2^{-1}) \in C$$

since $b_1 b_2^{-1} \in B$. Hence, $C \leq A \times B$.

(c) Since $1 \in A$, then $(1, 1) \in C$ so that C is nonempty. Suppose $(a_1, a_1), (a_2, a_2) \in C$. Then

$$(a_1, a_1)(a_2, a_2)^{-1} = (a_1, a_1)(a_2^{-1}, a_2^{-1}) = (a_1 a_2^{-1}, a_1 a_2^{-1}) \in C$$

since $a_1 a_2^{-1} \in A$. Hence, $C \leq A \times B$. ■

Exercise 2.1.12

Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:
(a) $\{a^n \mid a \in A\}$
(b) $\{a \in A \mid a^n = 1\}$

Solution. Let B be the sets in question.

(a) Since $1 = 1^n$, then $1 \in B$ so that B is nonempty. Suppose $a^n, b^n \in B$. Then

(b)
$$(a^n)(b^n)^{-1} = a^n b^{-n} = (ab^{-1})^n \in B$$
where the last equality follows from the fact that A is abelian. Hence, $B \leq A$.

(c) Since $1^n = 1$, then $1 \in B$ so that B is nonempty. Suppose $a, b \in B$. Then
$$(ab^{-1})^n = a^n(b^{-1})^n = a^n(b^n)^{-1} = 1 \cdot 1^{-1} = 1$$
where the second equality follows from the fact that A is abelian. Hence, $B \leq A$. ■

Exercise 2.1.13

Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero element x of H. Prove that $H = 0$ or $\mathbb{Q}$.

Solution. Let $H \leq \mathbb{Q}$. Then $0 \in H$. If no other elements are in H, then $H = 0$, and we are done. Suppose there exists some nonzero $a/b \in H$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Moreover, we may assume without loss of generality that $a/b > 0$, for otherwise we may take $-a/b$ since H contains additive inverses. We now use a/b to generate $\mathbb{Q}$.

Since $a/b \in H$, then $b(a/b) = a \in H$ so that $1/a \in H$. Then $a(1/a) = 1 \in H$. From this, we can see that $\mathbb{Z} \subseteq H$. Now let $c/d \in \mathbb{Q}$ for some $c, d \in \mathbb{Z}$ with $d \neq 0$. Since $1 \in H$, then $d(1) = d \in H$ so that $1/d \in H$. Then $c(1/d) = c/d \in H$. Since c/d was arbitrary, then $\mathbb{Q} \subseteq H$. Hence, $H = \mathbb{Q}$. ■

Exercise 2.1.14

Show that $\{x \in D_{2n} \mid x^2 = 1\}$ is *not* a subgroup of D_{2n} (here $n \geq 3$).

Solution. Let H be the set in question. Clearly, $s \in H$. Moreover,
$$(sr)^2 = srsr = ssr^{-1}r = 1$$
so that $|sr| = 2$ and $sr \in H$. However, $s(sr) = r \notin H$ since $|r| = n > 2$. Hence, H is not a subgroup of D_{2n}. ■

Exercise 2.1.15

Let $H_1 \subseteq H_2 \subseteq \cdots$ be an ascending chain of subgroups of G. Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G.

Solution. Let
$$H = \bigcup_{i=1}^{\infty} H_i$$
Since $H_i \leq G$ for each $i \in \mathbb{Z}^+$, then $1 \in H_i$ for all $i \in \mathbb{Z}^+$, hence $1 \in H$ so that H is nonempty. Suppose $a, b \in H$. Then there exists some $m, n \in \mathbb{Z}^+$ such that $a \in H_m$ and $b \in H_n$. Let $k = \max(m, n)$. Since $H_m \subseteq H_k$ and $H_n \subseteq H_k$, then $a, b \in H_k$. Since $H_k \leq G$, then $ab^{-1} \in H_k$, hence $ab^{-1} \in H$. It follows that $H \leq G$. ■

(∗) Exercise 2.1.16

Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in \mathrm{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$ is a subgroup of $\mathrm{GL}_n(F)$ (called the group of upper triangular matrices).

Solution. Let $\mathrm{UT}_n(F)$ denote the set of $n \times n$ upper triangular matrices with entries from F. Observe that I_n contains 0's everywhere except the diagonal, hence $I_n \in \mathrm{UT}_n(F)$ so that $\mathrm{UT}_n(F)$ is nonempty. Suppose $A, B \in \mathrm{UT}_n(F)$, and consider $C = AB$. Then the (i, j)-th entry of C is given by

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Consider the case when $i > j$, which is below the main diagonal.
- If $i > k$, then $a_{ik} = 0$ since A is upper triangular.
- If $k > j$, then $b_{kj} = 0$ since B is upper triangular.

Hence, for all k, either $a_{ik} = 0$ or $b_{kj} = 0$, so that $c_{ij} = 0$. It follows that $C \in \mathrm{UT}_n(F)$.

Let $A \in \mathrm{UT}_n(F)$, and let $D \in \mathrm{GL}_n(F)$ such that $AD = DA = I_n$. We show by induction that $D \in \mathrm{UT}_n(F)$. For the base case, consider $n = 2$. Since we know $A \in \mathrm{UT}_n(F)$ by assumption but do not know about D, we write

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, \quad D = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}, \quad AD = \begin{pmatrix} a_{11}d_{11} + a_{12}d_{21} & a_{11}d_{12} + a_{12}d_{22} \\ a_{22}d_{21} & a_{22}d_{22} \end{pmatrix} = I_2$$

Observe that $a_{22}d_{21} = 0$. Since $a_{22} \neq 0$ because $A \in \mathrm{UT}_2(F) \subseteq \mathrm{GL}_2(F)$, then $d_{21} = 0$, hence $D \in \mathrm{UT}_2(F)$. Now suppose that the inverse of any upper triangular matrix in $\mathrm{GL}_n(F)$ is also upper triangular, and consider $A \in \mathrm{UT}_{n+1}(F)$ and $D \in \mathrm{GL}_{n+1}(F)$ such that $AD = DA = I_{n+1}$. Using block matrices, we may write this as

$$A = \begin{pmatrix} A_0 & \mathbf{a}_{12} \\ 0 & a_{22} \end{pmatrix}, \quad D = \begin{pmatrix} D_0 & \mathbf{d}_{12} \\ \mathbf{d}_{21}^T & d_{22} \end{pmatrix}, \quad AD = \begin{pmatrix} A_0 D_0 & A_0\mathbf{d}_{12} + \mathbf{a}_{12}d_{22} \\ a_{22}\mathbf{d}_{21}^T & a_{22}d_{22} \end{pmatrix} = I_{n+1}$$

where $\mathbf{a}_{12}, \mathbf{d}_{12}, \mathbf{d}_{21}^T$ are $n \times 1$ column vectors, and $a_{22}, d_{22} \in F$. We can see that $A_0 D_0 = I_n$ so that $D_0 \in \mathrm{UT}_n(F)$ by assumption. Moreover, $a_{22}\mathbf{d}_{21}^T = \mathbf{0}_{n\times 1}^T$. Since $a_{22} \neq 0$ because $A \in \mathrm{UT}_{n+1}(F)$, then $\mathbf{d}_{21}^T = \mathbf{0}_{n\times 1}^T$. By induction, then $D \in \mathrm{UT}_{n+1}(F)$, hence the inverse of any upper triangular matrix is also upper triangular. ■

Exercise 2.1.17

Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in \mathrm{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j, \text{ and } a_{ii} = 1 \text{ for all } i\}$ is a subgroup of $\mathrm{GL}_n(F)$.

Solution. Let H be the set in question. Since the diagonal of I_n is only 1's, then $I_n \in H$. Suppose $A, B \in H$. By the previous exercise, $A, B \in \mathrm{UT}_n(F)$, so it remains to show that $a_{ii} = b_{ii} = 1$ for all $1 \leq i \leq n$. Then

$$(AB)_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki}$$

Since $a_{ik} = 0$ for $k < i$ and $b_{ki} = 0$ for $k > i$, then the sum degrades to $a_{ii}b_{ii} = 1$. Then H is closed under multiplication. Moreover, suppose $D \in \mathrm{UT}_n(F)$ such that $DA = I_n$. Then

$$1 = (DA)_{ii} = d_{ii}a_{ii}$$

where we use the above to collapse the ii-th term of DA. Then $d_{ii} = 1$, hence $D \in H$, and H is closed under inverses. Hence, $H \leq \mathrm{GL}_n(F)$. ■

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Exercise 2.2.1

Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

Solution. For any $a \in A \subseteq G$, then $g \in C_G(A)$ if and only if $gag^{-1} = a$ if and only if $ga = ag$ if and only if $g^{-1}ag = a$. Hence, $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$. ■

Exercise 2.2.2

Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Solution. By definition, $C_G(Z(G)) \subseteq G$. Now let $g \in G$ and $z \in Z(G)$. Then $gz = zg$, or $gzg^{-1} = z$. Then $g \in C_G(Z(G))$, hence $G \subseteq C_G(Z(G))$. It follows that $C_G(Z(G)) = G$. Since $C_G(Z(G)) \leq N_G(Z(G)) \leq G$, then $N_G(Z(G)) = G$. ■

Exercise 2.2.3

Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Solution. Pick $g \in C_G(B)$. Then $gbg^{-1} = b$ for all $b \in B$. In particular, $gag^{-1} = a$ for all $a \in A$ because $A \subseteq B$. Then $C_G(B) \subseteq C_G(A)$. Since $C_G(B)$ and $C_G(A)$ are subgroups of G, then $C_G(B) \leq C_G(A)$. ■

(∗) Exercise 2.2.4

For each of S_3, D_8, and Q_8 compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem (Exercise 1.7.19) simplify your work?

Solution. To compute the center of a group G, we need to compute the centralizer of each element in G and then take the intersection of all these centralizers. The proof of this is trivial.

We begin with S_3. It is trivial to see that $C_G(1) = G$ for any group G, since 1 commutes with every element of g. Now consider $(1\,2) \in S_3$, and consider the subgroup $A = \{1, (1\,2)\}$. Since A is a subgroup, then $A \leq C_{S_3}((1\,2))$. By Lagrange's Theorem, then 2 divides $|C_{S_3}((1\,2))|$ and $|C_{S_3}((1\,2))|$ divides 6. Since $(1\,3)(1\,2) = (1\,2\,3) \neq (1\,3\,2) = (1\,2)(1\,3)$, then $(1\,3) \notin C_{S_3}((1\,2))$. By Exercise 1.3.20, we know that $(1\,2)$ and $(1\,3)$ generate S_3 so that $|C_{S_3}((1\,2))| \neq 6$. Then $|C_{S_3}((1\,2))| = 2$ so that $C_{S_3}((1\,2)) = A$. By symmetry, the same argument holds for $(1\,3)$ and $(2\,3)$, so that

$$C_{S_3}((1\,3)) = \{1, (1\,3)\}, \quad C_{S_3}((2\,3)) = \{1, (2\,3)\}$$

Now consider $(1\,2\,3) \in S_3$, and the subgroup $B = \{1, (1\,2\,3), (1\,3\,2)\}$. Since B is a subgroup, then $B \leq C_{S_3}((1\,2\,3))$. By Lagrange's Theorem, then 3 divides $|C_{S_3}((1\,2\,3))|$ and $|C_{S_3}((1\,2\,3))|$ divides 6. Observe that $(1\,2) \notin C_{S_3}((1\,2\,3))$ since $(1\,2)(1\,2\,3) \neq (1\,2\,3)(1\,2)$. Then $|C_{S_3}((1\,2\,3))| \neq 6$, so that $|C_{S_3}((1\,2\,3))| = 3$ and $C_{S_3}((1\,2\,3)) = B$. By symmetry, the same argument holds for $(1\,3\,2)$. Moreover, $Z(G) = \{1\}$.

The following are the centralizers for each element in D_8:

$$\begin{aligned} C_{D_8}(1) &= D_8 & C_{D_8}(r) &= \{1, r, r^2, r^3\} \\ C_{D_8}(r^3) &= \{1, r, r^2, r^3\} & C_{D_8}(r^2) &= D_8 \\ C_{D_8}(sr) &= \{1, r^2, sr, sr^3\} & C_{D_8}(s) &= \{1, r^2, s, sr^2\} \\ C_{D_8}(sr^3) &= \{1, r^2, sr, sr^3\} & C_{D_8}(sr^2) &= \{1, r^2, s, sr^2\} \end{aligned}$$

and $Z(D_8) = \{1, r^2\}$. Lastly, the centralizers of Q_8 are

$$\begin{aligned} C_{Q_8}(1) &= Q_8 & C_{Q_8}(-1) &= Q_8 \\ C_{Q_8}(i) &= \{1, -1, i, -i\} & C_{Q_8}(-i) &= \{1, -1, i, -i\} \\ C_{Q_8}(j) &= \{1, -1, j, -j\} & C_{Q_8}(-j) &= \{1, -1, j, -j\} \\ C_{Q_8}(k) &= \{1, -1, k, -k\} & C_{Q_8}(-k) &= \{1, -1, k, -k\} \end{aligned}$$

and $Z(Q_8) = \{1, -1\}$. ■

Exercise 2.2.5

In each of parts (a) to (c) show that for the specified group G and subgroup A of G, $C_G(A) = A$ and $N_G(A) = G$.

(a) $G = S_3$ and $A = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$.

(b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.

(c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

Solution.

(a) Observe that A is generated by $(1\ 2\ 3)$. From the previous exercise, we know that $C_{S_3}((1\ 2\ 3)) = A$, hence $C_{S_3}(A) = A$. Since $C_G(A) \leq N_G(A)$, we know that 3 divides $|N_G(A)|$ and $|N_G(A)|$ divides 6 by Lagrange's Theorem. Consider $(1\ 2) \in S_3$. Then

$$(1\ 2)A(1\ 2) = \{(1\ 2)(1)(1\ 2), (1\ 2)(1\ 2\ 3)(1\ 2), (1\ 2)(1\ 3\ 2)(1\ 2)\} = \{1, (1\ 3\ 2), (1\ 2\ 3)\} = A$$

so that $(1\ 2) \in N_G(A)$. Then $|N_G(A)| \neq 3$, hence $|N_G(A)| = 6$ and $N_G(A) = G$.

