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.

4 Group Actions

4.1 Group Actions and Permutation Representations

Let G be a group and let A be a nonempty set.

Exercise 4.1.1

Let G act on the set A. Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$ (G_a is the stabilizer of a). Deduce that if G acts transitively on A then the kernel of the action is

$$\bigcap_{g \in G} gG_ag^{-1}.$$

Solution. Suppose $h \in G_b$. We want to show that $h \in gG_ag^{-1}$. Since $h \in G_b$, we have $h \cdot b = b$. But $b = g \cdot a$, so $h \cdot (g \cdot a) = g \cdot a$. Applying g^{-1} to both sides, we get $g^{-1}hg \cdot a = a$. This means that $g^{-1}hg \in G_a$, so $h \in gG_ag^{-1}$. Thus, we have shown that $G_b \subseteq gG_ag^{-1}$. For the other direction, suppose $h \in gG_ag^{-1}$. Then there exists some $k \in G_a$ such that $h = gkg^{-1}$. We want to show that $h \in G_b$. We have $h \cdot b = (gkg^{-1}) \cdot (g \cdot a) = g \cdot (k \cdot a) = g \cdot a = b$, since $k \in G_a$ implies $k \cdot a = a$. Thus, $h \in G_b$. Therefore, we have shown that $gG_ag^{-1} \subseteq G_b$. Combining both inclusions, we conclude that $G_b = gG_ag^{-1}$.

Now, if G acts transitively on A, then for any $b \in A$, there exists some $g \in G$ such that $b = g \cdot a$. From the first part, we have $G_b = gG_ag^{-1}$. The kernel of the action is the intersection of all stabilizers G_b for $b \in A$. Therefore, the kernel is

$$\bigcap_{b \in A} G_b = \bigcap_{g \in G} gG_ag^{-1}.$$ ■

Exercise 4.1.2

Let G be a permutation group on the set A (i.e., $G \leq S_A$), let $\sigma \in G$ and let $a \in A$. Prove that $\sigma G_a\sigma^{-1} = G_{\sigma(a)}$. Deduce that if G acts transitively on A then

$$\bigcap_{\sigma \in G} \sigma G_a\sigma^{-1} = 1.$$

Solution. Suppose $\tau \in \sigma G_a\sigma^{-1}$. We want to show that $\tau \in G_{\sigma(a)}$. Since $\tau \in \sigma G_a\sigma^{-1}$, there exists some $\rho \in G_a$ such that $\tau = \sigma\rho\sigma^{-1}$. We have $\tau \cdot \sigma(a) = (\sigma\rho\sigma^{-1}) \cdot \sigma(a) = \sigma \cdot (\rho \cdot a) = \sigma(a)$, since $\rho \in G_a$ implies $\rho \cdot a = a$. Thus, $\tau \in G_{\sigma(a)}$. Therefore, we have shown that $\sigma G_a\sigma^{-1} \subseteq G_{\sigma(a)}$. For the other direction, suppose $\tau \in G_{\sigma(a)}$. We want to show that $\tau \in \sigma G_a\sigma^{-1}$. We have $\tau \cdot \sigma(a) = \sigma(a)$. Applying σ^{-1} to both sides, we get $\sigma^{-1}\tau\sigma \cdot a = a$. This means that $\sigma^{-1}\tau\sigma \in G_a$, so $\tau \in \sigma G_a\sigma^{-1}$. Thus, we have shown that $G_{\sigma(a)} \subseteq \sigma G_a\sigma^{-1}$. Combining both inclusions, we conclude that $\sigma G_a\sigma^{-1} = G_{\sigma(a)}$.

Now, if G acts transitively on A, then for any $b \in A$, there exists some $\sigma \in G$ such that $b = \sigma(a)$. From the first part, we have $\sigma G_a\sigma^{-1} = G_b$. The kernel of the action is the intersection of all stabilizers G_b for $b \in A$. Therefore, the kernel is

$$\bigcap_{b \in A} G_b = \bigcap_{\sigma \in G} \sigma G_a\sigma^{-1} = 1.$$ ■

Exercise 4.1.3

Assume that G is an abelian, transitive subgroup of S_A. Show that $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$. Deduce that $|G| = |A|$. [Use the preceding exercise.]

Solution. Since G is abelian, then the conjugate of G_a is trivial, i.e., $\sigma G_a\sigma^{-1} = G_a$ for all $\sigma \in G$. From the previous exercise, we know that the kernel of this action is trivial. However, the intersection of all $\sigma G_a\sigma^{-1}$ is just G_a so that $G_a = 1$. Then G_a is trivial for every $a \in A$, hence $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$. It follows by Proposition 4.2 that $|G|/|G_a| = |A|$, hence $|G| = |A|$ because G_a is trivial. ■

Exercise 4.1.4

Let S_3 act on the set Ω of ordered pairs $\{(i,j) \mid 1 \le i,j \le 3\}$ by $\sigma((i,j)) = (\sigma(i),\sigma(j))$. Find the orbits of S_3 on Ω. For each $\sigma \in S_3$ find the cycle decomposition of σ under this action (i.e., find its cycle decomposition when σ is considered as an element of S_9—first fix a labeling of these nine ordered pairs). For each orbit $\mathcal{O}$ of S_3 acting on these nine points, pick some $a \in \mathcal{O}$ and find the stabilizer of a in S_3.

Solution. Note that in Ω, there are two types of ordered pairs: those with identical elements and those with distinct elements. In the former case, it is clear that any $\sigma \in S_3$ will map such a pair to another pair with identical elements. In the latter case, it is easy to find some $\sigma \in S_3$ that maps any ordered pair with distinct elements to any other such pair. We now label the elements of Ω accordingly:

- $1 = (1,1)$
- $2 = (2,2)$
- $3 = (3,3)$
- $4 = (1,2)$
- $5 = (2,1)$
- $6 = (1,3)$
- $7 = (3,1)$
- $8 = (2,3)$
- $9 = (3,2)$

We then have the two orbits

$$\mathcal{O}_1 = \{(i,i) \mid i \in \{1,2,3\}\} \quad \text{and} \quad \mathcal{O}_2 = \{(i,j) \mid i \ne j\}$$

of S_3 acting on Ω. Note that $|\mathcal{O}_1| = 3$ and $|\mathcal{O}_2| = 6$. Now for each $\sigma \in S_3$, we find its cycle decomposition as an element of S_9. We describe how to compute one such cycle decomposition, and the rest follow similarly. Consider $\sigma = (123) \in S_3$. Then we have the following mappings:
- $(1,1) \mapsto (2,2) \mapsto (3,3) \mapsto (1,1)$, which corresponds to the cycle (1 2 3) in S_9.
- $(1,2) \mapsto (2,3) \mapsto (3,1) \mapsto (1,2)$, which corresponds to the cycle (4 8 7) in S_9.
- $(2,1) \mapsto (3,2) \mapsto (1,3) \mapsto (2,1)$, which corresponds to the cycle (5 9 6) in S_9.

Combining these cycles, we find that the cycle decomposition of $\sigma = (123)$ in S_9 is (1 2 3)(4 8 7)(5 9 6). The cycle decompositions for all elements of S_3 acting on Ω are as follows:

- $1 \in S_3$ is the same as $1 \in S_9$.
- (12): (1 2)(4 5)(6 7)(8 9)
- (13): (1 3)(4 6)(5 7)(8 9)
- (23): (1 2)(2 3)(5 6)(7 8)
- (123): (1 2 3)(4 8 7)(5 9 6)
- (132): (1 3 2)(4 7 8)(5 6 9)

For $\mathcal{O}_1$, we pick $a = (1,1)$. The only $\sigma \in S_3$ that fixes $(1,1)$ is the identity permutation and (2 3), so the stabilizer of $(1,1)$ in S_3 is $\langle(2\ 3)\rangle$. Moreover, we have $|G_a||\mathcal{O}_1| = 2 \cdot 3 = 6 = |S_3|$ as expected. For $\mathcal{O}_2$, we pick $a = (1,2)$. The only $\sigma \in S_3$ that fixes $(1,2)$ is the identity permutation, so the stabilizer of $(1,2)$ in S_3 is 1. Again, $|G_a||\mathcal{O}_2| = 1 \cdot 6 = 6 = |S_3|$. ■

Exercise 4.1.5

For each of parts (a) and (b) repeat the preceding exercise but with S_3 acting on the specified set:

(a) the set of 27 triples $\{(i,j,k) \mid 1 \le i,j,k \le 3\}$

(b) the set $\mathcal{P}(\{1,2,3\}) - \{\varnothing\}$ of all 7 nonempty subsets of $\{1,2,3\}$

Solution.

(a) We begin by classifying these set of triples. There are five types of triples:
- Type 1: Triples with all identical elements.
- Type 2: Triples whose two first coordinates are identical.
- Type 3: Triples whose first and last coordinates are identical.
- Type 4: Triples whose last two coordinates are identical.
- Type 5: Triples with all distinct elements.

Note that this is a correct classification. One may suggest to combine Types 2, 3, and 4 into a singular type. However, observe that no elements may be permuted such that the location of a pair of identical coordinates move to another one, i.e., there is no such permutation σ in S_3 such that $(1,1,2)$ maps to $(1,2,2)$.We now label the elements of Ω lexicographically as follows, i.e., we begin by increasing the last coordinate, then increasing the middle coordinate, and finally increasing the first coordinate:

- $1 = (1,1,1)$
- $2 = (1,1,2)$
- $3 = (1,1,3)$
- $4 = (1,2,1)$
- $5 = (1,2,2)$
- $6 = (1,2,3)$
- $7 = (1,3,1)$
- $8 = (1,3,2)$
- $9 = (1,3,3)$
- $10 = (2,1,1)$
- $11 = (2,1,2)$
- $12 = (2,1,3)$
- $13 = (2,2,1)$
- $14 = (2,2,2)$
- $15 = (2,2,3)$
- $16 = (2,3,1)$
- $17 = (2,3,2)$
- $18 = (2,3,3)$
- $19 = (3,1,1)$
- $20 = (3,1,2)$
- $21 = (3,1,3)$
- $22 = (3,2,1)$
- $23 = (3,2,2)$
- $24 = (3,2,3)$
- $25 = (3,3,1)$
- $26 = (3,3,2)$
- $27 = (3,3,3)$

The classification yields the following orbits of S_3 acting on Ω:
- $O_1 = \{(i,i,i) \mid i \in \{1,2,3\}\}$ with order 3.
- $O_2 = \{(i,i,j) \mid i \neq j\}$ with order 6.
- $O_3 = \{(i,j,i) \mid i \neq j\}$ with order 6.
- $O_4 = \{(j,i,i) \mid i \neq j\}$ with order 6.
- $O_5 = \{(i,j,k) \mid i,j,k \text{ distinct}\}$ with order 6.

The cycle decompositions for all elements of S_3 acting on Ω are as follows:
- $1 \in S_3$ is the same as $1 \in S_{27}$.
- (1 2): (1 14)(2 13)(3 15)(4 11)(5 10)(6 12)(7 17)(8 16)(9 18)(19 23)(20 22)(21 24)(25 26)
- (1 3): (1 27)(2 26)(3 25)(4 24)(5 23)(6 22)(7 21)(8 20)(9 19)(10 18)(11 17)(12 16)(13 15)
- (2 3): (2 3)(4 7)(5 9)(6 8)(10 19)(11 21)(12 20)(13 25)(14 27)(15 26)(16 22)(17 24)(18 23)
- (1 2 3): (1 14 27)(2 15 25)(3 13 26)(4 17 21)(5 18 19)(6 16 20)(7 11 24)(8 12 22)(9 10 23)
- (1 3 2): (1 27 14)(2 25 15)(3 26 13)(4 21 17)(5 19 18)(6 20 16)(7 24 11)(8 22 12)(9 23 10)

For O_1, pick $a = (1\,1\,1)$. The elements that stabilize a are the identity permutation and (2 3), so the stabilizer of a in S_3 is $\langle(2\,3)\rangle$. We have $|G_a||O_1| = 2 \cdot 3 = 6 = |S_3|$. For the other orbits, note that S_3 acts transitively on each of them, so the stabilizer of any chosen element in these orbits is trivial. For example, for O_2, pick $a = (1\,1\,2)$. The only element that stabilizes a is the identity permutation, so the stabilizer of a in S_3 is 1. We have $|G_a||O_2| = 1 \cdot 6 = 6 = |S_3|$. The same logic applies to O_3, O_4, and O_5.

(b) We begin by classifying the nonempty subsets of $\{1,2,3\}$. There are three types of subsets: 1-element subsets, 2-element subsets, and the 3-element subset. We now label the elements of $\mathcal{P}(\{1,2,3\}) - \{\varnothing\}$ as follows:

- $1 = \{1\}$
- $2 = \{2\}$
- $3 = \{3\}$
- $4 = \{1,2\}$
- $5 = \{1,3\}$
- $6 = \{2,3\}$
- $7 = \{1,2,3\}$

The classification yields the following orbits of S_3 acting on $\mathcal{P}(\{1,2,3\}) - \{\varnothing\}$:
- $O_1 = \{\{1\},\{2\},\{3\}\}$ with order 3.
- $O_2 = \{\{1,2\},\{1,3\},\{2,3\}\}$ with order 3.
- $O_3 = \{\{1,2,3\}\}$ with order 1.

The cycle decompositions for all elements of S_3 acting on $\mathcal{P}(\{1,2,3\}) - \{\varnothing\}$ are as follows:
- $1 \in S_3$ is the same as $1 \in S_7$.
- (1 2): (1 2)(5 6)
- (1 3): (1 3)(4 6)
- (2 3): (2 3)(4 5)
- (1 2 3): (1 2 3)(4 6 5)
- (1 3 2): (1 3 2)(4 5 6)

For O_1, pick $a = \{1\}$. The only elements that stabilize a are the identity permutation and (2 3), so the stabilizer of a in S_3 is $\langle(2\,3)\rangle$. We have $|G_a||O_1| = 2 \cdot 3 = 6 = |S_3|$. For O_2, pick $a = \{1,2\}$. The only elements that stabilize a are the identity permutation and (1 2), so the stabilizer of a in S_3 is $\langle(1\,2)\rangle$. We have $|G_a||O_2| = 2 \cdot 3 = 6 = |S_3|$. For O_3, note that S_3 acts trivially on this orbit, so the stabilizer of $\{1,2,3\}$ in S_3 is all of S_3. We have $|G_a||O_3| = 6 \cdot 1 = 6 = |S_3|$. ■

Exercise 4.1.6

As in 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 and let S_4 act on R by permuting the indices of the four variables: $\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$ for all $\sigma \in S_4$.