(b) Since $A \subseteq C_G(A)$ is abelian and $C_G(A) \leq G$, then $A \leq G$. Since $|A| = 4$, then 4 divides $|C_G(A)|$ and $|C_G(A)|$ divides 8 by Lagrange's Theorem. Observe that $r \notin C_G(A)$ since $rs = sr^3 \neq sr$. Then $|C_G(A)| \neq 8$, hence $|C_G(A)| = 4$ and $C_G(A) = A$. Since $C_G(A) \leq N_G(A)$, then 4 divides $|N_G(A)|$ and $|N_G(A)|$ divides 8 by Lagrange's Theorem. Consider $r \in D_8$. Then

$$rAr^{-1} = \{r(1)r^{-1}, r(s)r^{-1}, r(r^2)r^{-1}, r(sr^2)r^{-1}\} = \{1, sr^3, r^2, sr\} = A$$

so that $r \in N_G(A)$. Then $|N_G(A)| \neq 4$, hence $|N_G(A)| = 8$ and $N_G(A) = G$.

(c) Since $A \leq C_G(A)$ and $|A| = 5$, then 5 divides $|C_G(A)|$ and $|C_G(A)|$ divides 10 by Lagrange's Theorem. Observe that $s \notin C_G(A)$ since $sr = r^4 s \neq rs$. Then $|C_G(A)| \neq 10$, hence $|C_G(A)| = 5$ and $C_G(A) = A$. Since $C_G(A) \leq N_G(A)$, then 5 divides $|N_G(A)|$ and $|N_G(A)|$ divides 10 by Lagrange's Theorem. Consider $s \in D_{10}$. Then

$$sAs^{-1} = \{s(1)s^{-1}, s(r)s^{-1}, s(r^2)s^{-1}, s(r^3)s^{-1}, s(r^4)s^{-1}\} = \{1, r^4, r^3, r^2, r\} = A$$

so that $s \in N_G(A)$. Then $|N_G(A)| \neq 5$, hence $|N_G(A)| = 10$ and $N_G(A) = G$. ■

Exercise 2.2.6

Let H be a subgroup of the group G.

(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.

(b) Show that $H \leq C_G(H)$ if and only if H is abelian.

Solution.

(a) Our goal is to any element $h \in H$ normalizes H. To that end, fix $h \in H$, and consider $x \in hHh^{-1}$. Then there exists $k \in H$ such that $x = hkh^{-1}$. Since $H \leq G$, then $hkh^{-1} \in H$, hence $x \in H$. It follows that $hHh^{-1} \subseteq H$.

Now consider $y \in H$. Since H is a subgroup, then $h^{-1}yh \in H$. Let $k = h^{-1}yh$. We then obtain $y = hkh^{-1} \in hHh^{-1}$, hence $H \subseteq hHh^{-1}$. It follows that $hHh^{-1} = H$, so that $h \in N_G(H)$. Since h was arbitrary, then $H \leq N_G(H)$.

As a counter example, consider the set $G = D_6$ and $H = \{1, r, s\}$. Then

$$rHr^{-1} = \{1, r, sr^2\} \neq H$$

so that r does not normalize H, and H is not a subgroup of $N_G(H)$.

(b)
- ($\Rightarrow$) Suppose $H \leq C_G(H)$. Then for any $h_1, h_2 \in H$, we have $h_1h_2 = h_2h_1$ since $h_1 \in C_G(H)$. Hence, H is abelian.
- ($\Leftarrow$) Suppose H is abelian, and let $h_1 \in H$. Then for any $h_2 \in H$, we have $h_1h_2 = h_2h_1$, so that $h_1 \in C_G(H)$. Since h_1 was arbitrary, then $H \leq C_G(H)$.

■

Exercise 2.2.7

Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = \{1\}$ if n is odd.

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Solution. We claim that $Z(D_{2n})$ contains no reflections and contains r^i if and only if $n \mid 2i$. To see the first part, suppose $sr^j \in Z(D_{2n})$ for some $0 \leq j < n$. Since it must commute with r, then

$$sr^j r = rsr^j \implies sr^{j+1} = r^{n-1}sr^j \implies sr^{j+1} = sr^{j-1} \implies r^{j+1} = r^{j-1} \implies r^2 = 1$$

which is a contradiction since $n \geq 3$. Hence, no reflections are in $Z(D_{2n})$.

Now consider $r^i \in Z(D_{2n})$ for some $0 \leq i < n$. Since it must commute with s, then

$$r^i s = sr^i \implies r^i s = sr^{n-i} \implies r^i = r^{n-i} \implies r^{2i} = 1$$

so that $n \mid 2i$.

(a) If n is odd, then $n \mid 2i$ implies that $n \mid i$. Since $0 \leq i < n$, then $i = 0$ and $Z(D_{2n}) = \{1\}$.

(b) If $n = 2k$, then $n \mid 2i$ implies that $2k \mid 2i$. Simplifying, we have $k \mid i$. Since $0 \leq i < 2k$, then $i = 0$ or $i = k$, so that $Z(D_{2n}) = \{1, r^k\}$. ■

Exercise 2.2.8

Let $G = S_n$, fix an $i \in \{1, 2, \ldots, n\}$ and let $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ (the stabilizer of i in G). Use group actions to prove that G_i is a subgroup of G. Find $|G_i|$.

Solution. Since $\mathrm{id}(1) = 1$, then $\mathrm{id} \in G_i$ so that G_i is nonempty. Suppose $\sigma \in G_i$. Then $\sigma(i) = i$. Then

$$\sigma^{-1}(i) = \sigma^{-1}(\sigma(i)) = i$$

so that $\sigma^{-1} \in G_i$. Now suppose $\tau \in G_i$. Then $\tau(i) = i$. It follows that

$$(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i) = i$$

so that $\sigma\tau \in G_i$. Hence, $G_i \leq G$.

To find $|G_i|$, observe that any $\sigma \in G_i$ is completely determined by its action on the set $\{1, 2, \ldots, n\} \setminus \{i\}$, which has $n - 1$ elements. Since σ is a permutation, then there are $(n-1)!$ ways to permute these $n - 1$ elements. It follows that $|G_i| = (n-1)!$. ■

Exercise 2.2.9

For any subgroup H of G and any nonempty subset A of G define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).

Solution. Suppose $h \in N_H(A)$. By definition, $hAh^{-1} = A$ and $h \in H$. Then $h \in N_G(A)$ and $h \in H$, so that $h \in N_G(A) \cap H$. It follows that $N_H(A) \subseteq N_G(A) \cap H$.

Now suppose $h \in N_G(A) \cap H$. Then $hAh^{-1} = A$ and $h \in H$. By definition, then $h \in N_H(A)$. It follows that $N_G(A) \cap H \subseteq N_H(A)$. Hence, $N_H(A) = N_G(A) \cap H$. Since $N_G(A) \leq G$ and $H \leq G$, and $N_H(A)$ is the intersection of these two subgroups, then $N_H(A) \leq H$ by Exercise 2.1.10. ■

Exercise 2.2.10

Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

Solution. By assumption, $H = \{1, h\}$ for some $h \in G$ with $h \neq 1$. Since $C_G(H) \leq N_G(H)$, it suffices to show that $N_G(H) \subseteq C_G(H)$. To that end, pick $g \in N_G(H)$. Then $gHg^{-1} = H$, so that

$$gHg^{-1} = \{g(1)g^{-1}, ghg^{-1}\} = \{1, ghg^{-1}\} = H = \{1, h\}$$

It follows that $ghg^{-1} = h$, so that $g \in C_G(H)$. Since g was arbitrary, then $N_G(H) \subseteq C_G(H)$, hence $N_G(H) = C_G(H)$.

Now suppose $N_G(H) = G$. Then $C_G(H) = G$, so that for any $g \in G$, we have $ghg^{-1} = h$. It follows that $hg = gh$ for all $g \in G$, hence $H \leq Z(G)$. ■

Exercise 2.2.11

Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

Solution. Let $z \in Z(G)$. We wish to show that z normalizes A. To that end, consider $x \in zAz^{-1}$. Then there exists $a \in A$ such that $x = zaz^{-1}$. Since $z \in Z(G)$, then $zaz^{-1} = a$, hence $x \in A$. It follows that $zAz^{-1} \subseteq A$.

Now consider $y \in A$. Since $z \in Z(G)$, then $z^{-1}yz = y$. Let $a = z^{-1}yz$. We then obtain $y = zaz^{-1} \in zAz^{-1}$, hence $A \subseteq zAz^{-1}$. It follows that $zAz^{-1} = A$, so that $z \in N_G(A)$. Since z was arbitrary, then $Z(G) \leq N_G(A)$. ■

Exercise 2.2.12

Let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 i.e., the members of R are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$ where a is any integer and $r_1, \ldots, r_4$ are nonnegative integers. For example,

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23} \qquad (*)$$

is a typical element of R. Each $\sigma \in S_4$ gives a permutation of $\{x_1, \ldots, x_4\}$ by defining $\sigma \cdot x_i = x_{\sigma(i)}$. This may be extended to a map from R to R by defining

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

for all $p(x_1, x_2, x_3, x_4) \in R$ (i.e., σ simply permutes the indices of the variables). For example, if $\sigma = (1\,2)(3\,4)$ and $p(x_1, \ldots, x_4)$ is the polynomial in $(*)$ above, then

$$\begin{aligned}\sigma \cdot p(x_1, x_2, x_3, x_4) &= 12x_2^5x_1^7x_4 - 18x_1^3x_4 + 11x_2^6x_1x_4^3x_3^{23} \\ &= 12x_1^7x_2^5x_4 - 18x_1^3x_4 + 11x_1x_2^6x_3^{23}x_4^3.\end{aligned}$$

(a) Let $p = p(x_1, \ldots, x_4)$ be the polynomial in $(*)$ above, let $\sigma = (1\,2\,3\,4)$ and let $\tau = (1\,2\,3)$. Compute $\sigma \cdot p, \tau \cdot (\sigma \cdot p), (\tau \circ \sigma) \cdot p$, and $(\sigma \circ \tau) \cdot p$.

(b) Prove that these definitions give a (left) group action of S_4 on R.

(c) Exhibit all permutations in S_4 that stabilize x_4 and prove that they form a subgroup isomorphic to S_3.

(d) Exhibit all permutations in S_4 that stabilize the element $x_1 + x_2$ and prove that they form an abelian subgroup of order 4.

(e) Exhibit all permutations in S_4 that stabilize the element $x_1x_2 + x_3x_4$ and prove that they form a subgroup isomorphic to the dihedral group of order 8.

(f) Show that the permutations in S_4 that stabilizes the element $(x_1 + x_2)(x_3 + x_4)$ are exactly the same as those found in part (e). (The two polynomials appearing in parts (e) and (f) and the subgroup that stabilizes them will play an important role in the study of roots of quartic equations in Section 14.6.)

Solution.

(a) Note that $\tau \circ \sigma = (1\ 3\ 4\ 2)$ and $\sigma \circ \tau = (1\ 3\ 2\ 4)$. Then

$$\begin{aligned}\sigma \cdot p &= 12x_1x_2^5x_3^7 - 18x_3^3x_4 + 11x_1^{23}x_2^6x_3x_4^3\\ \tau \cdot (\sigma \cdot p) &= 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3\\ (\tau \circ \sigma) \cdot p &= 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3\\ (\sigma \circ \tau) \cdot p &= 12x_1x_3^5x_4^7 - 18x_2x_4^3 + 11x_1^{23}x_2^3x_3^6x_4\end{aligned}$$

(b) Note that $1 \cdot p = p$ for any $p \in R$. Let $\sigma, \tau \in S_4$, then

$$\begin{aligned}\sigma \cdot (\tau \cdot p(x_1, x_2, x_3, x_4)) &= \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, x_{\tau(3)}, x_{\tau(4)})\\ &= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, x_{\sigma(\tau(3))}, x_{\sigma(\tau(4))})\\ &= (\sigma \circ \tau) \cdot p(x_1, x_2, x_3, x_4)\end{aligned}$$

(c) The permutations in S_4 that stabilize x_4 are those that fix 4 and permute $\{1, 2, 3\}$. These are exactly the elements of the subgroup

$$G = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

which is clearly isomorphic to S_3.

(d) To stabilize $x_1 + x_2$, a permutation must either fix both 1 and 2 or swap them. The permutations that do this are

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

which is abelian since every nonidentity element has order 2. Moreover, $|H| = 4$.

(e) To stabilize $x_1x_2 + x_3x_4$, a permutation must either swap 1 and 2 or fix them, and either swap 3 and 4 or fix them. Additionally, it may swap the pairs (1 2) and (3 4). The permutations that do this are

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

It is straightforward to see that K is generated by (1 2) and (1 3 2 4). Consider the mapping $\varphi : D_8 \to K$ defined by

$$\varphi(r) = (1\ 3\ 2\ 4), \quad \varphi(s) = (1\ 2)$$

Since $\varphi(r)^4 = \varphi(s)^2 = 1$ and $\varphi(s)\varphi(r) = (1\ 2)(1\ 3\ 2\ 4) = (1\ 4)(2\ 3) = \varphi(r)^{-1}\varphi(s)$, then φ is a homomorphism. Since φ is clearly surjective and $|D_8| = |K| = 8$, then φ is an isomorphism, so that $K \cong D_8$.

(f) The permutations that stabilize $(x_1 + x_2)(x_3 + x_4)$ must either swap 1 and 2 or fix them, and either swap 3 and 4 or fix them. Additionally, it may swap the pairs (1 2) and (3 4). These are exactly the same permutations found in part (e). ■

Exercise 2.2.13

Let n be a positive integer and let R be the set of all polynomials with integer coefficients in the independent variables $x_1, x_2, \ldots, x_n$, i.e., the members of R are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$ where a is any integer and $r_1, \ldots, r_n$ are nonnegative integers. For each $\sigma \in S_n$ define a map

$$\sigma : R \to R \quad \text{by} \quad \sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

Prove that this defines a (left) group action of S_n on R.