(a) Find the polynomials in the orbit of S_4 on R containing $x_1 + x_2$ (recall from Exercise 2.2.12 that the stabilizer of this polynomial has order 4).

(b) Find the polynomials in the orbit of S_4 on R containing $x_1x_2 + x_3x_4$ (recall from Exercise 2.2.12 that the stabilizer of this polynomial has order 8).

(c) Find the polynomials in the orbit of S_4 on R containing $(x_1 + x_2)(x_3 + x_4)$.

Solution.

(a) Note that the size of the orbit is given by $|S_4|/|G_{x_1+x_2}| = 24/4 = 6$. The polynomials in the orbit of S_4 on R containing $x_1 + x_2$ are

$$x_1 + x_2, x_1 + x_3, x_1 + x_4, x_2 + x_3, x_2 + x_4, x_3 + x_4$$

(b) The size of the orbit is 3. The polynomials in the orbit of S_4 on R containing $x_1x_2 + x_3x_4$ are

$$x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3$$

(c) Note that the stabilizer of $(x_1 + x_2)(x_3 + x_4)$ has order 8 (it is the same as that of $x_1x_2 + x_3x_4$). Thus, the size of the orbit is 3. The polynomials in the orbit of S_4 on R containing $(x_1 + x_2)(x_3 + x_4)$ are

$$(x_1 + x_2)(x_3 + x_4), (x_1 + x_3)(x_2 + x_4), (x_1 + x_4)(x_2 + x_3)$$ ■

(∗) Exercise 4.1.7

Let G be a transitive permutation group on the finite set A. A *block* is a nonempty subset B of A such that for all $\sigma \in G$ either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$ (here $\sigma(B) = \{\sigma(b) \mid b \in B\}$).

(a) Prove that if B is a block containing the element a of A, then the set G_B defined by $G_B = \{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of G containing G_a.

(b) Show that if B is a block and $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are all the distinct images of B under the elements of G, then these form a partition of A.

(c) A (transitive) group G on a set A is said to be *primitive* if the only blocks in A are the trivial ones: the sets of size 1 and A itself. Show that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Show that D_8 is not primitive as a permutation group on the four vertices of a square.

(d) Prove that the transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing G_a are G_a and G (i.e., G_a is a *maximal* subgroup of G, cf. Exercise 2.4.16). [Use part (a).]

Solution.

(a) We first show that G_B is a subgroup of G. Since $1(B) = B$, then $1 \in G_B$, hence it is nonempty. If $\sigma, \tau \in G$ such that $\sigma(B) = B$ and $\tau(B) = B$, we note that $\tau^{-1}(B) = B$ as well, hence $\sigma, \tau^{-1} \in G_B$. Then $(\sigma\tau^{-1})(B) = \sigma(\tau^{-1}(B)) = \sigma(B) = B$, so $\sigma\tau^{-1} \in G_B$. Hence $G_B \leq G$.

Now, let $a \in B$. If $\sigma \in G_a$, then $\sigma(a) = a$. Since $a \in B$, then $\sigma(a) \in \sigma(B)$. But $\sigma(a) = a \in B$, so $\sigma(B) \cap B \neq \emptyset$. By the definition of a block, this implies that $\sigma(B) = B$, hence $\sigma \in G_B$. Therefore, we have shown that $G_a \leq G_B$.

(b) Let B be a block and let $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ be all the distinct images of B under the elements of G. By transitivity of G on A, then for some $a \in A$, there exists $b \in B$ such that $\sigma(b) = a$. Then $a \in \sigma(B)$, and since $\sigma(B)$ is one of the sets $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$, it follows that

$$\bigcup_{i=1}^{n} \sigma_i(B) = A.$$

Suppose there existed $i \neq j$ where $\sigma_i(B) \cap \sigma_j(B) \neq \emptyset$. Then there are $b, b' \in B$ such that $\sigma_i(b) = \sigma_j(b')$, or $(\sigma_j^{-1}\sigma_i)(b) = b'$, hence $\sigma_j^{-1}\sigma_i(B) \cap B \neq \emptyset$. Since B is a block, then $\sigma_j^{-1}\sigma_i(B) = B$, hence $\sigma_i(B) = \sigma_j(B)$,

contradicting the assumption that they are distinct. Therefore, the sets $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are disjoint, and we conclude that they form a partition of A.

(c) Let $B \subset A$, i.e., a proper subset of A. If $|B| = 1$, then it is trivial. Suppose $|B| > 1$, and without loss of generality, let $1 \in B$ and some $1 \neq i \in B$ as well. Then there exists some $\sigma \in S_4$ such that $\sigma(1) = 1$ and $\sigma(i) = j$ for $j \notin B$. Then $\sigma(B) \cap B \neq \varnothing$ so that $\sigma(B) = B$, hence $j \in B$. We may repeat this to show that $B = A$, contradicting the assumption that B is a proper subset of A. Therefore, the only blocks in A are the trivial ones, and S_4 is primitive on A.

Now, consider D_8 acting on the four vertices of a square. Let B be the set containing the two opposite vertices. Then for any $\sigma \in D_8$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \varnothing$. Thus, B is a nontrivial block, and D_8 is not primitive in its action on the four vertices of a square.

(d) ($\Rightarrow$) If G is primitive on A. Let $H \leq G$ such that $G_a \leq H \leq G$, and let B be the orbit of H so that $B = H \cdot a$. Since $1 \in H$ because $H \leq G$, then $1 \cdot a = a \in B$. By part (a), we know that $a \in B$ implies $G_a \leq G_B$ so that B is now a block containing a. Primitivity of G implies that B is either $\{a\}$ or A itself. If $B = \{a\}$, then for any $\sigma \in H$, we have $\sigma \cdot a \in B$, hence $\sigma \cdot a = a$, so $\sigma \in G_a$. Therefore, $H \leq G_a$, and since $G_a \leq H$, then $H = G_a$. If $B = A$, then for any $b \in A$, there exists some $\sigma \in H$ such that $\sigma \cdot a = b$. Thus, for any $b \in A$, there exists some $\sigma \in H$ such that $\sigma(b) = a$, hence H is transitive on A. Therefore, $H = G$. We have shown that the only subgroups of G containing G_a are G_a and G.
($\Leftarrow$) Suppose now that G_a is maximal in G. Let B be a block of A that contains some $a \in A$. By part (a), we know that $G_a \leq G_B \leq G$. Maximality of G_a implies that either $G_B = G_a$ or $G_B = G$. If $G_B = G_a$, then for any $\sigma \in G_B$, we have $\sigma \in G_a$, hence $\sigma(a) = a$. Since $a \in B$, then $\sigma(a) \in \sigma(B)$, so $\sigma(a) \in B$. Therefore, $\sigma(a) = a \in B$, and it follows that $\sigma(B) \cap B \neq \varnothing$. By the definition of a block, this implies that $\sigma(B) = B$. Thus, for any $\sigma \in G_B$, we have $\sigma(B) = B$, so $B = \{a\}$. If $G_B = G$, then for any $b \in A$, there exists some $\sigma \in G$ such that $\sigma(a) = b$. Since $\sigma \in G_B$, then $\sigma(B) = B$, hence $b \in B$. Therefore, $B = A$. We have shown that the only blocks in A are the trivial ones, so G is primitive on A. ■

Exercise 4.1.8

A transitive permutation group G on a set A is called *doubly transitive* if for any (hence all) $a \in A$ the subgroup G_a is transitive on the set $A - \{a\}$.

(a) Prove that S_n is doubly transitive on $\{1, 2, \ldots, n\}$ for all $n \geq 2$.

(b) Prove that a doubly transitive group is primitive. Deduce that D_8 is not doubly transitive in its action on the 4 vertices of a square.

Solution.

(a) Let G_a be the stabilizer of $a \in \{1, 2, \ldots, n\}$. Note that G_a is the set of all permutations that fix a and permute the remaining $n - 1$ elements so that $G_a \cong S_{n-1}$. Since S_{n-1} is transitive on the set $\{1, 2, \ldots, n\} - \{a\}$ for all $n - 1 \geq 1$, then G_a is transitive on $A - \{a\}$ for all $n \geq 2$. Therefore, S_n is doubly transitive on $\{1, 2, \ldots, n\}$ for all $n \geq 2$.

(b) Let G be double transitive and let B be a block containing some $a \in A$. Take $b \in B$ such that $b \neq a$. Double transitivity of G implies that there exists some $\sigma \in G_a$ such that $\sigma(b) = c$ for any $c \in A - \{a\}$. Since $\sigma \in G_a$, then $\sigma(B) = B$, hence $c \in B$. Therefore, $B = A$, and we conclude that the only blocks in A are the trivial ones. Thus, G is primitive on A. Since D_8 is not primitive in its action on the four vertices of a square (as shown in part (c) of the previous exercise), then it is not doubly transitive. ■

(∗) Exercise 4.1.9

Assume G acts transitively on the finite set A and let H be a normal subgroup of G. Let $O_1, O_2, \ldots, O_r$ be the distinct orbits of H on A.

(a) Prove that G permutes the sets $O_1, O_2, \ldots, O_r$, in the sense that for each $g \in G$ and each $i \in \{1, \ldots, r\}$ there is a j such that $gO_i = O_j$, where $gO = \{g \cdot a \mid a \in O\}$ (i.e., in the notation of Exercise 7 the sets $O_1, \ldots, O_r$ are blocks). Prove that G is transitive on $\{O_1, \ldots, O_r\}$. Deduce that all orbits of H on A have the same cardinality.

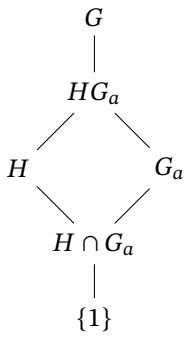
(b) Prove that if $a \in O_1$ then $|O_1| = |H : H \cap G_a|$ and prove that $r = |G : HG_a|$. [Draw the sublattice describing the Second Isomorphism Theorem for the subgroups H and G_a of G. Note that $H \cap G_a = H_a$.]

Solution.

(a) Let $g \in G$ and O_i be an orbit of H on A. Let $a \in O_i$ so that $O_i = H \cdot a = \{h \cdot a \mid h \in H\}$. Consider the set $gO_i = \{g \cdot (h \cdot a) \mid h \in H\}$. Since H is normal in G, then for any $h \in H$, we have $ghg^{-1} \in H$. Then $gO_i = H \cdot (g \cdot a)$, which is the orbit of H containing $g \cdot a$. Therefore, there exists some j such that $gO_i = O_j$.

To show that G is transitive on $\{O_1, \ldots, O_r\}$, let O_i and O_j be any two orbits of H on A. Since G is transitive on A, then for some $a \in O_i$ and $b \in O_j$, there exists some $g \in G$ such that $g \cdot a = b$. Then gO_i is the orbit of H containing b, hence $gO_i = O_j$. Therefore, G is transitive on $\{O_1, \ldots, O_r\}$. Since G is transitive on $\{O_1, \ldots, O_r\}$, then all orbits of H on A have the same cardinality.

(b) Suppose $a \in O_1$. By Proposition 4.2, we have $|O_1| = |H : H_a|$. Since $H_a = H \cap G_a$, then $|O_1| = |H : H \cap G_a|$. Moreover, the orbits of H partition A and have the same size by the previous solution, so we have $|A| = r|O_1|$. By applying Proposition 4.2 again, we have $|A| = |G : G_a|$. Therefore, $|G : G_a| = r|O_1| = r|H : H \cap G_a|$. By the Second Isomorphism Theorem, we also have that $H/(H \cap G_a) \cong HG_a/G_a$ so that $|H : H \cap G_a| = |HG_a : G_a|$. Now recall by Exercise 3.2.11 that $|G : K| = |G : H||H : K|$ for subgroups $K \leq H \leq G$. Applying this to the subgroups $G_a \leq HG_a \leq G$, we have $|G : G_a| = |G : HG_a||HG_a : G_a| = |G : HG_a||H : H \cap G_a|$. We then have $r|H : H \cap G_a| = |G : HG_a||H : H \cap G_a|$, or $r = |G : HG_a|$. Moreover, the sublattice is given as follows:



■

(∗) Exercise 4.1.10

Let H and K be subgroups of the group G. For each $x \in G$ define the HK *double coset* of x in G to be the set $HxK = \{hxk \mid h \in H, k \in K\}$.

(a) Prove that HxK is the union of the left cosets $x_1K, \ldots, x_nK$ where $\{x_1K, \ldots, x_nK\}$ is the orbit containing xK of H acting by left multiplication on the set of left cosets of K.

(b) Prove that HxK is a union of right cosets of H.

(c) Show that HxK and HyK are either the same set or are disjoint for all $x, y \in G$. Show that the set of HK double cosets partitions G.

(d) Prove that $|HxK| = |K| \cdot |H : H \cap xKx^{-1}|$.

(e) Prove that $|HxK| = |H| \cdot |K : K \cap x^{-1}Hx|$.

Solution.

(a) Let $\mathcal{O}$ be the orbit containing xK of H acting by left multiplication on the set of left cosets of K. Then $\mathcal{O} = \{hxK \mid h \in H\}$, and let $\{x_1K, \ldots, x_nK\}$ be the distinct left cosets in $\mathcal{O}$. Let $\mathcal{K}$ be the union of these left cosets, i.e., $\mathcal{K} = \bigcup_1^n x_iK$.

Now pick $y \in HxK$. Then there exist $h \in H$ and $k \in K$ such that $y = hxk$. Note that $hxK \in \mathcal{O}$, so there exists some i such that $hxK = x_iK$. Therefore, $y = hxk \in x_iK \subseteq \mathcal{K}$, hence $HxK \subseteq \mathcal{K}$. If $z \in \mathcal{K}$, then there exists some i and some $k' \in K$ such that $z = x_ik'$. Since $x_iK \in \mathcal{O}$, then there exists some $h' \in H$ such that $x_iK = h'xK$, hence $x_i = h'xk''$ for some $k'' \in K$. Therefore, $z = x_ik' = h'xkk'' \in HxK$, so $\mathcal{K} \subseteq HxK$. We have shown that $HxK = \mathcal{K}$, i.e., HxK is the union of the left cosets $x_1K, \ldots, x_nK$.