Solution. Since $\mathrm{id}(i) = i$ for all $1 \le i \le n$, then $\mathrm{id} \cdot p = p$ for any $p \in R$. Let $\sigma, \tau \in S_n$, then

$$\begin{aligned}\sigma \cdot (\tau \cdot p(x_1, x_2, \ldots, x_n)) &= \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)})\\ &= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))})\\ &= (\sigma \circ \tau) \cdot p(x_1, x_2, \ldots, x_n)\end{aligned}$$

Hence, this defines a (left) group action of S_n on R. ■

Exercise 2.2.14

Let $H(F)$ be the Heisenberg group over the field F introduced in Exercise 1.4.11. Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group F.

Solution. Let $X, Y \in H(F)$ be written as

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

where $X \in Z(H(F))$. Then $XY = YX$, implying that

$$XY = \begin{pmatrix} 1 & a+d & af+b+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & dc+e+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} = YX$$

so that $af + b + e = dc + e + b$. Simplifying, we have $af = dc$. Since this must hold for all $d, f \in F$, then $a = 0$ and $c = 0$. It follows that

$$Z(H(F)) = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, x \in F \right\}$$

Moreover, the mapping $\varphi : F \to Z(H(F))$ defined by

$$\varphi(x) = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is clearly surjective. If $\varphi(x) = I_3$, then $x = 0$, so that φ is injective. Finally, for any $x, y \in F$, we have

$$\varphi(x+y) = \begin{pmatrix} 1 & 0 & x+y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \varphi(x)\varphi(y)$$

so that φ is a homomorphism. Hence, φ is an isomorphism, and $F \cong Z(H(F))$. ■

2.3 Cyclic Groups and Cyclic Subgroups

Exercise 2.3.1

Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

Solution. Recall that the containment relation is the following:

$$\langle x^a \rangle \leq \langle x^b \rangle \iff (b, 45) \mid (a, 45)$$

The subgroups of Z_{45} are:

$$\begin{aligned} Z_{45} = \langle x \rangle &> \langle x^3 \rangle, \langle x^5 \rangle, \langle x^9 \rangle, \langle x^{15} \rangle, 1 \\ \langle x^3 \rangle &> \langle x^9 \rangle, \langle x^{15} \rangle \\ \langle x^5 \rangle &> \langle x^{15} \rangle \\ \langle x^9 \rangle &> 1 \\ \langle x^{15} \rangle &> 1 \\ 1 = \langle x^0 \rangle & \end{aligned}$$

■

Exercise 2.3.2

If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.

Solution. For some $x \in G$ where $|x| = |G| = n$, then Proposition 2.2 says that $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of G. Since G has n elements only, it follows that these are the elements of G, hence $G = \langle x \rangle$. Moreover, this is not true if G is infinite, since $|\mathbb{Z}| = |2| = \infty$, but $\langle 2 \rangle$ generates only the even integers. ■

Exercise 2.3.3

Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Solution. Using Proposition 2.5 and $|\mathbb{Z}/48\mathbb{Z}| = 48$, then $\langle \overline{a} \rangle$ generates $\mathbb{Z}/48\mathbb{Z}$ when $(a, 48) = 1$. We have the integers

$$a \in \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\}$$

■

Exercise 2.3.4

Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Solution. Note that $202 = 2 \cdot 101$, which are both prime numbers. Then its generators is every number between 1 and 202, except 101 and even numbers. ■

Exercise 2.3.5

Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Solution. Let φ denote the Euler-φ function. Then

$$\begin{aligned} \varphi(49000) &= \varphi(2^3)\varphi(5^3)\varphi(7^2) \\ &= 2^2(2-1)5^2(5-1)7(7-1) \\ &= 16800 \end{aligned}$$

■

Exercise 2.3.6

In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \bar{a} \rangle$ for every $\bar{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

Solution. The elements of each subgroup are

$$\begin{aligned}
\mathbb{Z}/48\mathbb{Z} = \langle \bar{1} \rangle &= \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{46}, \overline{47}\} & \langle \bar{2} \rangle &= \{\bar{0}, \bar{2}, \bar{4}, \ldots, \overline{44}, \overline{46}\} \\
\langle \bar{3} \rangle &= \{\bar{0}, \bar{3}, \bar{6}, \ldots, \overline{42}, \overline{45}\} & \langle \bar{4} \rangle &= \{\bar{0}, \bar{4}, \bar{8}, \ldots, \overline{40}, \overline{44}\} \\
\langle \bar{6} \rangle &= \{\bar{0}, \bar{6}, \overline{12}, \ldots, \overline{36}, \overline{42}\} & \langle \bar{8} \rangle &= \{\bar{0}, \bar{8}, \overline{16}, \overline{24}, \overline{32}, \overline{40}\} \\
\langle \overline{12} \rangle &= \{\bar{0}, \overline{12}, \overline{24}, \overline{36}\} & \langle \overline{16} \rangle &= \{\bar{0}, \overline{16}, \overline{32}\} \\
\langle \overline{24} \rangle &= \{\bar{0}, \overline{24}\} & \langle \bar{0} \rangle &= \{\bar{0}\}
\end{aligned}$$

Moreover, the subgroup inclusions are

$$\begin{aligned}
\langle \bar{1} \rangle &\geq \langle \bar{0} \rangle, \langle \bar{1} \rangle, \langle \bar{2} \rangle, \langle \bar{3} \rangle, \langle \bar{4} \rangle, \langle \bar{6} \rangle, \langle \bar{8} \rangle, \langle \overline{12} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle \\
\langle \bar{2} \rangle &\geq \langle \bar{0} \rangle, \langle \bar{2} \rangle, \langle \bar{4} \rangle, \langle \bar{6} \rangle, \langle \bar{8} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle \\
\langle \bar{3} \rangle &\geq \langle \bar{3} \rangle, \langle \bar{6} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle \\
\langle \bar{4} \rangle &\geq \langle \bar{0} \rangle, \langle \bar{4} \rangle, \langle \bar{8} \rangle, \langle \overline{12} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle \\
\langle \bar{6} \rangle &\geq \langle \bar{0} \rangle, \langle \bar{6} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle \\
\langle \bar{8} \rangle &\geq \langle \bar{0} \rangle, \langle \bar{8} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle \\
\langle \overline{12} \rangle &\geq \langle \bar{0} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle \\
\langle \overline{16} \rangle &\geq \langle 0 \rangle, \langle \bar{16} \rangle \\
\langle \overline{24} \rangle &\geq \langle 0 \rangle, \langle \overline{24} \rangle \\
\langle \bar{0} \rangle &\geq \langle \bar{0} \rangle
\end{aligned}$$

■

Exercise 2.3.7

Let $Z_{48} = \langle x \rangle$ and use the isomorphism $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$ given by $\bar{1} \mapsto x$ to list all subgroups of Z_{48} as computed in the preceding exercise.

Solution. The subgroups of Z_{48} are $\langle x \rangle, \langle x^2 \rangle, \langle x^3 \rangle, \langle x^4 \rangle, \langle x^6 \rangle, \langle x^8 \rangle, \langle x^{12} \rangle, \langle x^{16} \rangle, \langle x^{24} \rangle$, and 1. ■

Exercise 2.3.8

Let $Z_{48} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \bar{1} \mapsto x^a$ extend to an isomorphism from $\mathbb{Z}/48\mathbb{Z}$ to Z_{48}?

Solution. We know that $\bar{1}$ generates $\mathbb{Z}/48\mathbb{Z}$. By Theorem 2.4, φ_a extends to an isomorphism if and only if x^a generates Z_{48}. By Proposition 2.5, this occurs if and only if $(a, 48) = 1$. Hence, the integers a such that φ_a extends to an isomorphism are

$$a \in \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\}$$

■

Exercise 2.3.9

Let $Z_{36} = \langle x \rangle$. For which integers a does the map ψ_a defined by $\psi_a : \bar{1} \mapsto x^a$ extend to a *well defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ into Z_{36}. Can ψ_a ever be a surjective homomorphism?

Solution. Suppose $\bar{r}, \bar{s} \in \mathbb{Z}/48\mathbb{Z}$ such that $\bar{r} = \bar{s}$. Then $r \equiv s \bmod 48$, or $48 \mid (r-s)$. If ψ_a is well defined, then

$$\psi_a(\bar{r}) = \psi_a(r \cdot \bar{1}) = x^{ar} = x^{as} = \psi_a(s \cdot \bar{1}) = \psi_a(\bar{s})$$

so that $x^{a(r-s)} = 1$. Since $|x| = 36$, then $36 \mid a(r-s)$. Since $48 \mid (r-s)$, there exists some integer k such that $r - s = 48k$. It follows that $36 \mid 48ak$, or $3 \mid 4ak$. Since $3 \nmid 4$, then $3 \mid ak$. If $3 \nmid a$, then $3 \mid k$. But this need not be true for all integers k. Hence, we must have $3 \mid a$.

Now suppose ψ_a is surjective. Then $\langle x^a \rangle = Z_{36}$, so that $(a, 36) = 1$ by Proposition 2.5. But this contradicts the previous result that $3 \mid a$. Hence, ψ_a can never be surjective. ■

Exercise 2.3.10

What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all of the elements and their orders in $\langle \overline{30} \rangle$.

Solution. By Proposition 2.5, we have $|\bar{1}| = 54$. Then

$$|\overline{30}| = |30 \cdot \bar{1}| = \frac{54}{(54, 30)} = \frac{54}{6} = 9$$

The first element of order 9 in $\mathbb{Z}/54\mathbb{Z}$ is $\bar{6}$, so

$$\langle \overline{30} \rangle = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}\}$$

Moreover, the orders are

$$\begin{array}{lll} |\bar{0}| = 1 & |\bar{6}| = 9 & |\overline{12}| = 9 \\ |\overline{18}| = 3 & |\overline{24}| = 9 & |\overline{30}| = 9 \\ |\overline{36}| = 3 & |\overline{42}| = 9 & |\overline{48}| = 9 \end{array}$$

■

Exercise 2.3.11

Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.

Solution. The cyclic subgroups of D_8 are

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle r \rangle = \langle r^3 \rangle &= \{1, r, r^2, r^3\} \\ \langle r^2 \rangle &= \{1, r^2\} \\ \langle s \rangle &= \{1, s\} \\ \langle sr \rangle &= \{1, sr\} \\ \langle sr^2 \rangle &= \{1, sr^2\} \\ \langle sr^3 \rangle &= \{1, sr^3\} \end{aligned}$$

Moreover, a proper subgroup that is not cyclic is $\langle r^2, s \rangle = \{1, r^2, s, sr^2\}$. ■

Exercise 2.3.12

Prove that the following groups are *not* cyclic:
(a) $Z_2 \times Z_2$ (b) $Z_2 \times \mathbb{Z}$ (c) $\mathbb{Z} \times \mathbb{Z}$

Solution.

(a) Put $Z_2 = \langle x \rangle$. We may inspect all four elements:

$$\begin{aligned}\langle (1,1) \rangle &= \{(1,1)\} \\ \langle (x,1) \rangle &= \{(1,1),(x,1)\} \\ \langle (1,x) \rangle &= \{(1,1),(1,x)\} \\ \langle (x,x) \rangle &= \{(1,1),(x,x)\}\end{aligned}$$

No subgroup has order 4, hence no subgroup generates $Z_2 \times Z_2$.

(b) If (a,b) generates $Z_2 \times \mathbb{Z}$, then it must be one of the forms $(1,\pm 1)$ or $(x,\pm 1)$, since $\langle \pm 1 \rangle = \mathbb{Z}$. But $(1,\pm 1)$ generates elements whose first component is only 1. If we consider $(x,\pm 1)$, then this also doesn't generate $Z_2 \times \mathbb{Z}$ since $(1,1) \notin \langle (x,\pm 1) \rangle$.

(c) The only candidates for generators of $\mathbb{Z} \times \mathbb{Z}$ is $(\pm 1, \pm 1)$. But any subgroup generated by $(\pm 1, \pm 1)$ contain elements that differ only in sign as $(x,y) \notin \langle (\pm 1, \pm 1) \rangle$ when $|x| \neq |y|$. ■

Exercise 2.3.13

Prove that the following pairs of groups are *not* isomorphic:
(a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$ (b) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$.

Solution.

(a) $(0,x) \in \mathbb{Z} \times Z_2$ has order 2, but no element in $\mathbb{Z}$ has order 2.

(b) Same reason as above. ■

Exercise 2.3.14

Let $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. For each of the following integers a compute σ^a:
$a = 13, 65, 626, 1195, -6, -81, -570$, and -1211.

Solution. Since $|\sigma| = 12$, then we know that $\langle \sigma \rangle$ has 12 distinct elements. We may then use the Division Algorithm to reduce the integers to their least residue:

$$\begin{aligned}\sigma^{13} &= \sigma^{12+1} = \sigma \\ \sigma^{65} &= \sigma^{5(12)+5} = \sigma^5 = (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8) \\ \sigma^{626} &= \sigma^{52(12)+2} = \sigma^2 = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12) \\ \sigma^{1195} &= \sigma^{99(12)+7} = \sigma^7 = (1\ 8\ 3\ 10\ 5\ 12\ 7\ 2\ 9\ 4\ 11\ 6) \\ \sigma^{-6} &= \sigma^{-1(12)+6} = \sigma^6 = (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12) \\ \sigma^{-81} &= \sigma^{-7(12)+3} = \sigma^3 = (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12) \\ \sigma^{-570} &= \sigma^{-48(12)+6} = \sigma^6 \\ \sigma^{-1211} &= \sigma^{-101(12)+1} = \sigma\end{aligned}$$

■

Exercise 2.3.15

Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Solution. If it were cyclic, then all subgroups are also cyclic, by Theorem 2.7. But $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. ■

Exercise 2.3.16

Assume $|x| = n$ and $|y| = m$. Suppose that x and y *commute*: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true of x and y do *not* commute? Give an example of commuting elements x and y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

Solution. Let ℓ be the least common multiple of m and n. Then there exist $a, b \in \mathbb{Z}$ such that $\ell = am = bn$. Then

$$(xy)^\ell = x^\ell y^\ell = x^{bn} y^{am} = 1 \cdot 1 = 1$$

so that by Proposition 2.3, then $|xy|$ divides ℓ. Moreover, this is not true if x and y do not commute. If we consider $r, s \in D_8$, then $|r| = 4$ and $|s| = 2$, but $|rs| = 2$ which 4 does not divide. ■

Exercise 2.3.17

Find a presentation for Z_n with one generator.

Solution. $Z_n = \langle x \mid x^n = 1 \rangle$. ■

Exercise 2.3.18

Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x \rangle$ to h such that $x \mapsto h$.

Solution. Define the map $\varphi : Z_n \to H$ as

$$\varphi(x^k) = h^k$$

Then $\varphi(x) = h$. To show that φ is well defined, suppose $x^a = x^b$ for some $a, b \in \mathbb{Z}$. Then $n \mid (a - b)$, or $a - b = nk$ for some $k \in \mathbb{Z}$. It follows that

$$\varphi(x^a) = h^a = h^{b+nk} = h^b (h^n)^k = h^b \cdot 1 = h^b = \varphi(x^b)$$

so that φ is well defined. Moreover,

$$\varphi(x^{a+b}) = h^{a+b} = h^a h^b = \varphi(x^a)\varphi(x^b)$$

so that φ is a homomorphism. Lastly, if $\psi : Z_n \to H$ is another homomorphism such that $\psi(x) = h$, it must satisfy $\psi(x^k) = \psi(x)^k = h^k$. This shows that $\psi = \varphi$. ■

Exercise 2.3.19

Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.

Solution. Define the map $\varphi : \mathbb{Z} \to H$ as

$$\varphi(n) = h^n$$

Then $\varphi(1) = h$. Moreover, for any $s, t \in \mathbb{Z}$, then

$$\varphi(s + t) = h^{s+t} = h^s h^t = \varphi(s)\varphi(t)$$

so that φ is a homomorphism. Lastly, if $\psi : \mathbb{Z} \to H$ is another homomorphism such that $\psi(1) = h$, it must satisfy $\psi(n) = \psi(n \cdot 1) = \psi(1)^n = h^n$. ■

Exercise 2.3.20

Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$, then $|x| = p^m$ for some $m \leq n$.

Solution. If $x^{p^n} = 1$, then Proposition 2.3 says that $|x|$ divides p^n. Since p is prime, then $|x|$ must also be a power of p that is at most n. ■

(∗) Exercise 2.3.21

Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$ but $(1+p)^{p^{n-2}} \not\equiv 1 \bmod p^n$. Deduce that $1+p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Solution. By the Binomial Theorem, then

$$(1+p)^{p^{n-1}} = \sum_{k=0}^{p^{n-1}} \binom{p^{n-1}}{k} p^k = 1 + p^n + \sum_{k=2}^{p^{n-1}-2} \binom{p^{n-1}}{k} p^k$$

Observe that for $k \geq 2$, the binomial coefficient is

$$\binom{p^{n-1}}{k} = \frac{p^{n-1}(p^{n-1}) \cdots (p^{n-1}-k+1)}{k!}$$

where we note that the denominator $k!$ contains at most p^{k-1} as a factor since p is prime. Then the numerator contains at least p^{n-1} as a factor, so that the entire term contains at least $p^{n-1-(k-1)} = p^{n-k}$ as a factor. Since this is multiplied by p^k in the summation, then each term for $k \geq 2$ contains at least p^n as a factor, so that $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$.

Now consider $(1+p)^{p^{n-2}}$. Using the Binomial Theorem again, we have

$$(1+p)^{p^{n-2}} = \sum_{k=0}^{p^{n-2}} \binom{p^{n-2}}{k} p^k = 1 + p^{n-1} + \sum_{k=2}^{p^{n-2}-2} \binom{p^{n-2}}{k} p^k$$

While the rest of the summation terms are divisible by p^n like before, the $k=1$ term is p^{n-1} which is not divisible by p^n. Hence, $(1+p)^{p^{n-2}} \not\equiv 1 \bmod p^n$. Since the only integers that divide p^n are $1, p, p^2, \ldots, p^n$, and the first power that results in $1 \bmod p^n$ is p^{n-1}, it follows that the order of $1+p$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is p^{n-1}. ■

(∗) Exercise 2.3.22

Let n be an integer ≥ 3. Use the Binomial Theorem to show that $(1+2^2)^{2^{n-2}} \equiv 1 \bmod 2^n$ but $(1+2^2)^{2^{n-3}} \not\equiv 1 \bmod 2^n$. Deduce that 5 is an element of order 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Solution. The process is similar to the previous exercise, where we use the Binomial Theorem to expand $(1+2^2)^{2^{n-2}}$ and see that $k=0$ and $k=1$ terms are 1 and 2^n respectively. For $k \geq 2$, we have the summand as

$$\binom{2^{n-2}}{k} 2^{2k} = \frac{2^{n-2}(2^{n-2}-1)\cdots(2^{n-2}-k+1)}{k!} 2^{2k}$$

Using the formula obtained in Exercise 0.2.8, note that the largest power of 2 that $k!$ divides is $k-1$. Then $k!$ contains at most 2^{k-1} as a factor, while the numerator contains at least 2^{n-1} as a factor. Along with 2^{2k}, the entire term contains at least $2^{n-1-(k-1)+2k} = 2^{n+k}$ as a factor. Since $k \geq 2$, then $n+k \geq n+2 > n$, so that each term for $k \geq 2$ contains at least 2^n as a factor. Hence, $(1+2^2)^{2^{n-2}} \equiv 1 \bmod 2^n$ as desired. Moreover, considering $(1+2^2)^{2^{n-3}}$, the $k=1$ term is 2^{n-1} which is not divisible by 2^n. Hence, $(1+2^2)^{2^{n-3}} \not\equiv 1 \bmod 2^n$. Since the only integers that divide 2^n are $1, 2, 2^2, \ldots, 2^n$, and the first power that results in $1 \bmod 2^n$ is 2^{n-2}, it follows that the order of 5 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is 2^{n-2}. ■

Exercise 2.3.23

Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]

Solution. By Theorem 2.7, we must have one subgroup of order 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ if it were cyclic. However,

$$(2^n - 1)^2 = (-1)^2 \equiv 1 \bmod 2^n$$

and

$$(2^{n-1} + 1)^2 = 2^{2n-2} + 2^n + 1 \equiv 1 \bmod 2^n$$

Since $n \geq 3$, then $2^n - 1 \neq 2^{n-1} + 1$ but both have order 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Hence, it cannot be cyclic. ■

Exercise 2.3.24

Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$. [Show first that $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n, show that the elements $gx^ig^{-1}, i = 0, 1, \ldots, n-1$ are distinct, so that $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and conclude that $g\langle x \rangle g^{-1} = \langle x \rangle$.]

Note that this cuts down some of the work in commuting normalizers of cyclic subgroups since one does not have to check $ghg^{-1} \in \langle x \rangle$ for every $h \in \langle x \rangle$.

Solution.

(a) If $g \in N_G(\langle x \rangle)$, then $g\langle x \rangle g^{-1} = \langle x \rangle$. In particular, $gxg^{-1} \in \langle x \rangle$, so there exists some $a \in \mathbb{Z}$ such that $gxg^{-1} = x^a$.

(b) Suppose $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$. We first show that $gx^kg^{-1} = (gxg^{-1})^k$ by induction. For $k = 1$, the result is trivial. Suppose it holds for some $k \geq 1$. Then

$$gx^{k+1}g^{-1} = gx^kg^{-1}gxg^{-1} = (gxg^{-1})^k(gxg^{-1}) = (gxg^{-1})^{k+1}$$

so that the result holds for all positive integers k. For negative integers, observe that $(gxg^{-1})^{-1} = gx^{-1}g^{-1}$. Using the above result for all positive integers, we may extend it to negative integers as well.

Now, for any integer k, we have

$$gx^kg^{-1} = (gxg^{-1})^k = (x^a)^k = x^{ak}$$

so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. Since conjugation is an isomorphism, it is trivial to see that $|x| = |gxg^{-1}|$. If $|x| = n$, then the elements gx^ig^{-1} for $i = 0, 1, \ldots, n-1$ are distinct since if $gx^ig^{-1} = gx^jg^{-1}$ for some $0 \leq i < j \leq n-1$, then $x^i = x^j$ which contradicts the order of x. Hence, $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$, so that $g\langle x \rangle g^{-1} = \langle x \rangle$. Therefore, $g \in N_G(\langle x \rangle)$. ■

Exercise 2.3.25

Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem to prove that the same is true for any finite group of order n. (For such k each element has a kth root in G. It follows from Cauchy's Theorem in Section 3.2 that if k is not relatively prime to the order of G then the map $x \mapsto x^k$ is not surjective.)

Solution. Fix $k \in \mathbb{Z}^+$ such that $(k, n) = 1$. Since G is cyclic, then $G = \langle x \rangle$ for some $x \in G$. For any $y \in G$, there exists some integer m such that $y = x^m$. Since $(k, n) = 1$, there exist integers s, t such that $ks + nt = 1$. Then

$$\varphi(x^{ms}) = x^{kms} = x^{m(1-nt)} = x^m(x^n)^{-mt} = x^m \cdot 1 = y$$

so that φ is surjective.

Now let G be any finite group of order n. For any $y \in G$, consider the subgroup $\langle y \rangle$. If $|\langle y \rangle| = m$, then by Lagrange's Theorem, $m \mid n$. Since $(k, n) = 1$, then $(k, m) = 1$ as well. By the previous result, there exists some $z \in \langle y \rangle$ such that $z^k = y$. Hence, the map $x \mapsto x^k$ is surjective. ■

(∗) Exercise 2.3.26

Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \to Z_n \quad \text{by} \quad \sigma_a(x) = x^a \text{ for all } x \in Z_n$$

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime.
(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \bmod n$.
(c) Prove that *every* automorphism of Z_n is equal to σ_a for some integer a.
(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$).

Solution.

(a) • ($\Rightarrow$) Suppose $\sigma_a \in \mathrm{Aut}(Z_n)$, and let $d = (n, a)$. Assume, by way of contradiction, that $d \neq 1$. Then there are $s, t \in \mathbb{Z}$ such that $n = ds$ and $a = dt$. Let $Z_n = \langle x \rangle$. Then

$$\varphi(x^s) = x^{as} = x^{dts} = x^{ns} = 1$$

If $x^s \neq 1$, then $\ker \sigma_a$ would be non-trivial, contradicting that σ_a is an automorphism. Hence, $x^s = 1$, and since $|x| = n$ and $n \mid s$, then $s = n$ so that $d = 1$.

• ($\Leftarrow$) Suppose that $(a, n) = 1$. By the previous exercise, then σ_a is a surjective map. Since Z_n is finite, then σ_a is also bijective. Moreover,

$$\sigma_a(xy) = (xy)^a = x^a y^a = \sigma_a(x)\sigma_a(y)$$

for some $x, y \in Z_n$. Then σ_a is also a homomorphism, hence $\sigma_a \in \mathrm{Aut}(Z_n)$.

(b) • ($\Rightarrow$) Suppose $\sigma_a = \sigma_b$. Let $Z_n = \langle x \rangle$. Then

$$x^a = \sigma_a(x) = \sigma_b(x) = x^b$$

so that $n \mid (a - b)$, or $a \equiv b \bmod n$.

• ($\Leftarrow$) Suppose $a \equiv b \bmod n$. Then there exists some integer k such that $a - b = nk$. Let $Z_n = \langle x \rangle$. For any $x^m \in Z_n$, we have

$$\sigma_a(x^m) = x^{am} = x^{(b+nk)m} = x^{bm}(x^n)^{km} = x^{bm} \cdot 1 = \sigma_b(x^m)$$

so that $\sigma_a = \sigma_b$.

(c) Let $Z_n = \langle x \rangle$ and let $\varphi \in \mathrm{Aut}(Z_n)$. Since φ is surjective, then there exists some integer a such that $\varphi(x) = x^a$. For any $x^m \in Z_n$, we have

$$\varphi(x^m) = \varphi(x)^m = (x^a)^m = x^{am} = \sigma_a(x^m)$$

so that $\varphi = \sigma_a$.

(d) Let $Z_n = \langle x \rangle$. For any $x^m \in Z_n$, we have

$$\sigma_a \circ \sigma_b(x^m) = \sigma_a(x^{bm}) = x^{abm} = \sigma_{ab}(x^m)$$

so that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Consider the map

$$\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n) \quad \text{by} \quad \varphi(\overline{a}) = \sigma_a$$

By part (b), φ is well defined. Part (a) shows that φ is injective, while part (c) shows that φ is surjective. The first part of (d) shows that φ is a homomorphism. Hence, φ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto $\mathrm{Aut}(Z_n)$. ■

2.4 Subgroups Generated by Subsets of a Group

Exercise 2.4.1

Prove that if H is a subgroup of G then $\langle H\rangle = H$.

Solution. It is clear that $H \subseteq \langle H\rangle$. Recall that $\langle H\rangle$ is the intersection of all subgroups of G that contain H. Since H is itself a subgroup of G that contains H, then $\langle H\rangle \subseteq H$. Hence, $\langle H\rangle = H$. ■

Exercise 2.4.2

Prove that if A is a subset of B then $\langle A\rangle \leq \langle B\rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A\rangle = \langle B\rangle$.

Solution. Since $\langle B\rangle$ is the smallest subgroup of G that contains B, and $A \subseteq B$, then $A \subseteq \langle B\rangle$. Since $\langle A\rangle$ is the smallest subgroup of G that contains A, then $\langle A\rangle \subseteq \langle B\rangle$, so that $\langle A\rangle \leq \langle B\rangle$.