(b) The proof is similar to that of part (a).

(c) Let $x, y \in G$. Suppose $HxK \cap HyK \neq \emptyset$. Then there exist $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $h_1xk_1 = h_2yk_2$. Rearranging, we have $y = h_2^{-1}h_1xk_1k_2^{-1}$, hence $y \in HxK$. Therefore, $HyK \subseteq HxK$. By symmetry, we also have $HxK \subseteq HyK$, so $HxK = HyK$. We have shown that HxK and HyK are either the same set or are disjoint for all $x, y \in G$. Since every element of G is in some double coset of the form HxK, then the set of HK double cosets partitions G.

(d) Recall that the orbit of xK under this action is $\mathcal{O} = \{hxK \mid h \in H\}$. By Proposition 4.2, we have $|\mathcal{O}| = |H : H_{xK}|$, where H_{xK} is the stabilizer of xK in H. Observe that $H_{xK} = \{h \in H \mid hxK = xK\}$. Then $hxK = xK$ implies that there exists some $k \in K$ such that $hxk = x$, or equivalently, $h = xkx^{-1}$. Therefore, $H_{xK} = H \cap xKx^{-1}$. By part (a), we have $|HxK| = |\mathcal{O}| \cdot |K| = |H : H \cap xKx^{-1}| \cdot |K|$.

(e) Similar to part (d). ■

4.2 Groups Acting on Themselves by Left Mutliplication—Cayley's Theorem

Exercise 4.2.1

Let G be $\{1, a, b, c\}$, the Klein 4-group whose group table is written out in Section 2.5.

(a) Label $1, a, b, c$ with the integers $1, 2, 4, 3$, respectively, and prove that under the left regular representation of G into S_4 the nonidentity elements are mapped as follows:

$$a \mapsto (1\,2)(3\,4), \quad b \mapsto (1\,4)(2\,3), \quad c \mapsto (1\,3)(2\,4).$$

(b) Relabel $1, a, b, c$ as $1, 4, 2, 3$, respectively, and compute the image of each element of G under the left regular representation of G into S_4. Show that the image of G in S_4 under this labelling is the same *subgroup* as the image of G in part (a) (even though the nonidentity elements individually map to different permutations under the two different labellings).

Solution.

(a) We have $a \cdot 1 = a$ so that $\sigma_a(1) = 2$. Similarly, $\sigma_a(2) = 1$. We also have $a \cdot b = c$ so that $\sigma_a(4) = 3$, and $\sigma_a(3) = 4$, and we have $a \mapsto (1\,2)(3\,4)$. The others are computed similarly.

(b) Again, we have $a \cdot 1 = a$ so that $\sigma_a(1) = 4$. Similarly, $\sigma_a(4) = 1$. We also have $a \cdot b = c$ so that $\sigma_a(2) = 3$, and $\sigma_a(3) = 2$, and we have $a \mapsto (1\,4)(2\,3)$. For b, we have $b \mapsto (1\,2)(3\,4)$, and for c, we have $c \mapsto (1\,3)(2\,4)$. The image of G in S_4 under this labelling is $\{1, (1\,4)(2\,3), (1\,2)(3\,4), (1\,3)(2\,4)\}$, which is the same subgroup as in part (a). ■

Exercise 4.2.2

List the elements of S_3 as $1, (1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)$ and label these with the integers $1, 2, 3, 4, 5, 6$ respectively. Exhibit the image of each element of S_3 under the left regular representation of S_3 into S_6.

Solution. Consider $(1\,2)$. Then we have the following computations:

$$\begin{aligned}
(1\,2) \cdot 1 &= (1\,2) & \sigma_{(1\,2)}(1) &= 2\\
(1\,2) \cdot (1\,2) &= 1 & \sigma_{(1\,2)}(2) &= 1\\
(1\,2) \cdot (2\,3) &= (1\,3\,2) & \sigma_{(1\,2)}(4) &= 5\\
(1\,2) \cdot (1\,3) &= (1\,2\,3) & \sigma_{(1\,2)}(3) &= 6\\
(1\,2) \cdot (1\,2\,3) &= (2\,3) & \sigma_{(1\,2)}(5) &= 3\\
(1\,2) \cdot (1\,3\,2) &= (1\,3) & \sigma_{(1\,2)}(6) &= 4
\end{aligned}$$

Thus, we have $(1\,2) \mapsto (1\,2)(3\,6\,4\,5)$. We calculate that $(2\,3) \mapsto (1\,3\,5\,2)(4\,6)$. Since $(1\,2)(2\,3) = (1\,2\,3)$, then

$$(1\,2\,3) \mapsto (1\,2)(3\,6\,4\,5)(1\,3\,5\,2)(4\,6) = (1\,5\,6)(2\,4\,3)$$

Continuing in this way, we find that the images of the elements of S_3 under the left regular representation are as follows:

$$\begin{aligned}
1 &\mapsto 1\\
(1\,2) &\mapsto (1\,2)(3\,6\,4\,5)\\
(2\,3) &\mapsto (1\,3\,5\,2)(4\,6)\\
(1\,3) &\mapsto (1\,4)(2\,6)(3\,5)\\
(1\,2\,3) &\mapsto (1\,5\,6)(2\,4\,3)\\
(1\,3\,2) &\mapsto (1\,6\,5)(2\,3\,4)
\end{aligned}$$

■

Exercise 4.2.3

Let r and s be the usual generators for the dihedral group of order 8.

(a) List the elements of D_8 as $1, r, r^2, r^3, s, sr, sr^2, sr^3$ and label these with the integers $1, 2, \ldots, 8$ respectively. Exhibit the image of each element of D_8 under the left regular representation of D_8 into S_8.

(b) Relabel this same list of elements of D_8 with the integers $1, 3, 5, 7, 2, 4, 6, 8$ respectively and recompute the image of each element of D_8 under the left regular representation with respect to this new labelling. Show that the two subgroups of S_8 obtained in parts (a) and (b) are different.

Solution.

(a) We calculate $\sigma_r = (1\ 2\ 3\ 4)(5\ 8\ 7\ 6)$ and $\sigma_s = (1\ 5)(2\ 6)(3\ 7)(4\ 8)$. Continuing in this way, we find that the images of the elements of D_8 under the left regular representation are as follows:

$$\begin{aligned} 1 &\mapsto 1 & s &\mapsto (1\ 5)(2\ 6)(3\ 7)(4\ 8) \\ r &\mapsto (1\ 2\ 3\ 4)(5\ 8\ 7\ 6) & sr &\mapsto (1\ 6)(2\ 7)(3\ 8)(4\ 5) \\ r^2 &\mapsto (1\ 3)(2\ 4)(5\ 7)(6\ 8) & sr^2 &\mapsto (1\ 7)(2\ 8)(3\ 5)(4\ 6) \\ r^3 &\mapsto (1\ 4\ 3\ 2)(5\ 6\ 7\ 8) & sr^3 &\mapsto (1\ 8)(2\ 5)(3\ 6)(4\ 7) \end{aligned}$$

(b) The images of D_8 under the left regular representation with respect to this new labelling are as follows:

$$\begin{aligned} 1 &\mapsto 1 & s &\mapsto (1\ 2)(3\ 4)(5\ 6)(7\ 8) \\ r &\mapsto (1\ 3\ 5\ 7)(2\ 8\ 6\ 4) & sr &\mapsto (1\ 4)(2\ 7)(3\ 6)(5\ 8) \\ r^2 &\mapsto (1\ 5)(3\ 7)(2\ 6)(4\ 8) & sr^2 &\mapsto (1\ 6)(2\ 5)(3\ 8)(4\ 7) \\ r^3 &\mapsto (1\ 7\ 5\ 3)(2\ 4\ 6\ 8) & sr^3 &\mapsto (1\ 8)(2\ 3)(4\ 5)(6\ 7) \end{aligned}$$

Clearly, the two subgroups of S_8 obtained in parts (a) and (b) are different since, for example, the image of r in part (a) is a product of two 4-cycles while the image of r in part (b) is a product of two 4-cycles but with different elements. ■

Exercise 4.2.4

Use the left regular representation of Q_8 to produce two elements of S_8 which generate a subgroup of S_8 isomorphic to the quaternion group Q_8.

Solution. At minimum, we have that $Q_8 = \langle i, j \rangle$ (any 2 elements of order 4 can be used), so we compute the images of i and j under the left regular representation. We label Q_8 as $1, -1, i, -i, j, -j, k, -k$ and label these with the integers $1, 2 \ldots 8$ respectively. We find that

$$\begin{aligned} i &\mapsto \sigma_i = (1\ 3\ 4\ 2)(5\ 7)(6\ 8) \\ j &\mapsto \sigma_j = (1\ 5\ 2\ 6)(3\ 8)(4\ 7) \end{aligned}$$

Hence $Q_8 \cong \langle \sigma_i, \sigma_j \rangle \leq S_8$. ■

Exercise 4.2.5

Let r and s be the usual generators for the dihedral group of order 8 and let $H = \langle s \rangle$. List the left cosets of H in D_8 as $1H, rH, r^2H$ and r^3H.

(a) Label these cosets with the integers $1, 2, 3, 4$, respectively. Exhibit the image of each element of D_8 under the representation π_H of D_8 into S_4 obtained from the action of D_8 by left multiplication on the set of 4 left cosets of H in D_8. Deduce that this representation is faithful (i.e., the elements of S_4 obtained form a subgroup isomorphic to D_8).

(b) Repeat part (a) with the list of cosets relabelled by the integers $1, 3, 2, 4$, respectively. Show that the permutations obtained from this labelling form a subgroup of S_4 that is different from the subgroup obtained in part (a).

(c) Let $K = \langle sr \rangle$, list the cosets of K in D_8 as $1K, rK, r^2K$ and r^3K, and label these with the integers $1, 2, 3, 4$. Prove that, with respect to this labelling, the image of D_8 under the representation π_K obtained from left multiplication on the cosets of K is the same *subgroup* of S_4 as in part (a) (even though the subgroups H and K are different and some of the elements of D_8 map to different permutations under the two homomorphisms).

Solution.

(a) We have $\pi_H(r) = (1\,2\,3\,4)$ and $\pi_H(s) = (2\,4)$. We continue in this way to find that the images of the elements of D_8 under π_H are:

$$\begin{aligned} \pi_H(1) &= 1 & \pi_H(s) &= (2\,4) \\ \pi_H(r) &= (1\,2\,3\,4) & \pi_H(sr) &= (1\,2)(3\,4) \\ \pi_H(r^2) &= (1\,3)(2\,4) & \pi_H(sr^2) &= (1\,3) \\ \pi_H(r^3) &= (1\,4\,3\,2) & \pi_H(sr^3) &= (1\,4)(2\,3) \end{aligned}$$

so that the subgroup $\langle \pi_H(r), \pi_H(s) \rangle \leq S_4$ is isomorphic to D_8. Since the kernel of π_H is trivial, then the representation is faithful.

(b) The new labelling affords the permutations $\pi_H(r) = (1\,3\,2\,4)$ and $\pi_H(s) = (3\,4)$. We have the following images:

$$\begin{aligned} \pi_H(1) &= 1 & \pi_H(s) &= (3\,4) \\ \pi_H(r) &= (1\,3\,2\,4) & \pi_H(sr) &= (1\,3)(2\,4) \\ \pi_H(r^2) &= (1\,2)(3\,4) & \pi_H(sr^2) &= (1\,2) \\ \pi_H(r^3) &= (1\,4\,2\,3) & \pi_H(sr^3) &= (1\,4)(2\,3) \end{aligned}$$

Moreover, the subgroup is different from that in part (a) since, for example, the image of r in part (a) is $(1\,2\,3\,4)$ while the image of r in this part is $(1\,3\,2\,4)$.

(c) Under π_K, we have $\pi_K(r) = (1\,2\,3\,4)$ and $\pi_K(s) = (1\,2)(3\,4)$. With respect to this labeling, we have the subgroup $\widehat{K} = \langle (1\,2\,3\,4), (1\,2)(3\,4) \rangle$. Let $\widehat{H}$ be the subgroup obtained in part (a). Note that $(1\,2\,3\,4)$ is contained in both $\widehat{H}$ and $\widehat{K}$. Moreover, we have following:

$$(1\,2\,3\,4)(2\,4)(1\,4\,3\,2) = (1\,2)(3\,4) \in \widehat{H} \quad \text{and} \quad (1\,2\,3\,4)^2(1\,2)(3\,4) = (2\,4) \in \widehat{K}$$

so that both subgroups contain the other generator of the other subgroup. Therefore, $\widehat{H} = \widehat{K}$. ■

Exercise 4.2.6

Let r and s be the usual generators for the dihedral group of order 8 and let $N = \langle r^2 \rangle$. List the left cosets of N in D_8 as $1N, rN, sN$ and srN. Label these cosets with the integers $1, 2, 3, 4$ respectively. Exhibit the image of each element of D_8 under the representation π_N of D_8 into S_4 obtained from the action of D_8 by left multiplication on the set of 4 left cosets of N in D_8. Deduce that this representation is not faithful and prove that $\pi_N(D_8)$ is isomorphic to the Klein 4-group.

Solution. We have $\pi_N(r) = (1\ 2)(3\ 4)$ and $\pi_N(s) = (1\ 3)(2\ 4)$. Continuing in this way, we find that the images of the elements of D_8 under π_N are:

$$\begin{aligned} \pi_N(1) &= 1 & \pi_N(s) &= (1\ 3)(2\ 4) \\ \pi_N(r) &= (1\ 2)(3\ 4) & \pi_N(sr) &= (1\ 4)(2\ 3) \\ \pi_N(r^2) &= 1 & \pi_N(sr^2) &= (1\ 3)(2\ 4) \\ \pi_N(r^3) &= (1\ 2)(3\ 4) & \pi_N(sr^3) &= (1\ 4)(2\ 3) \end{aligned}$$

Since $\ker(\pi_N)$ contains the nontrivial element r^2, then the representation is not faithful. Moreover, we have $\pi_N(D_8) = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, which is isomorphic to the Klein 4-group. ■

Exercise 4.2.7

Let Q_8 be the quaternion group of order 8.

(a) Prove that Q_8 is isomorphic to a subgroup of S_8.

(b) Prove that Q_8 is not isomorphic to a subgroup of S_n for any $n \leq 7$. [If Q_8 acts on any set A of order ≤ 7 show that the stabilizer of any point $a \in A$ must contain the subgroup $\langle -1 \rangle$.]

Solution.

(a) This is done in Exercise 4.2.4.

(b) Let Q_8 act on a set A of order $n \leq 7$. For any $a \in A$, consider the orbit $\mathcal{O}_a$ of a under this action. By Proposition 4.2, we have $|\mathcal{O}_a| = |Q_8 : (Q_8)_a|$, where $(Q_8)_a$ is the stabilizer of a in Q_8. Since $|\mathcal{O}_a|$ divides $|A| \leq 7$, then $|\mathcal{O}_a|$ must be 1, 2, 4, or 7. However, since Q_8 has no subgroup of index 7, then $|\mathcal{O}_a|$ cannot be 7. If $|\mathcal{O}_a| = 4$, then $(Q_8)_a$ has order 2, but the only subgroup of order 2 in Q_8 is $\langle -1 \rangle$. If $|\mathcal{O}_a| = 2$, then $(Q_8)_a$ has order 4, and the only subgroups of order 4 in Q_8 are $\langle i \rangle$, $\langle j \rangle$, and $\langle k \rangle$, all of which contain $\langle -1 \rangle$. If $|\mathcal{O}_a| = 1$, then $(Q_8)_a = Q_8$, which also contains $\langle -1 \rangle$. Therefore, in all cases, the stabilizer $(Q_8)_a$ contains $\langle -1 \rangle$. Since this holds for all $a \in A$, then $\langle -1 \rangle$ is contained in the kernel of the action. The action is not faithful, hence Q_8 cannot be isomorphic to a subgroup of S_n for any $n \leq 7$. ■

Exercise 4.2.8

Prove that if H has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.

Solution. Let G act by left multiplication on the set of left cosets of H in G. Then we have the homomorphism $\varphi : G \to S_n$, which is the permutation representation of G on G/H. Let $K = \ker(\varphi) \subseteq H$, since $g \in K$ if and only if $gH = H$. By the First Isomorphism Theorem, we have $G/K \cong \varphi(G) \leq S_n$, so that $|G : K| = |G/K| = |\varphi(G)|$ divides $n!$. Therefore, $|G : K| \leq n!$. ■

Exercise 4.2.9

Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

Solution. Let H be a subgroup of G with index p. Then $|G : H| = p$, so the action of G on the left cosets of H in G gives a homomorphism $\varphi : G \to S_p$. Since $|G| = p^\alpha$, then by Lagrange's Theorem, the order of $\varphi(G)$ divides p^α. However, the only subgroups of S_p whose order divides p^α are the trivial group and groups of order p. Since $\varphi(G)$ acts transitively on the p cosets of H, then $\varphi(G)$ cannot be trivial. Therefore, $|\varphi(G)| = p$, which is prime, so $\varphi(G)$ is cyclic and hence abelian. The kernel of φ is a normal subgroup of G contained in H. Since the image $\varphi(G)$ has order p, then by the First Isomorphism Theorem, we have $|G : \ker(\varphi)| = p$. But since $\ker(\varphi) \subseteq H$ and both have index p, then $\ker(\varphi) = H$. Therefore, H is normal in G.

To deduce that every group of order p^2 has a normal subgroup of order p, let G be a group of order p^2. By Cauchy's Theorem, there exists an element of order p in G, which generates a subgroup H of order p. Since the index of H in G is p, by the previous result, H is normal in G. ■

Exercise 4.2.10

Prove that every non-abelian group of order 6 has a nonnormal subgroup of order 2. Use this to classify groups of order 6. [Produce an injective homomorphism into S_3.]

Solution. Note that $2 \mid 6$ and $3 \mid 6$. By Cauchy's Theorem, there exists subgroups H and K of orders 2 and 3 respectively. Let $H = \{1, h\}$, suppose it is normal, and let $g \in G - H$. Since $H \trianglelefteq G$, then $gHg^{-1} = H$. In particular, $ghg^{-1} \in H$, so either $ghg^{-1} = 1$ or $ghg^{-1} = h$. Since the first case implies $h = 1$, it must be that $ghg^{-1} = h$, or $gh = hg$. Then h commutes with every element. Moreover, we may use Exercise 3.3.3 to conclude that $G = HK$ since $H \trianglelefteq G$. Since K is also abelian as it is cyclic, then $G = hk$ for $h \in H$ and $k \in K$, implying that G is abelian, a contradiction. Therefore, H is not normal in G.

To classify groups of order 6, let G be a group of order 6. If G is abelian, then $G \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. If G is non-abelian, then by the above result, G has a nonnormal subgroup H of order 2. Let K be the subgroup of order 3. Then $G = HK$. Let G act by left multiplication on the left cosets of K in G. This action gives a homomorphism $\varphi : G \to S_3$. Since H is not normal in G, then the action is nontrivial, so φ is injective. Therefore, $G \cong \varphi(G) \leq S_3$. Since $|G| = 6 = |S_3|$, then $\varphi(G) = S_3$, and hence $G \cong S_3$. ■

Exercise 4.2.11

Let G be a finite group and let $\pi : G \to S_G$ be the left regular representation. Prove that if x is an element of G of order n and $|G| = mn$, then $\pi(x)$ is a product of m n-cycles. Deduce that $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $|G|/|x|$ is odd.

Solution. Let $x \in G$ with $|x| = n$. Consider the action of $\langle x \rangle$ on G by left multiplication. The orbit of any $g \in G$ under this action is $O_g = \{x^k g \mid k = 0, 1, \ldots, n-1\}$. Since $|x| = n$, then $|O_g| = n$ for all $g \in G$. By Proposition 4.2, we have $|O_g| = |\langle x \rangle : (\langle x \rangle)_g|$, where $(\langle x \rangle)_g$ is the stabilizer of g in $\langle x \rangle$. Since $|O_g| = n$, then $(\langle x \rangle)_g$ is trivial for all $g \in G$. Therefore, the orbits of this action partition G into subsets of size n. Since $|G| = mn$, there are exactly m such orbits. Each orbit corresponds to an n-cycle in the permutation $\pi(x)$. Therefore, $\pi(x)$ is a product of m n-cycles.

To determine when $\pi(x)$ is an odd permutation, we note that an n-cycle is an odd permutation if and only if n is even. Since $\pi(x)$ is a product of m n-cycles, the parity of $\pi(x)$ is determined by the parity of m and n. Specifically, $\pi(x)$ is odd if and only if n is even and m is odd. Thus, $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $|G|/|x|$ is odd. ■

Exercise 4.2.12

Let G and π be as in the preceding exercise. Prove that if $\pi(G)$ contains an odd permutation then G has a subgroup of index 2. [Use Exercise 3.3.3.]

Solution. Recall the ϵ homomorphism from Proposition 3.23. Moreover, π is a homomorphism from G to S_G. Consider the composition $\epsilon \circ \pi : G \to \{\pm 1\}$. Since $\pi(G)$ contains an odd permutation, then $\epsilon \circ \pi$ is surjective. By the First Isomorphism Theorem, we have $G/\ker(\epsilon \circ \pi) \cong \{\pm 1\}$, so that $|\ker(\epsilon \circ \pi)| = |G|/2$. Therefore, $\ker(\epsilon \circ \pi)$ is a subgroup of G of index 2. ■

Exercise 4.2.13

Prove that if $|G| = 2k$ where k is odd then G has a subgroup of index 2. [Use Cauchy's Theorem to produce an element of order 2 and then use the preceding two exercises.]

Solution. By Cauchy's Theorem, there exists $x \in G$ such that $|x| = 2$. Then $\pi(x)$ is of order 2 and is hence a product of disjoint transpositions. Since $|G| = 2k$ with k odd, then use $m = k$ and $n = 2$ in Exercise 4.2.11 along with even $|x|$ to conclude that $\pi(x)$ is an odd permutation. By the Exercise 4.2.12, G has a subgroup of index 2. ■

Exercise 4.2.14

Let G be a finite group of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n. Prove that G is not simple.

Solution. Let S be the set of all prime factors of n. By the Well Ordering Principle, this has a minimal element p. By hypothesis, G has a subgroup P of order n/p with index p. By Corollary 4.5, P is normal in G since p is the smallest prime dividing n. Therefore, G is not simple. ■

4.3 Groups Acting on Themselves by Conjugation—The Class Equation

Let G be a group.

(∗) Exercise 4.3.1

Suppose G has a left action on a set A, denoted by $g \cdot a$ for all $g \in G$ and $a \in A$. Denote the corresponding right action on A by $a \cdot g$. Prove that the (equivalence) relations $\sim$ and $\sim'$ defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \quad \text{for some } g \in G$$

and

$$a \sim' b \quad \text{if and only if} \quad a = b \cdot g \quad \text{for some } g \in G$$

are the same relation (i.e., $a \sim b$ if and only if $a \sim' b$).

Solution. If $a \sim b$, there exists $g \in G$ such that $a = g \cdot b$. Let $h = g^{-1}$. Then $b = h \cdot a$, so $a = b \cdot g$. Thus, $a \sim' b$. Conversely, if $a \sim' b$, there exists $g \in G$ such that $a = b \cdot g$. Let $h = g^{-1}$. Then $b = h \cdot a$, so $a = g \cdot b$. Thus, $a \sim b$. Therefore, the relations $\sim$ and $\sim'$ are the same. ■

Exercise 4.3.2

Find all conjugacy classes and their sizes in the following groups:

(a) D_8 (b) Q_8 (c) A_4

Solution.

(a) Discussed in the text, the conjugacy classes of D_8 are $\{1\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, sr^2\}$, and $\{sr, sr^3\}$ with sizes 1, 1, 2, 2, and 2 respectively.

(b) Again discussed in the text, the conjugacy classes of Q_8 are $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, and $\{k, -k\}$ with sizes 1, 1, 2, 2, and 2 respectively.

(c) We proceed similarly as the text. The possible cycle types are 1, (1 2 3), and (1 2)(3 4).

For (1 2 3), we have $C_{A_4}((1\,2\,3)) = \langle (1\,2\,3) \rangle$ since the only permutation that fixes 1, 2, and 3 is the identity. Therefore, the conjugacy class of (1 2 3) has size $12/3 = 4$. However, there are 8 3-cycles in A_4, so there exists a 3-cycle $\sigma \in A_4$ not in the conjugacy class of (1 2 3). By similar reasoning, the conjugacy class of σ also has size 4. There are then 2 conjugacy classes of size 4 corresponding to the 3-cycles.

For (1 2)(3 4), it is trivial to calculate that the remaining double transpositions are in its conjugacy class. Therefore, the conjugacy class of (1 2)(3 4) has size 3. ■

Exercise 4.3.3

Find all conjugacy classes and their sizes in the following groups:
(a) $Z_2 \times S_3$ (b) $S_3 \times S_3$ (c) $Z_3 \times A_4$

Solution. We first prove a (somewhat) trivial idea: if G and H are groups, let $g \in G$ and $h \in H$. Let $\mathcal{K}_g$ and $\mathcal{K}_h$ be the conjugacy classes of g in G and h in H respectively. Then $\mathcal{K}_{(g,h)} = \mathcal{K}_g \times \mathcal{K}_h$ is the conjugacy class of (g,h) in $G \times H$. To see this, note that for any $(x,y) \in G \times H$, we have

$$(x,y)(g,h)(x,y)^{-1} = (xgx^{-1}, yhy^{-1}) \in \mathcal{K}_g \times \mathcal{K}_h.$$

Conversely, for any $(g',h') \in \mathcal{K}_g \times \mathcal{K}_h$, there exist $x \in G$ and $y \in H$ such that $g' = xgx^{-1}$ and $h' = yhy^{-1}$. Therefore, $(g',h') = (x,y)(g,h)(x,y)^{-1}$, so (g',h') is in the conjugacy class of (g,h) in $G \times H$. This result shows two important things: the conjugacy classes of $G \times H$ are precisely the products of the conjugacy classes of G and H, and the size of the conjugacy class of (g,h) in $G \times H$ is the product of the sizes of the conjugacy classes of g in G and h in H. We now use this to answer the question.

(a) Let $Z_2 = \langle x \rangle$. The conjugacy classes $\mathcal{K}_1$ and $\mathcal{K}_x$ of Z_2 have sizes 1 and 1 respectively. For S_3, the partitions of 3 are 3 1-cycles, 2-cycle and 1-cycle, and a 3-cycle with representatives 1, (1 2), and (1 2 3) respectively. Since $C_{S_3}((1\,2)) = \langle (1\,2) \rangle$ and $C_{S_3}((1\,2\,3)) = \langle (1\,2\,3) \rangle$, then the conjugacy classes $\mathcal{K}_1$, $\mathcal{K}_{(1\,2)}$, and $\mathcal{K}_{(1\,2\,3)}$ of S_3 have sizes 1, 3, and 2 respectively. Therefore, $Z_2 \times S_3$ has 6 conjugacy classes of size 1, 3, 2, 1, 3, and 2 respectively.

(b) By the above, S_3 has 3 conjugacy classes of sizes 1, 3, and 2 respectively. Then $S_3 \times S_3$ has 9 conjugacy classes with sizes 1, 3, 2, 3, 9, 6, 2, 6, and 4 respectively.

(c) Z_3 has 3 conjugacy classes of size 1 each. From Exercise 4.3.2, we know that A_4 has 4 conjugacy classes of sizes 1, 4, 4, and 3. Therefore, $Z_3 \times A_4$ has 12 conjugacy classes with sizes 1, 4, 4, 3, 1, 4, 4, 3, 1, 4, 4, and 3 respectively. ■

Exercise 4.3.4

Prove that if $S \subseteq G$ and $g \in G$ then $gN_G(S)g^{-1} = N_G(gSg^{-1})$ and $gC_G(S)g^{-1} = C_G(gSg^{-1})$.