For an example, consider $G = \mathbb{Z}$, $A = \langle 1\rangle$, and $B = \{1, 2\}$. Then $A \subset B$ but $A \neq B$, and $\langle A\rangle = \langle B\rangle = \mathbb{Z}$. ■

Exercise 2.4.3

Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G)\rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H)\rangle$ is not abelian.

Solution. Let $g, h \in \langle H, Z(G)\rangle$. Using Proposition 2.9, we may put them as follows:

$$g = g_1^{\epsilon_1} g_2^{\epsilon_2} \dots g_m^{\epsilon_m}, \quad h = h_1^{\delta_1} h_2^{\delta_2} \dots h_n^{\delta_n}$$

where $\epsilon_i = \delta_i = \pm 1$, and $g_i, h_i \in H \cup Z(G)$ for all i. Since both H and $Z(G)$ are abelian, then elements of H and $Z(G)$ commute with each other. Then

$$gh = g_1^{\epsilon_1} \dots g_m^{\epsilon_m} h_1^{\delta_1} \dots h_n^{\delta_n} = h_1^{\delta_1} \dots h_n^{\delta_n} g_1^{\epsilon_1} \dots g_m^{\epsilon_m} = hg$$

so that $\langle H, Z(G)\rangle$ is abelian.

To obtain an example, consider groups that are non-abelian and their centers. Let $G = D_8$ and $H = Z(G) = \{1, r^2\}$. Then $C_G(H) = G$ since $H \leq Z(G)$. However, $\langle H, C_G(H)\rangle = \langle Z(G), G\rangle = G$ which is non-abelian. ■

Exercise 2.4.4

Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.

Solution. If H is trivial, then $H - \{1\} = \varnothing$ so that $\langle\varnothing\rangle = 1 = H$.

Suppose H is non-trivial, and let $h \in H$. If $h = 1$, then $h \in \langle H - \{1\}\rangle \leq G$. If $h \neq 1$, then $h \in H - \{1\}$ so that $h \in \langle H - \{1\}\rangle$. Hence, $H \subseteq \langle H - \{1\}\rangle$. Moreover, $\langle H - \{1\}\rangle$ is the smallest subgroup containing $H - \{1\}$ which is a subset of H so that $\langle H - \{1\}\rangle \subseteq H$. Therefore, $\langle H - \{1\}\rangle = H$. ■

Exercise 2.4.5

Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.

Solution. Consider the 2-cycles $(1\ 2)$ and $(1\ 3)$. Then

$$\begin{aligned}(1\ 2)(1\ 3) &= (1\ 3\ 2)\\ (1\ 3)(1\ 2) &= (1\ 2\ 3)\\ (1\ 3\ 2)(1\ 2) &= (2\ 3)\end{aligned}$$

so that $\langle(1\ 2), (1\ 3)\rangle = S_3$. One can also do similar calculations to ensure $\langle(1\ 2), (2\ 3)\rangle = \langle(1\ 3), (2\ 3)\rangle = S_3$. ■

Exercise 2.4.6

Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 2)(3\ 4)$ is a noncyclic group of order 4.

Solution. Let $a = (1\ 2)$ and $b = (3\ 4)$. Then $\langle a, ab\rangle = \{1, a, b, ab\}$ where $ab = ba$ since they are disjoint cycles. Moreover, $|a| = |b| = |ab| = 2$ so that it is noncyclic. ■

Exercise 2.4.7

Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 3)(2\ 4)$ is isomorphic to the dihedral group of order 8.

Solution. Let $\alpha = (1\ 2)$ and $\beta = (1\ 3)(2\ 4)$. Let $\gamma = \alpha\beta = (1\ 3\ 2\ 4)$. Note that $\gamma^4 = \alpha^2 = 1$, and $\gamma\alpha = \alpha\gamma^{-1}$ so that α and γ satisfy the relations for D_8. Moreover, any element of $\langle\alpha, \beta\rangle$ can be written as $\alpha^i\gamma^j$ for some $0 \le i \le 1$ and $0 \le j \le 3$ using the relations above. We may then extend the map

$$\varphi : D_8 \to \langle\alpha, \beta\rangle \quad \text{by} \quad r^j s^i \mapsto \gamma^j\alpha^i$$

to an injective homomorphism, since distinct elements in D_8 map to distinct elements in $\langle\alpha, \beta\rangle$. It is easy to see that $\langle\alpha, \beta\rangle$ has order 8, since each of $\gamma, \gamma^2, \gamma^3$ are distinct from each other and from $\alpha, \alpha\gamma, \alpha\gamma^2, \alpha\gamma^3$, along with the identity. Hence, φ is an isomorphism. ■

Exercise 2.4.8

Prove that $S_4 = \langle(1\ 2\ 3\ 4), (1\ 2\ 4\ 3)\rangle$.

Solution. Let $A = \langle(1\ 2\ 3\ 4), (1\ 2\ 4\ 3)\rangle$. Let $\alpha = (1\ 2\ 3\ 4)$ and $\beta = (1\ 2\ 4\ 3)$. To show that $A = S_4$, we will show that A must be of order 12 or 24, then show that it contains both $(1\ 2)$ and $(1\ 3)(2\ 4)$ so that by the previous exercise, it has a subgroup of order 8, hence A must be of order 24.

Note that $|\alpha| = 4$ so that A has a subgroup of order 4. Moreover, $\alpha\beta = (1\ 3\ 2)$ has order 3 so that A has a subgroup of order 3 as well. Since $A \le S_4$, we may use Lagrange's Theorem to conclude that $|A|$ is a multiple of 3 and 4 that divides 24, so that $|A| = 12$ or 24.

To obtain the elements $(1\ 2)$ and $(1\ 3)(2\ 4)$, observe that $\alpha^2 = (1\ 3)(2\ 4)$. To obtain $(1\ 2)$, we use β to "disrupt" the symmetry of α^2 to potentially obtain a smaller cycle. By computation, we get $\beta\alpha^2 = (2\ 3)$. Conjugating $(2\ 3)$ by $\alpha^{-1} = \alpha^3$ sends 2 to 1 and 3 to 2, so that $\alpha^3(2\ 3)\alpha = (1\ 2)$. Hence, $(1\ 2) \in A$. Then by the previous exercise, A has a subgroup of order 8, so that $|A| = 24$. Therefore, $A = S_4$. ■

Exercise 2.4.9

Prove that $\mathrm{SL}_2(\mathbb{F}_3)$ is the subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ generated by $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$. [Recall from Exercise 2.1.9 that $\mathrm{SL}_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1 You may assume this subgroup has order 24—this will be an exercise in Section 3.2.]

Solution. Let

$$A = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \quad B = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$$

Since we know that $\mathrm{SL}_2(\mathbb{F}_3)$ has order 24, we need to exhibit at least 13 distinct matrices using A and B, since

$\langle A, B\rangle$ divides 24. Since I, A, and B are 3 distinct matrices, we compute 10 more:

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad B^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$
$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \qquad BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$
$$(AB)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \qquad ABA^2 = \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$$
$$A^2B = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} \qquad B^2A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$$
$$ABA = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad BAB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Hence $\langle A, B\rangle = 24$ so that $\langle A, B\rangle = \mathrm{SL}_2(\mathbb{F}_3)$. ■

Exercise 2.4.10

Prove that the subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is isomorphic to the quaternion group of order 8. [Use a presentation for Q_8.]

Solution. Let

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

By computation, it is easy to see that $A^2 = B^2 = -I_2$. Let $C = AB$. Then

$$C = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \quad C^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = -I_2$$

By definition, I_2 and $-I_2$ commute with all matrices in $\mathrm{SL}_2(\mathbb{F}_3)$. Note that all the relations we have gathered satisfy the relations in the presentation of Q_8 given in Exercise 1.4.3. The mapping

$$\varphi : Q_8 \to \langle A, B\rangle \quad \text{by} \quad i \mapsto A, \quad j \mapsto B$$

extends to a homomorphism since the relations are satisfied. Moreover, φ maps generators of Q_8 to generators of $\langle A, B\rangle$ so that φ is surjective. Since $|Q_8| = |\langle A, B\rangle| = 8$, then φ is injective as well. Hence, $\langle A, B\rangle \cong Q_8$. ■

Exercise 2.4.11

Show that $\mathrm{SL}_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

Solution. Recall that Q_8 and S_4 both have 6 elements of order 4. However, no two elements in Q_8 can generate the entirety of $\mathrm{SL}_2(\mathbb{F}_3)$ since $|Q_8| = 8$, while $S_4 = \langle (1\,2\,3\,4), (1\,2\,4\,3)\rangle$, hence they cannot be isomorphic. ■

(∗) Exercise 2.4.12

Prove that the subgroup of upper triangular matrices in $\mathrm{GL}_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8. (First find the order of this subgroup.)

Solution. Let $\mathrm{UT}_3(\mathbb{F}_2)$ denote the subgroup of upper triangular matrices in $\mathrm{GL}_3(\mathbb{F}_2)$. Let each matrix in $\mathrm{UT}_3(\mathbb{F}_2)$ be represented as (a,b,c), which refer to the elements a_{12}, a_{13}, a_{23} in a 3×3 upper triangular matrix with 1's on the diagonal. Moreover, multiplication of two matrices $A=(a,b,c)$ and $B=(d,e,f)$ is written as follows:

$$AB=(a,b,c)(d,e,f)=(a+d,b+e+af,c+f)$$

Since each of a,b,c can be either 0 or 1, then there are $2^3=8$ elements in $\mathrm{UT}_3(\mathbb{F}_2)$.

We first need to find matrices $A,B\in\mathrm{UT}_3(\mathbb{F}_2)$ such that $A^4=B^2=I_3$, and $AB=BA^3$. Note that

$$(a,b,c)^2=(2a,ac+2b,2c)=(0,ac,0)$$

so that for $A=(a,b,c)$ to have order 4, it must be that $a=c=1$. Since b may vary, choose $A=(1,0,1)$. For $B=(d,e,f)$ to have order 2, then $B^2=(0,df,0)=I_3$, so $df=0$. Then either $d=0$ or $f=0$. To satisfy $AB=BA^3$, we compute both sides to obtain

$$(1,0,1)(d,e,f)=(1+d,e+f,1+f)=(1+d,1+d+e,1+f)=(d,e,f)(1,1,1)$$

Checking each coordinate, we see that the first and third coordinates are equal to each other, while equality of the second coordinates imply that

$$e+f=1+d+e$$

which implies that $f=1+d$. Since d and f must be different, we may set without loss of generality $d=1$ and $f=0$. Since e may vary, we may choose $B=(1,0,0)$. Since $A^4=B^2=I_3$, then we have a homomorphism $\varphi: D_8\to\mathrm{UT}_3(\mathbb{F}_2)$ given by

$$\varphi(r)=A,\quad \varphi(s)=B$$

It is easy to see that $\langle A,B\rangle=\mathrm{UT}_3(\mathbb{F}_2)$ since A and B generate all 8 elements of $\mathrm{UT}_3(\mathbb{F}_2)$. Since $\varphi(D_8)=\mathrm{UT}_3(\mathbb{F}_2)$, then φ is surjective. Moreover, $|D_8|=|\mathrm{UT}_3(\mathbb{F}_2)|=8$, so that φ is injective as well. Therefore, $\mathrm{UT}_3(\mathbb{F}_2)\cong D_8$. ■

Exercise 2.4.13

Prove that the multiplicative group of positive rational numbers is generated by the set $\{1/p \mid p \text{ is prime}\}$.

Solution. Let P denote the set of the prime reciprocals, and let $\mathbb{Q}_+^\times$ denote the multiplicative group of positive rational numbers. Observe that $(1/p)^{-1}=p\in\langle P\rangle$ for any $1/p\in P$, since $\langle P\rangle\leq\mathbb{Q}_+^\times$. It then follows that $p^k\in\langle P\rangle$ as well for any $k\in\mathbb{Z}$.

Let $q\in\mathbb{Q}_+^\times$. Then $q=m/n$ for some $m\in\mathbb{Z}^+\cup\{0\}$ and $n\in\mathbb{Z}^+$. By the Fundamental Theorem of Arithmetic, both m and n can be expressed as a product of primes. Then $m/n=q\in\langle P\rangle$ since $\langle P\rangle$ is closed under multiplication. Hence, $\mathbb{Q}_+^\times\subseteq\langle P\rangle$. Since $P\subseteq\mathbb{Q}_+^\times$, then $\langle P\rangle\subseteq\mathbb{Q}_+^\times$. Therefore, $\langle P\rangle=\mathbb{Q}_+^\times$. ■

(∗) Exercise 2.4.14

A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.

(a) Prove that every finite group is finitely generated.

(b) Prove that $\mathbb{Z}$ is finitely generated.

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle 1/k \rangle$, where k is the product of all denominators appearing in a set of generators for H.]

(d) Prove that $\mathbb{Q}$ is not finitely generated.

Solution.

(a) Any finite group G is generated by $\langle G \rangle$.

(b) $\mathbb{Z} = \langle 1 \rangle$.

(c) Let $H = \langle A \rangle$, where

$$A = \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n} \right\}$$

where $(p_i, q_i) = 1$ for all $1 \leq i \leq n$. Then every element $h \in H$ is of the form

$$h = \sum_{i=1}^{n} a_i \frac{p_i}{q_i}, \quad a_i \in \mathbb{Z}$$

since $\mathbb{Q}$ is abelian. Define the quantities

$$k = \prod_{i=1}^{n} q_i, \quad k_j = k/q_j$$

so that k is the product of all denominators in A, and k_j is the product of all denominators except the denominator in the j-th fraction of A. We may then rewrite h as

$$h = \frac{1}{k} \sum_{i=1}^{n} a_i p_i k_i$$

so that $h \in \langle 1/k \rangle$, which is a cyclic subgroup of $\mathbb{Q}$. Then $H \leq \langle 1/k \rangle$, hence it is cyclic.