Solution. Suppose $x \in gN_G(S)g^{-1}$, and consider $xgSg^{-1}x^{-1}$. Since $x = gng^{-1}$ for some $n \in N_G(S)$, then we have $gng^{-1}gSg^{-1}gn^{-1}g^{-1} = gnSn^{-1}g^{-1} = gSg^{-1}$, so that $x \in N_G(gSg^{-1})$. Conversely, suppose $x \in N_G(gSg^{-1})$. Then $xgSg^{-1}x^{-1} = gSg^{-1}$. Letting $n = g^{-1}xg$, we have $nSn^{-1} = S$, so $n \in N_G(S)$ and hence $x \in gN_G(S)g^{-1}$. Therefore, $gN_G(S)g^{-1} = N_G(gSg^{-1})$.

Suppose $x \in gC_G(S)g^{-1}$, and consider xsx^{-1} for some $s \in gSg^{-1}$. Since $x = gng^{-1}$ for some $n \in C_G(S)$, then we have $gng^{-1}sgn^{-1}g^{-1} = gn(g^{-1}sg)n^{-1}g^{-1} = g(g^{-1}sg)g^{-1} = s$, so that $x \in C_G(gSg^{-1})$. Conversely, suppose $x \in C_G(gSg^{-1})$. Then $xsx^{-1} = s$ for all $s \in gSg^{-1}$. Letting $n = g^{-1}xg$, we have $ntn^{-1} = t$ for all $t \in S$, so $n \in C_G(S)$ and hence $x \in gC_G(S)g^{-1}$. Therefore, $gC_G(S)g^{-1} = C_G(gSg^{-1})$. ■

Exercise 4.3.5

If the center of G is of index n, prove that every conjugacy class has at most n elements.

Solution. Let $\mathcal{K}_g$ be the conjugacy class of some $g \in G$. By Proposition 4.6, we have $|\mathcal{K}_g| = |G : C_G(g)|$. Since $Z(G) \leq C_G(g)$ for all $g \in G$, Lagrange's Theorem shows that $|Z(G)|$ divides $|C_G(g)|$. Therefore, $|G : C_G(g)|$ divides $|G : Z(G)| = n$. Hence, $|\mathcal{K}_g| \leq n$. ■

(∗) Exercise 4.3.6

Assume G is a non-abelian group of order 15. Prove that $Z(G) = 1$. Use the fact that $\langle g \rangle \leq C_G(g)$ for all $g \in G$ to show that there is at most one possible class equation for G. [Use Exercise 3.1.36.]

Solution. Recall that $Z(G) \leq G$. Since G is non-abelian, then $Z(G) \neq G$. Assume $1 < Z(G) < 15$. By Lagrange's Theorem, $Z(G)$ has order 3 or 5. If $|Z(G)| = 3$, then $|G/Z(G)| = 5$ and $G/Z(G) \cong Z_5$. If $|Z(G)| = 5$, then $|G/Z(G)| = 3$ and $G/Z(G) \cong Z_3$. In either case, $G/Z(G)$ is cyclic by Corollary 3.10, and Exercise 3.1.36 implies that G is abelian, a contradiction. Therefore, $Z(G) = 1$.

Now suppose $g \in G$ is nonidentity. Since $\langle g \rangle \leq C_G(g)$, then $|C_G(g)|$ is 3, 5, or 15 by Lagrange's Theorem. If $|C_G(g)| = 15$, then $C_G(g) = G$, so $g \in Z(G)$, a contradiction. Therefore, $|C_G(g)|$ is 3 or 5 for all nonidentity $g \in G$. By Proposition 4.6, we have $|\mathcal{K}_g| = |G : C_G(g)|$, so that $|\mathcal{K}_g|$ is 5 or 3 respectively. The identity element forms a conjugacy class of size 1, and the class equation must involve a summation of sizes 3 and 5 that adds to 14. The only such combination is three classes of size 3 and one class of size 5. Therefore, the class equation of G is $15 = 1 + 3 + 3 + 3 + 5$. ■

Exercise 4.3.7

For $n = 3, 4, 6$, and 7 make lists of the partitions of n and give representatives for the corresponding conjugacy classes of S_n.

Solution. $n = 3$:

Partition of 3	Representative of Cycle Type
1, 1, 1	1
2, 1	(1 2)
3	(1 2 3)

$n = 4$:

Partition of 4	Representative of Cycle Type
1, 1, 1, 1	1
2, 1, 1	(1 2)
2, 2	(1 2)(3 4)
3, 1	(1 2 3)
4	(1 2 3 4)

$n = 6$:

Partition of 6	Representative of Cycle Type
1, 1, 1, 1, 1, 1	1
2, 1, 1, 1, 1	(1 2)
2, 2, 1, 1	(1 2)(3 4)
2, 2, 2	(1 2)(3 4)(5 6)
3, 1, 1, 1	(1 2 3)
3, 2, 1	(1 2 3)(4 5)
3, 3	(1 2 3)(4 5 6)
4, 1, 1	(1 2 3 4)
4, 2	(1 2 3 4)(5 6)
5, 1	(1 2 3 4 5)
6	(1 2 3 4 5 6)

$n = 7$:

Partition of 7	Representative of Cycle Type
1, 1, 1, 1, 1, 1, 1	1
2, 1, 1, 1, 1, 1	(1 2)
2, 2, 1, 1, 1	(1 2)(3 4)
2, 2, 2, 1	(1 2)(3 4)(5 6)
3, 1, 1, 1, 1	(1 2 3)
3, 2, 1, 1	(1 2 3)(4 5)
3, 2, 2	(1 2 3)(4 5)(6 7)
3, 3, 1	(1 2 3)(4 5 6)
4, 1, 1, 1	(1 2 3 4)
4, 2, 1	(1 2 3 4)(5 6)
4, 3	(1 2 3 4)(5 6 7)
5, 1, 1	(1 2 3 4 5)
5, 2	(1 2 3 4 5)(6 7)
6, 1	(1 2 3 4 5 6)
7	(1 2 3 4 5 6 7)

■

Exercise 4.3.8

Prove that $Z(S_n) = 1$ for all $n \geq 3$.

Solution. Suppose $\sigma \in Z(S_n)$ for some $n \geq 3$. Then σ commutes with every element of S_n. In particular, σ commutes with all transpositions (the set of which generate S_n). Let $(a\ b)$ be any transposition in S_n. Then we have $\sigma(a\ b)\sigma^{-1} = (a\ b)$. This implies that $(\sigma(a)\ \sigma(b)) = (a\ b)$, so $\sigma(a) = a$ and $\sigma(b) = b$. Since a and b were arbitrary, σ fixes every element of $\{1, 2, \ldots, n\}$. Therefore, σ is the identity permutation. Hence, $Z(S_n) = \{1\}$ for all $n \geq 3$. ■

Exercise 4.3.9

Show that $|C_{S_n}((1\ 2)(3\ 4))| = 8(n-4)!$ for all $n \geq 4$. Determine the elements in this centralizer explicitly.

Solution. The $(n-4)!$ factor arises from the fact that permutations on the $n-4$ integers not involved in the cycle $(1\ 2)(3\ 4)$ commute with it. Therefore, we need only consider the permutations of $\{1, 2, 3, 4\}$ that commute with $(1\ 2)(3\ 4)$. Computing $C_{S_4}((1\ 2)(3\ 4))$ directly, the permutations that fall in this set need to leave $(1\ 2)(3\ 4)$ unchanged, or swap the two transpositions. The permutations that leave $(1\ 2)(3\ 4)$ unchanged are 1, $(1\ 2)$, $(3\ 4)$, and $(1\ 2)(3\ 4)$. The permutations that swap the two transpositions are $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$, $(1\ 3\ 2\ 4)$, and $(1\ 4\ 2\ 3)$. Therefore,

$$C_{S_4}((1\ 2)(3\ 4)) = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\},$$

which has size 8. Combining this with the $(n-4)!$ factor, we have $|C_{S_n}((1\ 2)(3\ 4))| = 8(n-4)!$ for all $n \geq 4$. ■

Exercise 4.3.10

Let σ be the 5-cycle $(1\ 2\ 3\ 4\ 5)$ in S_5. In each of (a) to (c) find an explicit element $\tau \in S_5$ which accomplishes the specified conjugation:

(a) $\tau\sigma\tau^{-1} = \sigma^2$

(b) $\tau\sigma\tau^{-1} = \sigma^{-1}$

(c) $\tau\sigma\tau^{-1} = \sigma^{-2}$

Solution.

(a) $\sigma^2 = (1\ 3\ 5\ 2\ 4)$. Then $\tau = (2\ 3\ 5\ 4)$.

(b) $\sigma^{-1} = (1\ 5\ 4\ 3\ 2)$. Then $\tau = (1\ 5)(2\ 4)$.

(c) $\sigma^{-2} = (1\ 4\ 2\ 5\ 3)$. Then $\tau = (2\ 4\ 5\ 3)$. ■

Exercise 4.3.11

In each of (a) – (d) determine whether σ_1 and σ_2 are conjugate. If they are, given an explicit permutation τ such that $\tau\sigma_1\tau^{-1} = \sigma_2$.

(a) $\sigma_1 = (1\ 2)(3\ 4\ 5)$ and $\sigma_2 = (1\ 2\ 3)(4\ 5)$

(b) $\sigma_1 = (1\ 5)(3\ 7\ 2)(10\ 6\ 8\ 11)$ and $\sigma_2 = (3\ 7\ 5\ 10)(4\ 9)(13\ 11\ 2)$

(c) $\sigma_1 = (1\ 5)(3\ 7\ 2)(10\ 6\ 8\ 11)$ and $\sigma_2 = \sigma_1^3$

(d) $\sigma_1 = (1\ 3)(2\ 4\ 6)$ and $\sigma_2 = (3\ 5)(2\ 4)(5\ 6)$

Solution.

(a) Rewrite σ_2 as $(4\ 5)(1\ 2\ 3)$ so that both have the same cycle type. Then $\tau = (1\ 4\ 2\ 5\ 3)$.

(b) Rewrite σ_2 as $(4\ 9)(13\ 11\ 2)(3\ 7\ 5\ 10)$. Then $\tau = (1\ 4)(8\ 5\ 9)(6\ 7\ 11\ 10\ 3\ 13)$.

(c) Note that $\sigma_2 = (1\ 5)(6\ 10\ 11\ 8)$, which does not have the same cycle type as σ_1. Therefore, they are not conjugate.

(d) $\sigma_2 = (2\ 4)(3\ 5\ 6)$. Then $\tau = (1\ 2\ 3\ 4\ 5)$. ■

Exercise 4.3.12

Find a representative for each conjugacy class of elements of order 4 in S_8 and S_{12}.

Solution. S_8:

Cycle Type	Representative
4, 4	(1 2 3 4)(5 6 7 8)
4, 2, 2	(1 2 3 4)(5 6)(7 8)
4, 2, 1, 1	(1 2 3 4)(5 6)
4, 1, 1, 1, 1	(1 2 3 4)

S_{12}:

Cycle Type	Representative
4, 4, 4	(1 2 3 4)(5 6 7 8)(9 10 11 12)
4, 4, 2, 2	(1 2 3 4)(5 6 7 8)(9 10)(11 12)
4, 4, 2, 1, 1	(1 2 3 4)(5 6 7 8)(9 10)
4, 4, 1, 1, 1, 1	(1 2 3 4)(5 6 7 8)
4, 2, 2, 2, 2	(1 2 3 4)(5 6)(7 8)(9 10)(11 12)
4, 2, 2, 2, 1, 1	(1 2 3 4)(5 6)(7 8)(9 10)
4, 2, 2, 1, 1, 1, 1	(1 2 3 4)(5 6)(7 8)
4, 2, 1, 1, 1, 1, 1, 1	(1 2 3 4)(5 6)
4, 1, 1, 1, 1, 1, 1, 1, 1	(1 2 3 4)

■

(∗) Exercise 4.3.13

Find all finite groups which have exactly two conjugacy classes.

Solution. Let G be a finite group with exactly two conjugacy classes. One of these classes must be $\{1\}$, the identity element. Let $\mathcal{K}$ be the other conjugacy class, and let $g \in \mathcal{K}$. By Proposition 4.6, we have $|\mathcal{K}| = |G : C_G(g)|$. Since there are only two conjugacy classes, then $|\mathcal{K}| = |G| - 1$. Therefore, $|G : C_G(g)| = |G| - 1$, which implies that $|C_G(g)| = |G|/(|G| - 1)$. Since $|C_G(g)|$ is an integer, then $|G| - 1$ divides $|G|$. This is only possible if $|G| - 1 = 1$, so that $|G| = 2$. Therefore, the only finite group with exactly two conjugacy classes is the group of order 2, which is isomorphic to Z_2. ■

Exercise 4.3.14

In Exercise 4.2.1 two labellings of the elements $\{1, a, b, c\}$ of the Klein 4-group V_4 were chosen to give two versions of the left regular representation of V_4 into S_4. Let π_1 be the version of regular representation obtained in part (a) of that exercise, and let π_2 be the version obtained via the labelling in part (b). Let $\tau = (2\,4)$. Show that $\tau \circ \pi_1(g) \circ \tau^{-1} = \pi_2(g)$ for each $g \in V_4$ (i.e., conjugation by τ sends the image of π_1 to the image of π_2 elementwise).

Solution. We will compute for a, as the rest follow similarly. We have $\pi_1(a) = (1\,2)(3\,4)$ and $\pi_2(a) = (1\,4)(2\,3)$. Then $\tau \circ \pi_1(a) \circ \tau^{-1} = (2\,4)(1\,2)(3\,4)(2\,4) = (1\,4)(2\,3) = \pi_2(a)$. ■

Exercise 4.3.15

Find an element of S_8 which conjugates the subgroup of S_8 obtained in part (a) of Exercise 4.2.3 to the subgroup of S_8 obtained in part (b) of that same exercise (both of these subgroups are isomorphic to D_8).

Solution. Recall by Exercise 1.7.17 that left conjugation is an automorphism, so it suffices to find an element which sends the generators of the first subgroup to the generators of the second subgroup. The generators of the first subgroup are $(1\,2\,3\,4)(5\,8\,7\,6)$ and $(1\,5)(2\,6)(3\,7)(4\,8)$, while the generators of the second subgroup are $(1\,3\,5\,7)(2\,8\,6\,4)$ and $(1\,2)(3\,4)(5\,6)(7\,8)$ respectively. It suffices to check some element τ which sends the first generator to the second; the second generator will follow automatically. One such element is $\tau = (5\,2\,3)(6\,4\,7)$. ■

Exercise 4.3.16

Find an element of S_4 which conjugates the subgroup of S_4 obtained in part (a) of Exercise 4.2.5 to the subgroup of S_4 obtained in part (b) of that same exercise (both of these subgroups are isomorphic to D_8).