(d) Suppose $\mathbb{Q}$ was finitely generated. Then $\mathbb{Q} = \langle p/q \rangle$ where $(p, q) = 1$, by the previous part. Let $r \in \mathbb{Z}$ such that r does not divide q. Then there is some $n \in \mathbb{Z}$ such that

$$n \frac{p}{q} = \frac{1}{r}$$

Then $q = npr$, contradicting that r doesn't divide q. ■

Exercise 2.4.15

Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

Solution. By the previous exercise, such a subgroup cannot be finitely generated. Consider the set

$$A = \left\{ \frac{1}{2^k} \middle| k \in \mathbb{Z}^+ \cup \{0\} \right\}$$

where $\langle A \rangle \leq \mathbb{Q}$. Note that $\langle A \rangle < \mathbb{Q}$ since $1/3 \notin \langle A \rangle$. Moreover, if $\langle A \rangle = \langle p/q \rangle$, then $q = 2^m$ since every element of A has a power of 2. Then $2^{m+1} \notin \langle p/q \rangle$, but $2^{m+1} \in \langle A \rangle$, hence $\langle A \rangle$ cannot be cyclic. ■

(∗) Exercise 2.4.16

A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G.

(a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

(b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

(c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only if $H = \langle x^p \rangle$ for some prime p dividing n.

Solution.

(a) If H is maximal, then we are done. If not, there exists a subgroup $H_1 < G$ such that $H < H_1$. If H_1 is maximal, we are done, but if not, then there must be another subgroup such that $H_1 < H_2$. Continuing on, we can create a chain of subgroups H_i such that $H_i < H_{i+1}$. Since G is finite, the process of creating subgroups must terminate at some k. Then $H_k < G$ is a maximal subgroup that contains H.

(b) Note that $s \notin \langle r \rangle$ so that $\langle r \rangle$ is a proper subgroup of D_{2n}. If $\langle r \rangle$ was not maximal, there must exist some H such that $\langle r \rangle < H$ so that some reflection $sr^k \in H$ for some $1 \leq k < n$. Note that $r^{n-k} \in H$ so that $sr^k r^{n-k} = s \in H$. But then $H = D_{2n}$, contradicting that $H < D_{2n}$. It must be that $\langle r \rangle$ is maximal.

(c) Suppose H is maximal, and put $H = \langle x^k \rangle$ and $d = (n, k)$. Note that $d > 1$ for the subgroup to be proper. Let p be a prime that divides n. If $k = p$, then we are done. If $k \neq p$, consider $\langle x^p \rangle$. Then $H < \langle x^p \rangle$ since $p \mid d$. Since H is maximal, then $\langle x^p \rangle = G$. Then $(p, n) = 1$, but this contradicts that $p \mid n$. Then $k = p$.

Suppose that $H = \langle x^p \rangle$ for prime $p \mid n$. If H is not maximal, there exists $\langle x^d \rangle$ such that $d \mid p$. Since p is prime, then either $d = 1$ or p. If $d = 1$, then $\langle x^d \rangle = G$ which shows that $\langle x^d \rangle$ is not a proper subgroup of G. If $d = p$, then $\langle x^d \rangle = \langle x^p \rangle$ so that H is not a proper subgroup of $\langle x^d \rangle$. It follows that H is maximal. ■

(∗) Exercise 2.4.17

This is an exercise involving Zorn's Lemma. Prove that every nontrivial finitely generated group possesses maximal subgroups. Let G be a finitely generated group, say $G = \langle g_1, g_2, \ldots, g_n \rangle$, and let $\mathcal{S}$ be the set of all proper subgroups of G. Then $\mathcal{S}$ is partially ordered by inclusion. Let C be a chain in $\mathcal{S}$.

(a) Prove that the union H of all the subgroups in C is a subgroup of G.

(b) Prove that H is a proper subgroup.

(c) Use Zorn's Lemma to show that $\mathcal{S}$ has a maximal element (which is, by definition, a maximal subgroup).

Solution.

(a) Let $C \subseteq \mathcal{S}$ be a chain. Put

$$H = \bigcup_{K \in C} K$$

Since at least one subgroup is in C and subgroups are nonempty, then C is nonempty. Suppose $g, h \in H$. Then $g \in K_1$ and $h \in K_2$ for some $K_1, K_2 \in C$ such that $K_1 \leq K_2$ or $K_2 \leq K_1$, or both. Without loss of generality, suppose $K_1 \leq K_2$. Then $g \in K_2$ as well so that $gh^{-1} \in K_2 \subseteq H$. Then $H \leq G$.

(b) If H was not a proper subgroup, then H must contain all generators g_i. Associate each generator with a (not necessarily distinct) subgroup K_i so that $g_i \in K_i$ for every $1 \leq i \leq n$. Since C is a chain, then we may order the subgroups such that $K_j \leq K_{j+1}$ for all $1 \leq j \leq n-1$. It follows that K_n contains every generator g_i so that $K_n = G$, contradicting that C is a chain of proper subgroups of G.

(c) Because G is nontrivial, then $\{1\} \in \mathcal{S}$ so that $\mathcal{S}$ is nonempty. Moreover, $H \in \mathcal{S}$ by the previous part, and for any $K \in C$, we have $K \leq H$ so that H is an upper bound for C. Then every chain in $\mathcal{S}$ has an upper bound, so by Zorn's Lemma, $\mathcal{S}$ must have a maximal element. ■

Exercise 2.4.18

Let p be a prime and let $Z = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$ (so Z is the multiplicative group of all p-power roots of unity in $\mathbb{C}$). For each $k \in \mathbb{Z}^+$ let $H_k = \{z \in Z \mid z^{p^k} = 1\}$ (the group of p^kth roots of unity). Prove:

(a) $H_k \leq H_m$ if and only if $k \leq m$.

(b) H_k is cyclic for all k.

(c) Every proper subgroup of Z equals H_k for some k. In particular, every proper subgroup of Z is finite and cyclic.

(d) Z is not finitely generated.

Solution.

(a) Note that $|H_k| = p^k$ for any k as there are exactly p^k roots of unity. Now, if $H_k \leq H_m$, then $p^k \mid p^m$ by Lagrange's Theorem. Then $p^k \leq p^m$, or $k \leq m$ since $p > 0$.

If $k \leq m$, then $p^k \leq p^m$. In particular, $p^k \mid p^m$. Then for any $z \in H_k$, we have

$$z^{p^m} = (z^{p^k})^{p^{m-k}} = 1$$

so that $z \in H_m$. Then $H_k \leq H_m$.

(b) Let $\theta = e^{2\pi i/p^k}$. Note that $\langle\theta\rangle$ has order p^k, and $\langle\theta\rangle \subseteq H_k$. Now for some $z \in H_k$, we have $z = e^{2\pi ix/p^k}$ for some $0 \leq x < p^k$. Then $z = (e^{2\pi i/p^k})^x \in \langle\theta\rangle$ so that $\langle\theta\rangle = H_k$.

(c) Let H be a proper subgroup of Z. Note that every element in Z has order p^i for some $i \in \mathbb{Z}^+$, so elements of H will have similar orders. Define the set

$$S = \{n \in \mathbb{Z}^+ \mid |h| = p^n \text{ for some } h \in H\}$$

so that S is the set of integers n such that H contains a p^n–th root of unity. Moreover, H is trivially nonempty if we define $H_0 = \{z \in Z \mid z^{p^0} = z = 1\}$ so that the trivial proper subgroup $\{1\}$ of Z allows $1 \in H$.

Suppose now that S is infinite. For any $n \in \mathbb{Z}^+$, there exists $h \in H$ and $m \in \mathbb{Z}^+$ such that $|h| = p^m > p^n$, for otherwise it would be that every $h \in H$ has order $|h| \leq p^n$, meaning that n is an upper bound for S. Then $|h| = p^m$ so that $H_m = \langle h\rangle$, and $H_m \leq H$. Since $H_n \leq H_m$ for every $n \in \mathbb{Z}^+$, then

$$Z = \bigcup_{n\in\mathbb{Z}^+} H_n \subseteq H$$

which shows $Z \leq H$. But $H \leq Z$, hence $Z = H$, which contradicts that $Z = H$. It must be that S is finite, so it has some maximal element s. Because $s \in S$, then there is $h_0 \in H$ where $|h_0| = p^s$ so that $H_s = \langle h_0\rangle \leq H$. Suppose $h \in H$ with $|h| = p^k$ for some $k \in \mathbb{Z}^+$. Then $k \in S$ where $k \leq s$ so that $H_k \leq H_s$. Since $h \in H_k$, then $h \in H_s$ so $H \leq H_s$. Hence, $H = H_s$.

(d) Put $Z = \langle z_1, z_2, \ldots, z_n\rangle$ for some $n \in \mathbb{Z}^+$ such that $|z_i| = p^{x_i}$. Let $x = \max(x_1, x_2, \ldots, x_n)$. Then $z_i \in H_x$ for every $1 \leq i \leq n$ so that $Z \leq H_x$. But recall that Z comprises every p-power roots of unity so that $H_x \leq H_x$, contradicting part (a). It must be that Z is infinitely generated. ■

(∗) Exercise 2.4.19

A nontrivial abelian group A (written multiplicatively) is called *divisible* if for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$.

(a) Prove that the additive group of rational numbers $\mathbb{Q}$ is divisible.

(b) Prove that no finite abelian group is divisible.

Solution.

(a) Suppose $p/q \in \mathbb{Q}$. Then $(p/qn)n = p/q$, where $p/qn \in \mathbb{Q}$.

(b) Suppose we have a finite abelian group G with $|G| = n$. Pick some nonidentity $g \in G$. Then there is no such $h \in$ where $h^n = g$, since $h^n = 1$. ■

Exercise 2.4.20

Prove that if A and B are nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible.

Solution. Suppose $A \times B$ is divisible, and let $a \in A$, $b \in B$, and $k \in \mathbb{Z}^+$. Then there exists $(c, d) \in A \times B$ such that $(c, d)^k = (c^k, d^k) = (a, b)$. But then $c^k = a$ and $d^k = b$ so that A and B are divisible.

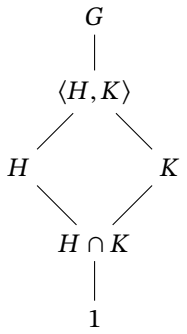
If A and B are both divisible, pick $(a, b) \in A \times B$ and let $k \in \mathbb{Z}^+$. Then there exists $c \in A$ and $d \in B$ such that $c^k = a$ and $d^k = b$. Then $(c, d)^k = (c^k, d^k) = (a, b)$ so that $A \times B$ is divisible. ■

2.5 The Lattice of Subgroups of a Group

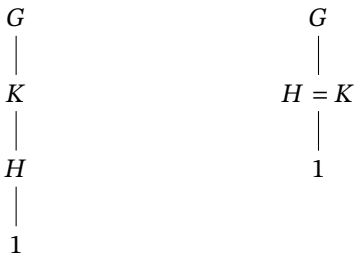
Exercise 2.5.1

Let H and K be subgroups of G. Exhibit all possible sublattices which show only $G, 1, H, K$ and their joins and intersections. What distinguishes the different drawings?

Solution. If H and K are distinct and neither is contained in the other, then the sublattice is a diamond shape:



If $H \leq K$, then the sublattice is a chain, noting that $\langle H, K\rangle = K$ and $H \cap K = H$. If $H = K$, then the sublattice is also a chain, noting that $\langle H, K\rangle = H = K$ and $H \cap K = H = K$:



Remaining scenarios include more trivial cases where one of H or K is either G or 1. ■

Exercise 2.5.2

In each of (a) to (d) list all subgroups of D_{16} that satisfy the given condition.

(a) Subgroups that are contained in $\langle sr^2, r^4\rangle$

(b) Subgroups that are contained in $\langle sr^7, r^4\rangle$

(c) Subgroups that contain $\langle r^4\rangle$

(d) Subgroups that contain $\langle s\rangle$.

Solution. Using the subgroup lattice of D_{16}, we find:

(a) $\langle sr^2, r^4\rangle, \langle sr^6\rangle, \langle sr^2\rangle, \langle r^4\rangle, 1$.

(b) Note $sr^7 = sr^3$, so $\langle sr^3, r^4\rangle, \langle r^4\rangle, \langle sr^3\rangle, \langle sr^7\rangle, 1$.

(c) $\langle r^4\rangle, \langle sr^2, r^4\rangle, \langle s, r^4\rangle, \langle r^2\rangle, \langle sr^3, r^4\rangle, \langle sr^5, r^4\rangle, \langle s, r^2\rangle, \langle r\rangle, \langle sr, r^2\rangle, D_{16}$.

(d) $\langle s\rangle, \langle s, r^4\rangle, \langle s, r^2\rangle, D_{16}$. ■

Exercise 2.5.3

Show that the subgroup $\langle s, r^2 \rangle$ of D_8 is isomorphic to V_4.

Solution. Recall that $V_4 = \{1, a, b, c\}$ where $a^2 = b^2 = c^2 = 1$ and $ab = c$, $bc = a$, and $ca = b$. Note that every element in $\langle s, r^2 \rangle$ has order 2 since $(r^2)^2 = s^2 = 1$ and $(sr^2)^2 = sr^2sr^2 = 1$. Then we may define a mapping $\varphi : V_4 \to \langle s, r^2 \rangle$ by

$$\varphi(1) = 1, \quad \varphi(a) = s, \quad \varphi(b) = r^2, \quad \varphi(c) = sr^2$$

We show that φ is a homomorphism by checking the products:

$$\begin{aligned} \varphi(a^2) &= \varphi(1) = 1 = s^2 = \varphi(a)^2 \\ \varphi(b^2) &= \varphi(1) = 1 = (r^2)^2 = \varphi(b)^2 \\ \varphi(ab) &= \varphi(c) = sr^2 = \varphi(a)\varphi(b) \end{aligned}$$

Similar calculations show that $\varphi(bc) = \varphi(b)\varphi(c)$ and $\varphi(ca) = \varphi(c)\varphi(a)$. Since φ is defined on all elements of V_4, then φ is a homomorphism. Moreover, φ is surjective since $\varphi(V_4) = \langle s, r^2 \rangle$. Since $|V_4| = |\langle s, r^2 \rangle| = 4$, then φ is injective as well. Therefore, $\langle s, r^2 \rangle \cong V_4$. ■

Exercise 2.5.4

Use the given lattice to find all pairs of elements that generate D_8 (there are 12 pairs).