Solution. We proceed similarly to the preceding exercise. The generators of the first subgroup are $(1\,2\,3\,4)$ and $(2\,4)$, while the generators of the second subgrgoup are $(1\,3\,2\,4)$ and $(3\,4)$. We obtain $\tau = (2\,3)$. ■

(∗) Exercise 4.3.17

Let A be a nonempty set and let X be any subset of S_A. Let

$$F(X) = \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in X\} \qquad \text{—the } \textit{fixed set} \text{ of } X$$

Let $M(X) = A - F(X)$ be the elements which are *moved* by some element of X. Let $D = \{\sigma \in S_A \mid |M(\sigma)| < \infty\}$. Prove that D is a normal subgroup of S_A.

Solution. Note that $1 \in D$, since $M(1) = \varnothing$ as it fixes all elements of A. Let $\sigma, \tau \in D$. Then $|M(\sigma)| < \infty$ and $|M(\tau)| < \infty$. Suppose $a \in F(\sigma) \cap F(\tau)$. Clearly, $a \in F(\sigma\tau)$. By contrapositive, then $a \in M(\sigma\tau)$ implies $a \in M(\sigma) \cup M(\tau)$, which are both finite, hence $M(\sigma\tau)$ is finite. Therefore, $\sigma\tau \in D$.

Now consider $\sigma \in D$. If $a \in A$ is fixed by σ, then it is fixed by σ^{-1}. Therefore, any element moved by σ^{-1} must be moved by σ, and vice-versa. Hence, $M(\sigma^{-1}) = M(\sigma)$, which is finite. Therefore, $\sigma^{-1} \in D$.

Finally, consider $\sigma \in D$ and $\tau \in S_A$. Suppose $a \in F(\tau\sigma\tau^{-1})$ so that $\tau\sigma\tau^{-1}(a) = a$. Then $\sigma(\tau^{-1}(a)) = \tau^{-1}(a)$, hence $\tau^{-1}(a) \in F(\sigma)$. By contrapositive, if $a \in M(\tau\sigma\tau^{-1})$, then $\tau^{-1}(a) \in M(\sigma)$. Since $M(\sigma)$ is finite, then $M(\tau\sigma\tau^{-1})$ is finite. Therefore, $\tau\sigma\tau^{-1} \in D$. ■

Exercise 4.3.18

Let A be a set, let H be a subgroup of S_A, and let $F(H)$ be the fixed points of H on A as defined in the preceding exercise. Prove that if $\tau \in N_{S_A}(H)$, then τ stabilizes the set $F(H)$ and its complement $A - F(H)$.

Solution. Suppose $\sigma \in H$. Since $\tau \in N_{S_A}(H)$, we have $\tau^{-1} \in N_{S_A}(H)$, hence $\tau^{-1}\sigma\tau \in H$. Suppose $a \in F(H)$. Then $\tau^{-1}\sigma\tau(a) = a$, so that $\sigma\tau(a) = \tau(a)$. Therefore, $\tau(a) \in F(H)$, and $\tau(F(H)) \subseteq F(H)$. Bijectivity of τ also implies that $\tau^{-1}(F(H)) \subseteq F(H)$, which shows that $F(H) \subseteq \tau(F(H))$, hence $\tau(F(H)) = F(H)$. Therefore, τ stabilizes $F(H)$. Moreover, since τ is a bijection, it also stabilizes the complement $A - F(H)$. ■

Exercise 4.3.19

Assume H is a normal subgroup of G, $\mathcal{K}$ is a conjugacy class of G contained in H and $x \in \mathcal{K}$. Prove that $\mathcal{K}$ is a union of k conjugacy classes of equal size in H, where $k = |G : HC_G(x)|$. Deduce that a conjugacy class in S_n which consists of even permutations is either a single conjugacy class under the action of A_n or is a union of two classes of the same size in A_n. [Let $A = C_G(x)$ and $B = H$ so $A \cap B = C_H(x)$. Draw the lattice diagram associated to the Second Isomorphism Theorem and interpret the appropriate indices. See also Exercise 4.1.9.]

Solution. Let G act on $\mathcal{K}$ by conjugation. Since $\mathcal{K}$ is a conjugacy class of G, this action is transitive. Because $H \trianglelefteq G$ and $\mathcal{K} \subseteq H$, then H also acts on $\mathcal{K}$ by conjugation. Let $\mathcal{O}$ be one such orbit of this action, and suppose $y \in \mathcal{O}$. By Proposition 4.6, we have $|\mathcal{O}| = |H : C_H(y)|$. By normality of H in G, we have $C_H(y) = C_G(y) \cap H$. Using the Second Isomorphism Theorem, we have

$$HC_G(y)/C_G(y) \cong H/C_H(y)$$

so that $|H : C_H(y)| = |HC_G(y) : C_G(y)|$. Therefore, $|\mathcal{O}| = |HC_G(y) : C_G(y)|$. Using Exercise 4.1.9, we know that each orbit of H on $\mathcal{K}$ has the same size, so every orbit has size $|HC_G(y) : C_G(y)|$. Suppose there are k orbits. Then

$$|\mathcal{K}| = k|HC_G(y) : C_G(y)|.$$

By Proposition 4.6, we also have $|\mathcal{K}| = |G : C_G(y)|$. Therefore,

$$|G : C_G(y)| = k|HC_G(y) : C_G(y)|.$$

Dividing both sides by $|HC_G(y) : C_G(y)|$, we obtain $k = |G : HC_G(y)|$. Hence, $\mathcal{K}$ is a union of k conjugacy classes of equal size in H.

Now suppose $\mathcal{K} \subseteq A_n$ is a conjugacy class of S_n consisting of even permutations. Let $x \in \mathcal{K}$. Applying the preceding result with $H = A_n$, we have that $\mathcal{K}$ is a union of k conjugacy classes of equal size in A_n, where $k = |S_n : A_nC_{S_n}(x)|$. Since $|S_n : A_n| = 2$, then k is either 1 or 2. Therefore, $\mathcal{K}$ is either a single conjugacy class under the action of A_n or is a union of two classes of the same size in A_n. ■

Exercise 4.3.20

Let $\sigma \in A_n$. Show that all elements in the conjugacy class of σ in S_n (i.e., all elements of the same cycle type as σ) are conjugate in A_n if and only if σ commutes with an odd permutation. [Use the preceding exercise.]

Solution. ($\Rightarrow$) Recall by the previous exercise that the conjugacy class of σ in S_n is either a single conjugacy class in A_n or a union of two conjugacy classes of equal size in A_n. Suppose all elements in the conjugacy class of σ in S_n are conjugate in A_n. Then the conjugacy class of σ in S_n is a single conjugacy class in A_n, so that $k = |S_n : A_nC_{S_n}(\sigma)| = 1$. Therefore, $S_n = A_nC_{S_n}(\sigma)$, so that there exists some odd permutation $\tau \in S_n$ such that $\tau \in C_{S_n}(\sigma)$. Hence, σ commutes with an odd permutation.

($\Leftarrow$) Suppose σ commutes with an odd permutation $\tau \in S_n$. Then $\tau \in C_{S_n}(\sigma)$, so that $A_nC_{S_n}(\sigma)$ contains odd permutations. Therefore, $|S_n : A_nC_{S_n}(\sigma)| = 1$, so that the conjugacy class of σ in S_n is a single conjugacy class in A_n. Hence, all elements in the conjugacy class of σ in S_n are conjugate in A_n. ■

(∗) Exercise 4.3.21

Let $\mathcal{K}$ be a conjugacy class in S_n and assume that $\mathcal{K} \subseteq A_n$. Show $\sigma \in S_n$ does *not* commute with any odd permutation if and only if the cycle type of σ consists of distinct odd integers. Deduce that $\mathcal{K}$ consists of two conjugacy clases in A_n if and only if the cycle type of an element of $\mathcal{K}$ consists of distinct odd integers. [Assume first that $\sigma \in \mathcal{K}$ does not commute with any odd permutation. Observe that σ commutes with each individual cycle in its cycle decomposition—use this to show that all its cycles must be of odd length. If two cycles have the same odd length, k, find a product of k transpositions which interchanges them and commutes with σ. Conversely, if the cycle type of σ consists of distinct integers, prove that σ commutes *only* with the group generated by the cycles in its cycle decomposition.]

Solution. ($\Rightarrow$) Suppose $\sigma \in S_n$ does not commute with any odd permutation. Let the cycle decomposition of σ be $\sigma = \tau_1\tau_2\cdots\tau_k$, where each τ_i is a disjoint cycle. Since σ commutes with each τ_i, then each τ_i must be of odd length; otherwise, τ_i would be an odd permutation commuting with σ. Now suppose two cycles τ_i and τ_j have the same odd length m. Then the product of m transpositions which interchanges the elements of τ_i and τ_j is an odd permutation which commutes with σ, contradicting our assumption. Therefore, all cycles in the cycle decomposition of σ must have distinct odd lengths.

($\Leftarrow$) Suppose the cycle type of σ consists of distinct odd integers. Let the cycle decomposition of σ be $\sigma = \tau_1\tau_2\cdots\tau_k$, where each τ_i is a disjoint cycle of odd length. Any permutation that commutes with σ must permute the cycles τ_i among themselves. However, since the lengths of the cycles are distinct, the only way to permute them while preserving their lengths is to leave them unchanged. Therefore, any permutation that commutes with σ must be a product of powers of the individual cycles τ_i. Since each τ_i has odd length, any such product will be an even permutation. Hence, σ does not commute with any odd permutation. ■

Exercise 4.3.22

Show that if n is odd, then the set of all n-cycles consists of two conjugacy classes of equal size in A_n.

Solution. Let $\sigma \in S_n$ be an n-cycle. Since n is odd, the cycle type of σ consists of the single odd integer n, which is distinct. By the previous exercise, σ does not commute with any odd permutation. Therefore, by the exercise before that, the conjugacy class of σ in S_n consists of two conjugacy classes of equal size in A_n. Since this holds for any n-cycle σ, the set of all n-cycles consists of two conjugacy classes of equal size in A_n. ■

Exercise 4.3.23

Recall (cf. Exercise 2.4.16) that a proper subgroup M of G is called *maximal* if whenever $M \leq H \leq G$, either $H = M$ or $H = G$. Prove that if M is a maximal subgroup of G then either $N_G(M) = M$ or $N_G(M) = G$. Deduce that if M is a maximal subgroup of G that is not normal in G, then the number of nonidentity elements of G that are contained in conjugates of M is at most $(|M| - 1)|G : M|$.

Solution. Suppose M is a maximal subgroup of G. By definition, $N_G(M)$ is a subgroup of G containing M. Therefore, by maximality of M, either $N_G(M) = M$ or $N_G(M) = G$.

Now suppose M is a maximal subgroup of G that is not normal in G. Then by the previous result, we have $N_G(M) = M$. By Proposition 4.6, the size of the conjugacy class of M in G is $|G : N_G(M)| = |G : M|$. Each conjugate of M contains $|M| - 1$ nonidentity elements. Therefore, the total number of nonidentity elements of G contained in conjugates of M is at most $(|M| - 1)|G : M|$. ■

Exercise 4.3.24

Assume H is a proper subgroup of the finite group G. Prove

$$G \neq \bigcup_{g \in G} gHg^{-1}$$

i.e., G is not the union of the conjugates of any proper subgroup. [Put H in some maximal subgroup and use the preceding exercise.]

Solution. Suppose H is a proper subgroup of the finite group G. Then there exists a maximal subgroup M of G such that $H \leq M < G$. By the previous exercise, either $N_G(M) = M$ or $N_G(M) = G$, so that we have two cases: either $M \trianglelefteq G$ or M is not normal in G.

If M is normal in G, then all conjugates of M are equal to M. Therefore, the union of the conjugates of H is contained in M, which is a proper subset of G. Hence,

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

Now suppose M is not normal in G. Then by the previous exercise, the number of nonidentity elements of G contained in conjugates of M is at most $(|M| - 1)|G : M|$. Moreover, $H \leq M$ implies that any conjugate of H is contained in a conjugate of M. Therefore, the number of nonidentity elements of G contained in conjugates of H is also at most $(|M|-1)|G : M|$. Since M is a proper subgroup of G, then $|G : M| \geq 2$, so that $(|M|-1)|G : M| < |G|-1$. Therefore, there exists at least one nonidentity element of G that is not contained in any conjugate of H, hence

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$ ∎

Exercise 4.3.25

Let $G = \mathrm{GL}_2(\mathbb{C})$ and let

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a, b, c \in \mathbb{C}, ac \neq 0 \right\}.$$

Prove that every element of G is conjugate to some element of the subgroup H and deduce that G is the union of conjugates of H. [Show that every element of $\mathrm{GL}_2(\mathbb{C})$ has an eigenvector.]

Solution. Suppose $X \in G$, where X is the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and consider the characteristic polynomial $\chi_X(t) = \det(X - tI) = t^2 - (a + d)t + (ad - bc)$. Since $\mathbb{C}$ is closed under complex multiplication, $\chi_X(t)$ has at least one root $\lambda \in \mathbb{C}$. Therefore, there exists a nonzero vector $\mathbf{v} \in \mathbb{C}^2$ such that $X\mathbf{v} = \lambda\mathbf{v}$, so that $\mathbf{v}$ is an eigenvector of X corresponding to the eigenvalue λ. We may extend $\mathbf{v}$ to a basis $\{\mathbf{v}, \mathbf{w}\}$ of $\mathbb{C}^2$. Let P be the matrix whose columns are $\mathbf{v}$ and $\mathbf{w}$. Then P is invertible, and we have

$$P^{-1}XP = \begin{pmatrix} \lambda & \alpha \\ 0 & \beta \end{pmatrix} \in H.$$

for some $\alpha, \beta \in \mathbb{C}$ such that $X\mathbf{w} = \alpha\mathbf{v} + \beta\mathbf{w}$. Therefore, every element of G is conjugate to some element of the subgroup H, hence every element of G is contained in some conjugate of H. Thus,

$$G = \bigcup_{g \in G} gHg^{-1}.$$ ∎

Exercise 4.3.26

Let G be a transitive permutation group on the finite set A with $|A| > 1$. Show that there is some $\sigma \in G$ such that $\sigma(a) \neq a$ for all $a \in A$ (such an element σ is called *fixed point free*).

Solution. For each $a \in A$, consider G_a. By transitivity of G on A, we have $|G : G_a| = |A| > 1$, so that G_a is a proper subgroup of G. By Exercise 4.3.24, we have

$$G \neq \bigcup_{g \in G} gG_ag^{-1}.$$

Therefore, there exists some $\sigma \in G$ such that $\sigma \notin gG_ag^{-1}$ for all $g \in G$. Moreover, if $\sigma(a) = a$ for some $a \in A$, then $\sigma \in G_a$, hence $\sigma \in gG_ag^{-1}$ for $g = 1$, a contradiction. Therefore, $\sigma(a) \neq a$ for all $a \in A$. ■

Exercise 4.3.27

Let $g_1, g_2, \ldots, g_r$ be representatives of the conjugacy classes of the finite group G and assume these elements pairwise commute. Prove that G is abelian.

Solution. Pick some g_i and consider its conjugacy class $\mathcal{K}_i$. Since g_i commutes with all g_j for $1 \leq j \leq r$, then for any $x \in G$, we have $xg_ix^{-1} = g_i$ so that $x \in C_G(g_i)$. Therefore, $C_G(g_i) = G$, so that $\mathcal{K}_i = \{g_i\}$. Since this holds for all $1 \leq i \leq r$, then every conjugacy class of G is a singleton set. Hence, for any $x, y \in G$, we have $xyx^{-1} = y$, so that $xy = yx$. Therefore, G is abelian. ■

Exercise 4.3.28

Let p and q be primes with $p < q$. Prove that a non-abelian group G of order pq has a nonnormal subgroup of index q so that there exists an injective homomorphism into S_q. Deduce that G is isomorphic to a subgroup of the normalizer in S_q of the cyclic group generated by the q-cycle $(1\ 2\ \cdots\ q)$.

Solution. By Cauchy's Theorem, there exists $g \in G$ such that $|g| = q$, hence $\langle g \rangle$ has order q and is of index p. Moreover, $\langle g \rangle$ is not normal in G, for otherwise $G/\langle g \rangle$ would be cyclic and isomorphic to Z_p, contradicting that G is non-abelian. Similarly, G also contains a subgroup P of order p and index q and is similarly not normal in G.

Let G act on the left cosets of P in G by left multiplication. Then there is the associated permutation representation $\pi : G \to S_q$. In particular, π is injective: If $\pi(x) = 1$ for some $x \in G$, then $xgP = gP$ for every $g \in G$, or $g^{-1}xg \in P$ for every $g \in G$. But $\ker \pi \trianglelefteq G$ and is contained in P so that $\ker \pi$ has order 1 or p. If $|\ker \pi| = p$, then $\ker \pi = P$ is normal in G, a contradiction. Therefore, $\ker \pi = 1$ and π is injective.

Recall that $|g| = q$ so that $|\pi(g)| = q$, so $\pi(g)$ acts transitively on G/P since its powers generate q distinct cosets. Now pick $h \in G$. From Exercise 1.1.22, it follows that $|hgh^{-1}| = |g| = q$ so that $hgh^{-1} = g^k$ for some integer k with $1 \leq k < q$. Therefore,

$$\pi(h)\pi(g)\pi(h)^{-1} = \pi(hgh^{-1}) = \pi(g^k) = (\pi(g))^k \in \langle \pi(g) \rangle.$$

Hence, $\pi(h) \in N_{S_q}(\langle \pi(g) \rangle)$. Since h was arbitrary, we have $G \cong \pi(G) \leq N_{S_q}(\langle \pi(g) \rangle)$. Therefore, G is isomorphic to a subgroup of the normalizer in S_q of the cyclic group generated by the q-cycle $(1\ 2\ \cdots\ q)$. ■

Exercise 4.3.29

Let p be a prime and let G be a group of order p^α. Prove that G has a subgroup of order p^β, for every β with $0 \leq \beta \leq \alpha$. [Use Theorem 8 and induction on α.]

Solution. We proceed by induction on α. If $\alpha = 0$, then G is the trivial group, which has a subgroup of order $p^0 = 1$. Now suppose the result holds for all groups of order p^k for some $k \geq 0$. Let G be a group of order p^{k+1}. By Theorem 8, $Z(G)$ is nontrivial, so there exists some $x \in Z(G)$ such that $|x| = p$. Then $\langle x \rangle$ is a normal subgroup of G of order p. Consider the quotient group $G/\langle x \rangle$, which has order p^k. By the induction hypothesis, for every β with $0 \leq \beta \leq k$, there exists a subgroup $H/\langle x \rangle$ of $G/\langle x \rangle$ such that $|H/\langle x \rangle| = p^\beta$. By the Lattice

Isomorphism Theorem, there exists a subgroup H of G such that $\langle x\rangle \leq H$ and $|H| = p^{\beta+1}$. Therefore, for every β with $1 \leq \beta \leq k+1$, there exists a subgroup of G of order p^β. Since the trivial subgroup has order $p^0 = 1$, the result holds for all β with $0 \leq \beta \leq k+1$. By induction, the result holds for all $\alpha \geq 0$. ■

Exercise 4.3.30

If G is a group of odd order, prove for any nonidentity element $x \in G$ that x and x^{-1} are not conjugate in G.

Solution. Suppose for contradiction that x and x^{-1} are conjugate in G. Then there exists $g \in G$ such that $gxg^{-1} = x^{-1}$. If we conjugate both sides by g again, we obtain

$$g^2xg^{-2} = gx^{-1}g^{-1} = (gxg^{-1})^{-1} = (x^{-1})^{-1} = x$$

so that $g^2x = xg^2$. Then $g^2 \in C_G(x)$. Consider the quotient group $G/C_G(x)$. Since $g^2 \in C_G(x)$, we have $(gC_G(x))^2 = C_G(x)$, so that the order of $gC_G(x)$ in $G/C_G(x)$ is 1 or 2. However, since G has odd order, then $G/C_G(x)$ also has odd order, so the order of $gC_G(x)$ cannot be 2. Therefore, the order of $gC_G(x)$ is 1, so that $g \in C_G(x)$. But this implies that $gxg^{-1} = x$, contradicting our assumption. Therefore, x and x^{-1} are not conjugate in G. ■

Exercise 4.3.31

Using the usual generators and relations for the dihedral group D_{2n} (cf. Section 1.2) show that for $n = 2k$ an even integer the conjugacy classes in D_{2n} are the following: $\{1\}, \{r^k\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(k-1)}\}, \{sr^{2b} \mid b = 1, \ldots, k\}$ and $\{sr^{2b-1} \mid b = 1, \ldots, k\}$. Give the class equation for D_{2n}.

Solution. We immediately have two conjugacy classes, $\{1\}$ and $\{r^n\}$, since $r^n \in Z(D_{2n})$ when n is even. Moreover, recall that the elements of D_{2n} are of the form r^m or sr^m for some integer m. Consider the conjugacy class of r^k for some $1 \leq k < n$ except $k = n/2$. For any j, we have

$$r^j r^k r^{-j} = r^k, \quad \text{and} \quad sr^j r^k r^{-j} s = r^{-k}$$

so that the conjugacy class of r^k is $\{r^{\pm k}\}$. Now consider the conjugacy class of sr^m for some integer m. For any j, we have

$$r^j sr^m r^{-j} = sr^{m-2j}, \quad \text{and} \quad sr^j sr^m r^{-j} s = r^{-(m-2j)}$$

so that the conjugacy class of sr^m is $\{sr^{m-2j} \mid j \in \mathbb{Z}\}$. If m is even, then this conjugacy class is $\{sr^{2b} \mid b = 1, \ldots, k\}$; if m is odd, then this conjugacy class is $\{sr^{2b-1} \mid b = 1, \ldots, k\}$. Therefore, the conjugacy classes in D_{2n} when n is even are $\{1\}, \{r^k\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(k-1)}\}, \{sr^{2b} \mid b = 1, \ldots, k\}$ and $\{sr^{2b-1} \mid b = 1, \ldots, k\}$. Lastly, the class equation for D_{2n} is

$$|D_{2n}| = 1 + 1 + 2(k-1) + k + k.$$ ■

Exercise 4.3.32

For $n = 2k+1$ an odd integer, show that the conjugacy classes in D_{2n} are $\{1\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm k}\}$, and $\{sr^b \mid b = 1, \ldots, n\}$. Give the class equation for D_{2n}.

Solution. We immediately have the conjugacy class $\{1\}$. Moreover, recall that the elements of D_{2n} are of the form r^m or sr^m for some integer m. Consider the conjugacy class of r^k for some $1 \leq k \leq n$ except $k = n/2$. For any j, we have

$$r^j r^k r^{-j} = r^k, \quad \text{and} \quad sr^j r^k r^{-j} s = r^{-k}$$

so that the conjugacy class of r^k is $\{r^{\pm k}\}$. Now consider the conjugacy class of sr^m for some integer m. For any j, we have

$$r^j sr^m r^{-j} = sr^{m-2j}, \quad \text{and} \quad sr^j sr^m r^{-j} s = r^{-(m-2j)}$$

so that the conjugacy class of sr^m is $\{sr^{m-2j} \mid j \in \mathbb{Z}\}$. Since n is odd, this conjugacy class is $\{sr^b \mid b = 1, \ldots, n\}$. Therefore, the conjugacy classes in D_{2n} when n is odd are $\{1\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm k}\}$, and $\{sr^b \mid b = 1, \ldots, n\}$. Lastly, the class equation for D_{2n} is

$$|D_{2n}| = 1 + 2k + n.$$ ■

(∗) Exercise 4.3.33

This exercise gives a formula for the size of each conjugacy class in S_n. Let σ be a permutation in S_n and let $m_1, m_2, \ldots, m_s$ be the *distinct* integers which appear in the cycle type of σ (including 1-cycles). For each $i \in \{1, 2, \ldots, s\}$ assume σ has k_i cycles of length m_i (so that $\sum_1^s k_i m_i = n$). Prove that the number of conjugates of σ is

$$\frac{n!}{(k_1! m_1^{k_1})(k_2! m_2^{k_2}) \cdots (k_s! m_s^{k_s})}$$

[See Exercise 1.3.6 and Exercise 1.3.7 where this formula was given in some special cases.]

Solution. We start with n integers. We see that there are $n!$ ways to arrange these integers. Now consider the k_1 cycles of length m_1 in the cycle decomposition of σ. Clearly, we must use $k_1 m_1$ of the n integers to form these cycles. However, there are $m_1^{k_1}$ ways to arrange the integers within each of these k_1 cycles, and there are $k_1!$ ways to arrange the k_1 cycles among themselves. Therefore, we must divide $n!$ by $(k_1! m_1^{k_1})$ to account for these arrangements. Continuing in this manner for each i from 1 to s, we see that the total number of distinct arrangements of the n integers that correspond to the same cycle type as σ is given by

$$\frac{n!}{(k_1! m_1^{k_1})(k_2! m_2^{k_2}) \cdots (k_s! m_s^{k_s})}.$$

Since the conjugacy class of σ in S_n consists of all permutations with the same cycle type as σ, the number of conjugates of σ is given by this formula. ■

Exercise 4.3.34

Prove that if p is a prime and P is a subgroup of S_p of order p, then $|N_{S_p}(P)| = p(p-1)$. [Argue that every conjugate of P contains exactly $p-1$ p-cycles and use the formula for the number of p-cycles to compute the index of $N_{S_p}(P)$ in S_p.]

Solution. Note that P is cyclic of order p, so $P = \langle \sigma \rangle$ for some p-cycle $\sigma \in S_p$. Moreover, every nonidentity element of P is a p-cycle, so P contains exactly $p-1$ p-cycles. Now for some $\tau \in S_p$, the conjugate $\tau P \tau^{-1} = \langle \tau \sigma \tau^{-1} \rangle$ also has order p and contains exactly $p-1$ p-cycles. Therefore, each conjugate of P contains exactly $p-1$ p-cycles. Note that the number of distinct p-cycles in S_p is given by $p!/p = (p-1)!$.

Recall by Proposition 4.6 that the size of the conjugacy class of P in S_p is given by $|S_p : N_{S_p}(P)|$. Let this index be k. Since each conjugate of P contains exactly $p-1$ p-cycles, the total number of distinct p-cycles contained in all conjugates of P is $k(p-1)$. However, since every p-cycle in S_p is contained in some conjugate of P, we have $k(p-1) = (p-1)!$. Therefore, $k = (p-2)!$, so that

$$|N_{S_p}(P)| = \frac{|S_p|}{k} = \frac{p!}{(p-2)!} = p(p-1).$$ ■

Exercise 4.3.35

Let p be a prime. Find a formula for the number of conjugacy classes of elements of order p in S_n (using the greatest integer function).

Solution. Note that elements of order p in S_n are products of disjoint p-cycles. Moreover, each p-cycle is conjugate to any other p-cycle in S_n. Therefore, the conjugacy class of an element of order p in S_n is determined by the number of disjoint p-cycles in its cycle decomposition. Let k be the number of disjoint p-cycles in the cycle decomposition of such an element. Then we have $1 \leq k \leq \lfloor n/p \rfloor$, hence the number of conjugacy classes of elements of order p in S_n is given by $\lfloor n/p \rfloor$. ■

(∗) Exercise 4.3.36

Let $\pi : G \to S_G$ be the left regular representation afforded by the action of G on itself by left multiplication. For each $g \in G$ denote the permutation $\pi(g)$ by σ_g so that $\sigma_g(x) = gx$ for all $x \in G$. Let $\lambda : G \to S_G$ be the permutation representation afforded by the corresponding right action of G on itself, and for each $h \in G$ denote the permutation $\lambda(h)$ by τ_h. Thus $\tau_h(x) = xh^{-1}$ for all $x \in G$ (λ is called the *right regular representation* of G).

(a) Prove that σ_g and τ_h commute for all $g, h \in G$. (Thus the centralizer in S_G of $\pi(G)$ contains the subgroup $\lambda(G)$ which is isomorphic to G).