Solution. Note that $D_8 = \langle s, r \rangle$. Moreover, $s \neq rs$, and $r \in \langle s, rs \rangle$ so that $\langle s, rs \rangle = D_8$. Since $r = r^3$, we also have $\langle s, r^3 \rangle = D_8$. We may also replace the reflection s with sr^2, since combinations of a reflection with an odd rotation and a reflection with an even rotation contain r and thus generates D_8. It follows that the pairs of elements that generate D_8 are:

$$\langle s, r \rangle, \langle s, r^3 \rangle, \langle s, rs \rangle, \langle s, r^3 s \rangle, \langle r^2 s, r \rangle, \langle r^2 s, r^3 \rangle, \langle r^2 s, rs \rangle, \langle r^2 s, r^3 s \rangle, \langle r, rs \rangle, \langle r^3, rs \rangle, \langle r, r^3 s \rangle, \langle r^3, r^3 s \rangle$$ ■

Exercise 2.5.5

Use the given lattice to find all elements $x \in D_{16}$ such that $D_{16} = \langle x, s \rangle$ (there are 8 such elements x).

Solution. Note that $\langle r \rangle = \langle r^3 \rangle = \langle r^5 \rangle = \langle r^7 \rangle$. We then pair each generator with an s so that we obtain just the rotation to then generate D_{16}: $x = r, r^3, r^5, r^7, sr, sr^3, sr^5, sr^7$. ■

Exercise 2.5.6

Use the given lattices to help find the centralizers of every element in the following groups:
(a) D_8 (b) Q_8 (c) S_3 (d) D_{16}.

Solution.

(a) To calculate the centralizer of an element a, start with the cyclic subgroup that contains a and see if any other elements are contained in $\langle a \rangle$. For example, to calculate $C_{D_8}(rs)$, start with $\langle rs \rangle$ in the subgroup lattice. Since $r^4, sr^5 \in C_{D_8}(rs)$, then $C_{D_8}(rs) \leq \langle sr^5, r^4 \rangle$. Checking the next subgroup, it follows that $r^2 \in C_{D_8}(rs)$ so that $C_{D_8}(rs) \leq \langle rs, r^2 \rangle$. Since $r \notin C_{D_8}(rs)$, then $C_{D_8}(rs) \neq D_{16}$ so that $C_{D_8}(rs) = \langle rs, r^2 \rangle$. We use similar reasoning to deduce the other centralizers:

$$\begin{aligned} C_{D_8}(1) &= D_8 & C_{D_8}(s) &= \langle s, r^2 \rangle \\ C_{D_8}(r) &= \langle r \rangle & C_{D_8}(rs) &= \langle rs, r^2 \rangle \\ C_{D_8}(r^2) &= D_8 & C_{D_8}(r^2 s) &= \langle s, r^2 \rangle \\ C_{D_8}(r^3) &= \langle r \rangle & C_{D_8}(r^3 s) &= \langle sr, r^2 \rangle \end{aligned}$$

(b) Note that $1, -1 \in Z(Q_8)$, while none of i, j, and k commute with anything but themselves. Then:

$$\begin{aligned} C_{Q_8}(1) &= C_{Q_8}(-1) = Q_8 \\ C_{Q_8}(i) &= C_{Q_8}(-i) = \langle i \rangle \\ C_{Q_8}(j) &= C_{Q_8}(-j) = \langle j \rangle \\ C_{Q_8}(k) &= C_{Q_8}(-k) = \langle k \rangle \end{aligned}$$

(c) Since no element in S_3 commutes with each other, then $C_{S_3}(a) = \langle a \rangle$ for all $a \in S_3 - \{1\}$, where $C_{S_3}(1) = S_3$.

(d) Use similar reasoning as in part (a) to obtain the centralizers:

$$\begin{aligned} C_{D_{16}}(1) = C_{D_{16}}(r^4) &= D_{16} \\ C_{D_{16}}(r^k) &= \langle r \rangle \text{ for all } k = 1, 2, 3, 5, , 6, \\ C_{D_{16}}(s) = C_{D_{16}}(sr^4) &= \langle s, r^4 \rangle \\ C_{D_{16}}(sr) = C_{D_{16}}(sr^5) &= \langle sr^5, r^4 \rangle \\ C_{D_{16}}(sr^2) = C_{D_{16}}(sr^6) &= \langle sr^2, r^4 \rangle \\ C_{D_{16}}(sr^3) = C_{D_{16}}(sr^7) &= \langle sr^3, r^4 \rangle \end{aligned}$$

■

Exercise 2.5.7

Find the center of D_{16}.

Solution. $Z(D_{16}) = \{1, r^4\}$ by Exercise 2.2.7. ■

Exercise 2.5.8

In each of the following groups find the normalizer of each subgroup:
(a) S_3 (b) Q_8.

Solution.

(a) From the subgroup lattice of S_3, we can deduce that each subgroup is cyclic and maximal except for $\{\text{id}\}$, where $N_{S_3}(\text{id}) = S_3$. Then for any $\alpha \in S_3$, we observe that $N_{S_3}(\langle \alpha \rangle) = \langle \alpha \rangle$ or S_3.

Consider $\alpha = (1\ 2)$. Since $(1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin \langle (1\ 2) \rangle$, then $N_{S_3}(\langle (1\ 2) \rangle) \neq S_3$ so that $N_{S_3}(\langle (1\ 2) \rangle) = \langle (1\ 2) \rangle$. By symmetry, the same holds for $\langle (1\ 3) \rangle$ and $\langle (2\ 3) \rangle$.

Consider $\alpha = (1\ 2\ 3)$. Observe that

$$(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2) \quad \text{and} \quad (1\ 2)(1\ 3\ 2)(1\ 2) = (1\ 2\ 3)$$

so that $(1\ 2) \in N_{S_3}(\langle (1\ 2\ 3) \rangle)$. Then $N_{S_3}(\langle (1\ 2\ 3) \rangle) = S_3$.

(b) Note that the subgroups $\langle -1 \rangle$ and $\{1\}$ are normal in Q_8 so that $N_{Q_8}(\langle -1 \rangle) = N_{Q_8}(\{1\}) = Q_8$. Consider the subgroups of order 4 in Q_8. In particular, observe for i:

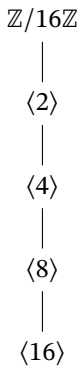
$$jij^{-1} = -i, j(-i)j^{-1} = i$$

so that $j \in N_{Q_8}(\langle i \rangle)$. Then $N_{Q_8}(\langle i \rangle) = Q_8$. By symmetry, the same holds for $\langle j \rangle$ and $\langle k \rangle$. ■

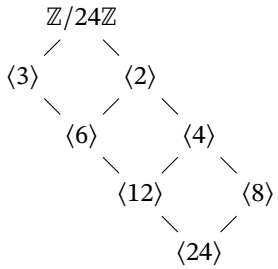
Exercise 2.5.9

Draw the lattices of subgroups of the following groups:
(a) $\mathbb{Z}/16\mathbb{Z}$ (b) $\mathbb{Z}/24\mathbb{Z}$ (c) $\mathbb{Z}/48\mathbb{Z}$.

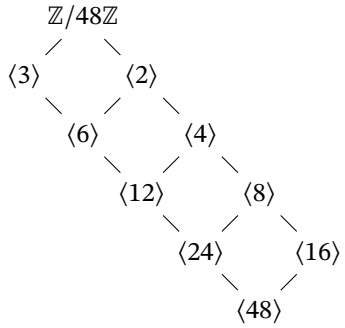
Solution.
(a) $\mathbb{Z}/16\mathbb{Z}$



(b) $\mathbb{Z}/24\mathbb{Z}$



(c) $\mathbb{Z}/48\mathbb{Z}$



■

Exercise 2.5.10

Classify groups of order 4 by proving that if $|G| = 4$, then $G \cong Z_4$ or $G \cong V_4$. [See Exercise 1.1.36.]

Solution. Let $G = \{1, a, b, c\}$. If G has an element of order 4, then $G \cong Z_4$ by Theorem 2.4.

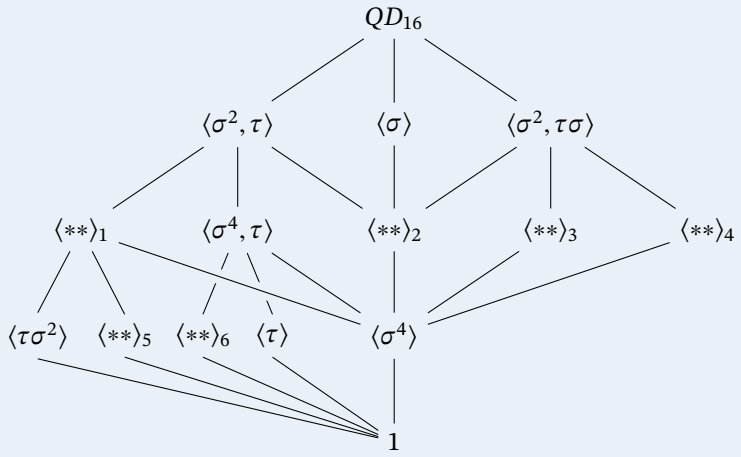
Suppose G is not cyclic. Then every nonidentity element has order 2 by Lagrange's Theorem. In particular, $a^2 = b^2 = c^2 = 1$. Note that $ab \neq 1$, since otherwise $b = a^{-1} = a$. Similarly, $ab \neq a$ and $ab \neq b$, so that $ab = c$. By similar reasoning, we have $bc = a$ and $ca = b$. This is precisely the definition of V_4, so that $G \cong V_4$. ■

Exercise 2.5.11

Consider the group of order 16 with the following presentation:

$$QD_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

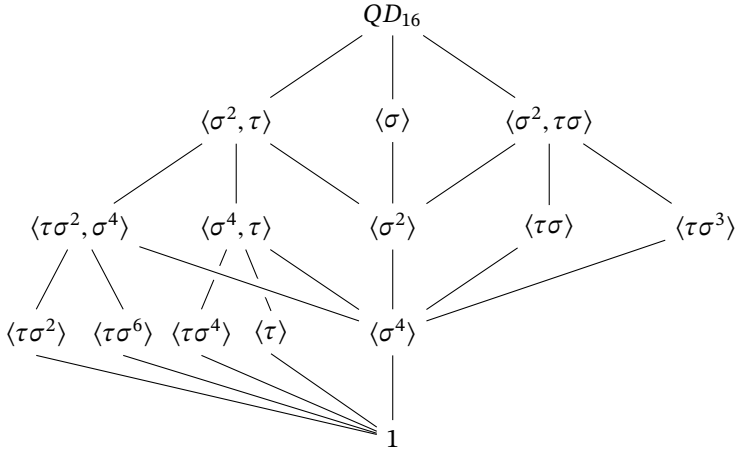
(called the *quasidihedral* or *semidihedral* group of order 16). This group has three subgroups of order 8: $\langle \tau, \sigma^2 \rangle \cong D_8, \langle \sigma \rangle \cong Z_8$, and $\langle \sigma^2, \sigma\tau \rangle \cong Q_8$, and every proper subgroup is contained in one of these three subgroups. Fill in the missing subgroups in the lattice of all subgroups of the quasidihedral group, exhibiting each subgroup with at most two generators.



Solution. The above has had subscripts added to distinguish the unknown subgroups. It is clear that $\langle ** \rangle_2$ must be $\langle \sigma^2 \rangle$ since it is the only subgroup contained in both $\langle \sigma \rangle$ and $\langle \sigma^2, \tau \rangle$. To find the other subgroups, we calculate the cyclic subgroups of the form $\langle \tau\sigma^k \rangle$:

$$\langle \tau\sigma \rangle = \{1, \tau\sigma, \sigma^4, \tau\sigma^5\} \qquad \langle \tau\sigma^3 \rangle = \{1, \tau\sigma^3, \sigma^4, \tau\sigma^7\}$$
$$\langle \tau\sigma^4 \rangle = \{1, \tau\sigma^4\} \qquad \langle \tau\sigma^6 \rangle = \{1, \tau\sigma^6\}$$

It becomes clear that 6 must be $\langle \tau\sigma^4 \rangle$, since the subgroup above contains both τ and σ^4. 3 and 4 must be $\langle \tau\sigma \rangle$ and $\langle \tau\sigma^3 \rangle$ respectively, since $\langle \sigma^2, \tau\sigma \rangle$ both contain $\tau\sigma$ and σ^2 which multiply to $\tau\sigma^3$. Certainly, 1 cannot be $\langle \tau\sigma^6 \rangle$ as it does not contain $\langle \tau\sigma^2 \rangle$, so it must be 5. Then 1 must be $\langle \tau\sigma^2, \sigma^4 \rangle$ as it contains both subgroups. Hence, the completed diagram is



■

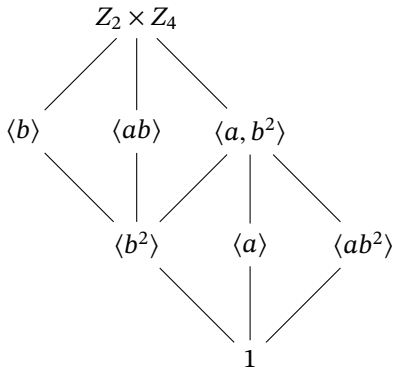
Exercise 2.5.12

The group $A = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1, ab = ba \rangle$ has order 8 and has three subgroups of order 4: $\langle a, b^2 \rangle \cong V_4$, $\langle b \rangle \cong Z_4$, and $\langle ab \rangle \cong Z_4$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of A, giving each subgroup in terms of at most two generators.

Solution. Observe that A is the direct product of two abelian groups, so A is abelian, and we may write it as

$$A = \{1, a, b, b^2, b^3, ab, ab^2, ab^3\}$$

We know that A has three subgroups of order 4: $\langle a, b^2 \rangle$, $\langle b \rangle$, and $\langle ab \rangle$. To find what the containment relations are, observe that $\langle a, b \rangle^2$ has three subgroups of order 2: $\langle b^2 \rangle$, $\langle a \rangle$, and $\langle ab^2 \rangle$. $\langle b \rangle$ has the single subgroup of order 2: $\langle b^2 \rangle$, and $\langle ab \rangle$ has the single subgroup of order 2: $\langle ab^2 \rangle$. Then the subgroup lattice of A is

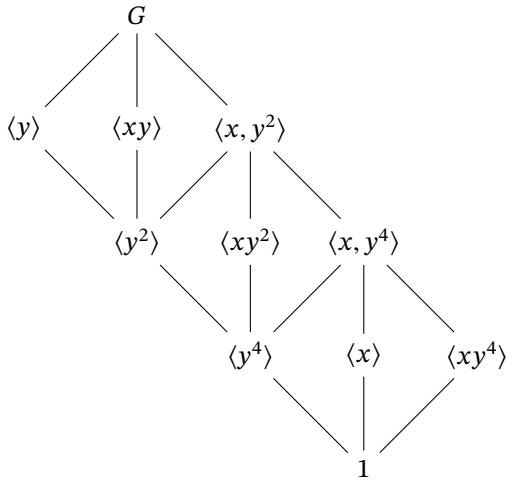


■

Exercise 2.5.13

The group $G = Z_2 \times Z_8 = \langle x, y \mid x^2 = y^8 = 1, xy = yx \rangle$ has order 16 and has three subgroups of order 8: $\langle x, y^2 \rangle \cong Z_2 \times Z_4$, $\langle y \rangle \cong Z_8$, and $\langle xy \rangle \cong Z_8$, and every proper subgroup is contained in one of those three. Draw the lattice of all subgroups of G, giving each subgroups in terms of at most two generators (cf. Exercise 2.5.12).

Solution. Let $x = a$ and $y^2 = b$, where a and b are the generators from Exercise 2.5.12. It follows that G contains a copy of $Z_2 \times Z_4$ as $\langle x, y^2 \rangle = \langle a, b \rangle$. Moreover, we may append $\langle y \rangle$ and $\langle xy \rangle$ to this lattice as follows:



■

Exercise 2.5.14

Let M be the group of order 16 with the following presentation:

$$\langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$$

(sometimes called the *modular* group of order 16). It has three subgroups of order 8: $\langle u, v^2 \rangle$, $\langle v \rangle$, and $\langle uv \rangle$, and every proper subgroup is contained in one of those three. Prove that $\langle u, v^2 \rangle \cong Z_2 \times Z_4$, $\langle v \rangle \cong Z_8$, and $\langle uv \rangle \cong Z_8$. Show that the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$ (cf. Exercise 13) but that these two groups are not isomorphic.

Solution. It is clear that $|v| = 8$ implies that $\langle v \rangle \cong Z_8$. Similarly, since $|uv| = 8$, then $\langle uv \rangle \cong Z_8$. To see that $\langle u, v^2 \rangle \cong Z_2 \times Z_4$, we verify the relations. Note that $u^2 = (v^2)^4 = 1$, and

$$v^2 u = vuv^5 = uv^{10} = uv^2$$

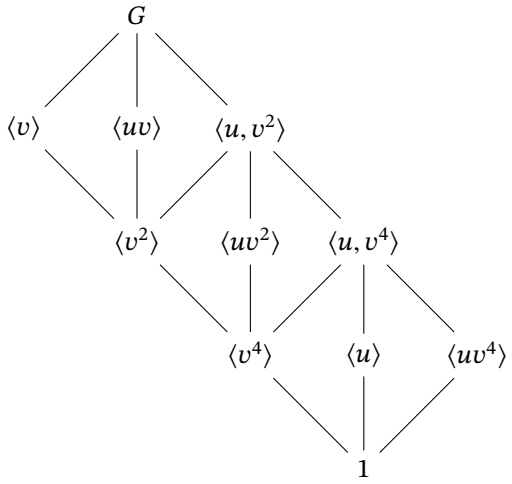
so that u and v^2 commute, hence it is abelian. We may then list out the elements of $\langle u, v^2 \rangle$:

$$\langle u, v^2 \rangle = \{1, v^2, v^4, v^6, u, uv^2, uv^4, uv^6\}$$

Then the mapping $\varphi : Z_2 \times Z_4 \to \langle u, v^2 \rangle$ defined by

$$\varphi(a) = u, \quad \varphi(b) = v^2$$

extends to a homomorphism. Moreover, it is clear that distinct elements in $Z_2 \times Z_4$ map to distinct elements in $\langle u, v^2 \rangle$, so that φ is injective. As shown above, $|\langle u, v^2 \rangle| = 8 = |Z_2 \times Z_4|$, so that φ is surjective. Hence, φ is an isomorphism and $Z_2 \times Z_4 \cong \langle u, v^2 \rangle$. The subgroup lattice of M is then the same as that of $Z_2 \times Z_8$ as shown in Exercise 2.5.13, but with $u = x$ and $v = y$:



Finally, M is not isomorphic to $Z_2 \times Z_8$ since M is not abelian. If it were, then $vu = uv$, but $vu = uv^5 = uv$ would imply that $v^4 = 1$, contradicting that $|v| = 8$. ■

Exercise 2.5.15

Describe the isomorphism type of each of the three subgroups of D_{16} of order 8.

Solution. Since $|r| = 8$, then $\langle r \rangle \cong Z_8$. For the remaining subgroups, note that the lattice for D_{16} shows a striking similarity to the lattice for D_8; in fact, these subgroups *are* isomorphic to D_8 as follows:

For the subgroup $\langle s, r^2 \rangle$, observe that $(r^2)4 = s^2 = 1$, and $sr^2 = r^6 s = (r^2)^{-1}s$. Then the mapping $\varphi : D_8 \to \langle s, r^2 \rangle$ given by

$$\varphi(r) = r^2, \quad \varphi(s) = s$$

extends to a homomorphism. Moreover, this mapping is surjective by construction. Since $\langle s, r^2 \rangle$ contains a subgroup of order 4 and is a subgroup of D_{16}, it must be 8 so that φ is an isomorphism, and $D_8 \cong \langle s, r^2 \rangle$.

For the subgroup $\langle sr, r^2 \rangle$, we again observe that $(r^2)^4 = (sr)^2 = 1$, and $(sr)r^2 = sr^3 = r^5 s = r^6 r^7 s = (r^2)^{-1}(sr)$. The mapping $\psi : D_8 \to \langle sr, r^2 \rangle$ given by

$$\varphi(r) = r^2, \varphi(s) = sr$$

extends to a homomorphism, surjective by construction, and is an isomorphism because $\langle sr, r^2 \rangle$ has order 8. Then $D_8 \cong \langle sr, r^2 \rangle$. ■

Exercise 2.5.16

Use the lattice of subgroups of the quasidihedral of order 16 to show that every element of order 2 is contained in the proper subgroup $\langle \tau, \sigma^2 \rangle$ (cf. Exercise 2.5.11).

Solution. Every element of order 2 generates a cyclic subgroup of order 2. Using the lattice, $\langle \tau, \sigma^2 \rangle$ properly contains all cyclic subgroups, except $\langle \tau\sigma \rangle$ and $\langle \tau\sigma^3 \rangle$, both of which are order 4. Then $\langle \tau, \sigma^2 \rangle$ contains all cyclic subgroups of order 2, hence contain all elements of order 2. ■

Exercise 2.5.17

Use the lattice of subgroups of the modular group M of order 16 to show that the set $\{x \in M \mid x^2 = 1\}$ is a subgroup of M isomorphic to the Klein 4-group (cf. Exercise 2.5.14).

Solution. Using the lattice in Exercise 14, we see that we have 3 candidates to be isomorphic to V_4, namely $\langle v^2 \rangle$, $\langle uv^2 \rangle$, and $\langle u, v^4 \rangle$. The first and second subgroups are cyclic, while $\langle u, v^4 \rangle = \{1, u, v^4, uv^4\}$. Since it is not generated by one element, each of these elements are of order 2, and $v^4 u = v^3 uv^5 = \cdots = uv^{20} = uv^4$ so that it is abelian, then $\langle u, v^4 \rangle \cong V_4$. ■

Exercise 2.5.18

Use the lattice to help find the centralizer of every element of QD_{16} (cf. Exercise 2.5.11).

Solution. Note that $\sigma^4\tau = \sigma^3\tau\sigma^3 = \cdots = \tau\sigma^{12} = \tau\sigma^4$ so that $\sigma^4 \in Z(QD_{16})$ as σ^4 already commutes with powers of σ. Moreover, any power of σ does not commute with τ except for σ^4. The elements $\tau\sigma$ and $\tau\sigma^3$ do not commute with σ^2 as $(\tau\sigma)\sigma^2 = \tau\sigma^3 = \sigma\tau \neq \sigma^2(\tau\sigma) = \tau\sigma^2$, and $(\tau\sigma^3)\sigma^2 = \sigma^7\tau \neq \sigma^3\tau = \sigma^2(\tau\sigma^3)$. Next, $(\tau\sigma^2)\sigma^2 = \tau\sigma^4 \neq \tau = \sigma^2(\tau\sigma^2)$ so that σ^2 does not commute with $\tau\sigma^2$. Moreover, $(\tau\sigma^6)(\tau\sigma^2) = \tau\sigma^2\sigma^4\tau\sigma^2 = (\tau\sigma^2)(\tau\sigma^6)$ so that $\tau\sigma^2$ commutes with $\tau\sigma^6$, but $\sigma^2\tau\sigma^6 = \tau\sigma^4 \neq \tau = (\tau\sigma^6)\sigma^2$ so σ^2 does not commute with $\tau\sigma^6$. Lastly, $\sigma^2(\tau\sigma^4) = \tau\sigma^2 \neq (\tau\sigma^4)\sigma^2$, and $\sigma^2\tau = \tau\sigma^6 \neq \tau\sigma^2$ so that σ^2 does not commute with $\tau\sigma^4$ nor with τ. It follows that the centralizers of the elements of QD_{16} are

$$\begin{aligned}
C_{QD_{16}}(1) = C_{QD_{16}}(\sigma^4) &= QD_{16} \\
C_{QD_{16}}(\langle \sigma^k \rangle) &= \langle \sigma \rangle \text{ for } k = 1, 2, 3, 5, 6, 7 \\
C_{QD_{16}}(\langle \tau\sigma \rangle) = C_{QD_{16}}(\langle \tau\sigma^5 \rangle) &= \langle \tau\sigma \rangle \\
C_{QD_{16}}(\langle \tau\sigma^3 \rangle) = C_{QD_{16}}(\langle \tau\sigma^7 \rangle) &= \langle \tau\sigma^3 \rangle \\
C_{QD_{16}}(\langle \tau \rangle) = C_{QD_{16}}(\langle \tau\sigma^4 \rangle) &= \langle \sigma^4, \tau \rangle \\
C_{QD_{16}}(\langle \tau\sigma^2 \rangle) = C_{QD_{16}}(\langle \tau\sigma^6 \rangle) &= \langle \tau\sigma^2, \sigma^4 \rangle
\end{aligned}$$

■

Exercise 2.5.19

Use the lattice to help find $N_{D_{16}}(\langle s, r^4\rangle)$.

Solution. Based on the placement of $\langle s, r^4\rangle$, its normalizer may be itself, $\langle s, r^2\rangle$, or D_{16}. Note that $\langle s, r^4\rangle = \{1, s, r^4, sr^4\}$, and taking r^2 and $(r^2)^{-1} = r^6$, we have

$$r^2\langle s, r^4\rangle r^6 = \{1, sr^4, r^4, s\} = \langle s, r^4\rangle$$

so that $r^2 \in N_{D_{16}}(\langle s, r^4\rangle)$, and $\langle s, r^2\rangle \leq N_{D_{16}}(\langle s, r^4\rangle)$. Since $rsr^{-1} = r^2 s \neq r$, then $r \notin N_{D_{16}}(\langle s, r^4\rangle)$ so that $N_{D_{16}}(\langle s, r^4\rangle) = \langle s, r^2\rangle$. ■

Exercise 2.5.20

Use the lattice of subgroups of QD_{16} (cf. Exercise 2.5.11) to help find the normalizers

(a) $N_{QD_{16}}(\langle \tau\sigma\rangle)$ (b) $N_{QD_{16}}(\langle \tau, \sigma^4\rangle)$.

Solution.

(a) Note that $\langle \tau\sigma\rangle = \{1, \tau\sigma, \sigma^4, \tau\sigma^5\}$. Moreover, $(\sigma^2)^{-1} = \sigma^6$ so that

$$\sigma^2\langle \tau\sigma\rangle\sigma^6 = \{1, \tau\sigma^4, \sigma^4, \tau\sigma\} = \langle \tau\sigma\rangle$$

and $\sigma(\tau\sigma)\sigma^7 = \tau\sigma^3 \neq \tau\sigma$ so that $\sigma \notin N_{QD_{16}}(\langle \tau\sigma\rangle)$. Then $N_{QD_{16}}(\langle \tau\sigma\rangle) = \langle \sigma^2, \tau\sigma\rangle$.

(b) $\langle \tau, \sigma^4\rangle = \{1, \tau, \sigma^4, \tau\sigma^4\}$, and

$$\sigma^2\langle \tau, \sigma^4\rangle\sigma^6 = \{1, \tau\sigma^4, \sigma^4, \tau\}$$

while $\sigma\tau\sigma^7 = \tau\sigma^2 \neq \tau$ so that $\sigma \notin N_{QD_{16}}(\langle \tau, \sigma^4\rangle)$. Then $N_{QD_{16}}(\langle \tau, \sigma^4\rangle) = \langle \sigma^2, \tau\rangle$. ■