(b) Prove that $\sigma_g = \tau_g$ if and only if g is an element of order 1 or 2 in the center of G.

(c) Prove that $\sigma_g = \tau_h$ if and only if g and h lie in the center of G. Deduce that $\pi(G) \cap \lambda(G) = \pi(Z(G)) = \lambda(Z(G))$.

Solution.

(a) For any $x \in G$, we have

$$\sigma_g(\tau_h(x)) = \sigma_g(xh^{-1}) = g(xh^{-1}) = (gx)h^{-1} = \tau_h(gx) = \tau_h(\sigma_g(x)).$$

Therefore, σ_g and τ_h commute for all $g, h \in G$.

(b) If $\sigma_g = \tau_g$, then $gx = xg^{-1}$ for all $x \in G$. In particular, $x = 1$ implies $g = g^{-1}$ so that $g^2 = 1$, hence $|g|$ is 1 or 2. Moreover, for any $x \in G$, we have $gx = xg^{-1} = xg$, so that $g \in Z(G)$

If g is an element of order 1 or 2 in the center of G, then for any $x \in G$, we have $\sigma_g(x) = gx = xg = xg^{-1} = \tau_g(x)$. Therefore, $\sigma_g = \tau_g$.

(c) If $\sigma_g = \tau_h$, then $gx = xh^{-1}$ for all $x \in G$. In particular, $x = 1$ implies $g = h^{-1}$, so that $h = g^{-1}$. Therefore, $gx = xg^{-1}$ for all $x \in G$, so that by part (b), g lies in the center of G. Since $h = g^{-1}$, then h also lies in the center of G.

If g and h lie in the center of G, then for any $x \in G$, we have $\sigma_g(x) = gx = xg = xh^{-1} = \tau_h(x)$. Therefore, $\sigma_g = \tau_h$. Moreover, if $\sigma_g \in \pi(G) \cap \lambda(G)$, then there exists $h \in G$ such that $\sigma_g = \tau_h$. By the above result, both g and h lie in the center of G, so that $\sigma_g \in \pi(Z(G))$ and $\tau_h \in \lambda(Z(G))$. Conversely, if $g \in Z(G)$, then by part (b), we have $\sigma_g = \tau_g$, so that $\sigma_g \in \pi(G) \cap \lambda(G)$. Therefore, $\pi(G) \cap \lambda(G) = \pi(Z(G)) = \lambda(Z(G))$. ■

4.4 Automorphisms

(∗) Exercise 4.4.1

Let G be a group. If $\sigma \in \mathrm{Aut}(G)$ and ϕ_g is conjugation by g, prove that $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)}$. Deduce that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. (The group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G.)

Solution. For any $x \in G$, then

$$(\sigma\varphi_g\sigma^{-1})(x) = \sigma(\varphi_g(\sigma^{-1}(x))) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g)^{-1} = \sigma(g)x\sigma(g)^{-1} = \varphi_{\sigma(g)}(x).$$

Then $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Therefore, for any $\varphi_g \in \mathrm{Inn}(G)$ and any $\sigma \in \mathrm{Aut}(G)$, we have $\sigma\varphi_g\sigma^{-1} \in \mathrm{Inn}(G)$, so that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. ■

(∗) Exercise 4.4.2

Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic. (Use Cauchy's Theorem to produce elements of order p and q and consider the order of their product.)

Solution. By Cauchy's Theorem, there are elements $g, h \in G$ such that $|g| = p$ and $|h| = q$. Since G is abelian, we have $|gh| = \mathrm{lcm}(|g|, |h|) = \mathrm{lcm}(p, q) = pq$. Therefore, $G = \langle gh \rangle$ is cyclic. ■

Exercise 4.4.3

Prove that under any automorphism of D_8, r has at most 2 possible images and s has at most 4 possible images (where r and s are the usual generators). Deduce that $|\mathrm{Aut}(D_8)| \leq 8$.

Solution. Since $|r| = 4$, any automorphism σ of D_8 must send r to an element of order 4. The only elements of order 4 in D_8 are r and r^3, so r has at most 2 possible images under σ. Moreover, $|s| = 2$, so $\sigma(s)$ must be an element of order 2. The elements of order 2 in D_8 are s, sr, sr^2, and sr^3, so s has at most 4 possible images under σ. Therefore, there are at most $2 \cdot 4 = 8$ possible automorphisms of D_8, so that $|\mathrm{Aut}(D_8)| \leq 8$. ■

Exercise 4.4.4

Use arguments similar to those in the preceding exercise to show that $|\mathrm{Aut}(Q_8)| \leq 24$.

Solution. Note that $|i| = |j| = |k| = 4$, so any automorphism σ of Q_8 must send i to an element of order 4. The only elements of order 4 in Q_8 are $i, j, k, i^{-1}, j^{-1}, k^{-1}$, so i has at most 6 possible images under σ. Moreover, since $ij = k$, we have $\sigma(i)\sigma(j) = \sigma(k)$. Therefore, once we choose the image of i, there are 4 possible choices for the image of j (since it cannot be the inverse of the image of i). Hence, there are at most $6 \cdot 4 = 24$ possible automorphisms of Q_8, so that $|\mathrm{Aut}(Q_8)| \leq 24$. ■

Exercise 4.4.5

Use the fact that $D_8 \trianglelefteq D_{16}$ to prove that $\mathrm{Aut}(D_8) \cong D_8$.

Solution. Consider the subgroup $H = \langle r^2, s \rangle$ of D_{16}. Note that $(r^2)^4 = s^2 = 1$, so this satisfies the same relations as D_8, hence $H \cong D_8$. Moreover, H is normal in D_{16} as it has index 2. Then $N_{D_{16}}(H) = D_{16}$. Moreover, $C_{D_{16}}(H)$ can be computed by considering the centralizers of the generators of H. Note that $C_{D_{16}}(r^2) = \langle r \rangle$ since only rotations commute with each other. Consider now the centralizer of s. For any rotation r^k, we have $sr^k = r^k s$ if and only if $r^{-k} = r^k$, which holds if and only if $k = 0$ or $k = 4$. For any reflection sr^k, we obtain the same conclusion so that $C_{D_{16}}(s) = \{1, r^4, s, sr^4\}$. Intersecting these, it is easy to see that $C_{D_{16}}(H) = Z(D_{16})$.

We now have that $N_{D_{16}}(H)/C_{D_{16}}(H) \cong D_{16}/Z(D_{16}) \cong D_8$. Now recall that $D_{16}/Z(D_{16})$ is still isomorphic to a subgroup of $\mathrm{Aut}(H)$ when acted on by conjugation. By Exercise 4.4.3, we know that $|\mathrm{Aut}(D_8)| \leq 8$, so that $\mathrm{Aut}(H) \cong D_8$. Therefore, $\mathrm{Aut}(D_8) \cong D_8$. ■

Exercise 4.4.6

Prove that characteristic subgroups are normal. Give an example of a normal subgroup that is not characteristic.

Solution. If H char G, then $\varphi(H) = H$ for every $\varphi \in \mathrm{Aut}(G)$. In particular, this holds for every $\varphi_g \in \mathrm{Inn}(G)$ so that $\varphi_g(H) = gHg^{-1} = H$ for every $g \in G$. Therefore, $H \trianglelefteq G$.

Consider the abelian group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then every subgroup of G is normal since G is abelian. However, the subgroup $H = \{(0,0),(1,0)\}$ is not characteristic in G since the automorphism $\sigma : G \to G$ defined by $\sigma((a,b)) = (b,a)$ sends H to the distinct subgroup $\{(0,0),(0,1)\}$. Therefore, H is a normal subgroup of G that is not characteristic. ■

Exercise 4.4.7

If H is the unique subgroup of a given order in a group G, prove that H is characteristic in G.

Solution. For any $\sigma \in \mathrm{Aut}(G)$, the subgroup $\sigma(H)$ has the same order as H. Since H is the unique subgroup of that order in G, we must have $\sigma(H) = H$. Therefore, H is characteristic in G. ■

(∗) Exercise 4.4.8

Let G be a group with subgroups H and K with $H \leq K$.

(a) Prove that if H is characteristic in K and K is normal in G, then H is normal in G.

(b) Prove that if H is characteristic in K and K is characteristic in G, then H is characteristic in G. Use this to prove that the Klein 4-group V_4 is characteristic in S_4.

(c) Give an example to show that if H is normal in K and K is characteristic in G, then H need not be normal in G.

Solution.

(a) For any $g \in G$, consider the inner automorphism $\varphi_g \in \mathrm{Inn}(G)$. Since $K \trianglelefteq G$, we have $\varphi_g(K) = K$. Moreover, since H char K, we have $\varphi_g(H) = H$. Therefore, $gHg^{-1} = H$ for all $g \in G$, so that $H \trianglelefteq G$.

(b) For any $\sigma \in \mathrm{Aut}(G)$, since K char G, we have $\sigma(K) = K$. Moreover, since H char K, we have $\sigma(H) = H$. Therefore, H char G.

Consider V_4. By Exercise 3.5.8, V_4 is the unique subgroup of order 4 in A_4 so that V_4 char A_4 by Exercise 4.4.7. Moreover, A_4 is the unique subgroup of order 12 in S_4, for otherwise if $H \leq S_4$ such that $|H| = 12$, then it would contain only odd permutations, which is impossible since the product of two odd permutations is an even permutation. Therefore, A_4 char S_4 by Exercise 4.4.7. By the above result, V_4 char S_4.

(c) Consider A_4. Then V_4 char A_4 as shown previously. Consider $H = \langle (1\,2)(3\,4) \rangle \leq V_4$. Since V_4 is abelian, then $H \trianglelefteq V_4$. However, taking $(1\,2\,3) \in A_4$, we have

$$(1\,2\,3)(1\,2)(3\,4)(3\,2\,1) = (1\,4)(2\,3) \notin H$$

so that H is not normal in A_4. ■

Exercise 4.4.9

If r, s are the usual generators for the dihedral group D_{2n}, use the preceding two exercises to deduce that every subgroup of $\langle r \rangle$ is normal in D_{2n}.

Solution. By Exercise 3.1.34, we know $\langle r \rangle$ is normal in D_{2n}. Moreover, every subgroup of a cyclic group is characteristic, so every subgroup of $\langle r \rangle$ is characteristic in $\langle r \rangle$. Since $\langle r \rangle \trianglelefteq D_{2n}$, then by Exercise 4.4.8, every subgroup of $\langle r \rangle$ is normal in D_{2n}. ■

Exercise 4.4.10

Let G be a group, let A be an abelian normal subgroup of G, and write $\overline{G} = G/A$. Show that $\overline{G}$ acts (on the left) by conjugation on A by $\bar{g} \cdot a = gag^{-1}$, where g is any representative of the coset $\bar{g}$ (in particular, show that this action is well defined). Give an explicit example to show that this action is not well defined if A is non-abelian.

Solution. Let $\bar{g}$ and $\bar{h}$ be the same coset in $\overline{G}$. Then there exists some $a_0 \in A$ such that $h = ga_0$. Then for any $a \in A$, we have

$$\bar{g} \cdot a = gag^{-1} = gaa_0a_0^{-1}g^{-1} = ga_0a(ga_0)^{-1} = hah^{-1} = \bar{h} \cdot a$$

since A is abelian. Therefore, the action is well defined.

Consider $G = S_3$ and $A = S_3$ itself. Then $\bar{1} = \overline{(1\ 2)}$ in $\overline{G}$. However, for $a = (1\ 3)$, we have $\bar{1} \cdot a = a = (1\ 3)$ but, but $\overline{(1\ 2)} \cdot a = (1\ 2)(1\ 3)(1\ 2) = (2\ 3) \neq a$. Therefore, the action is not well defined if A is non-abelian. ■

Exercise 4.4.11

If p is a prime and P is a subgroup of S_p of order p, prove that $N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{Aut}(P)$. (Use Exercise 4.3.34).

Solution. By Exercise 4.3.34, we know that $|N_{S_p}(P)| = p(p-1)$. Moreover, since P is cyclic of order p, we have $\mathrm{Aut}(P) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ by Proposition 4.16, so that $|\mathrm{Aut}(P)| = p-1$. Let N_{S_p} act on P by conjugation. Then we have the map

$$\varphi : N_{S_p}(P) \to \mathrm{Aut}(P), \quad \varphi(g)(x) = gxg^{-1}$$

for all $g \in N_{S_p}(P)$ and $x \in P$. Recall that $\ker\varphi = C_{S_p}(P)$ by Proposition 4.13. Therefore, by the First Isomorphism Theorem, we have

$$N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{im}\,\varphi \leq \mathrm{Aut}(P).$$

Since P is cyclic, then the only permutations that centralize P are the elements of P itself, so that $C_{S_p}(P) = P$. Therefore,

$$|N_{S_p}(P)/C_{S_p}(P)| = \frac{|N_{S_p}(P)|}{|C_{S_p}(P)|} = \frac{p(p-1)}{p} = p-1 = |\mathrm{Aut}(P)|.$$

Hence, $\mathrm{im}\,\varphi = \mathrm{Aut}(P)$ so that $N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{Aut}(P)$. ■

Exercise 4.4.12

Let G be a group of order 3825. Prove that if H is a normal subgroup of order 17 in G then $H \leq Z(G)$.

Solution. Observe that $3825 = 15^2 \cdot 17$. Since $|H| = 17$ a prime, then H is cyclic. Moreover, we have $\mathrm{Aut}(H) \cong (\mathbb{Z}/17\mathbb{Z})^\times$ by Proposition 4.16, so that $|\mathrm{Aut}(H)| = 16$. Now consider the action of G on H by conjugation. This gives the map

$$\varphi : G \to \mathrm{Aut}(H), \quad \varphi(g)(x) = gxg^{-1}$$

for all $g \in G$ and $x \in H$. Recall that $\ker\varphi = C_G(H)$ by Proposition 4.13. Therefore, by the First Isomorphism Theorem, we have

$$G/C_G(H) \cong \mathrm{im}\,\varphi \leq \mathrm{Aut}(H).$$

Hence, $|G/C_G(H)|$ divides $|\mathrm{Aut}(H)| = 16$. However, $|G| = 3825$ is relatively prime to 16, so that $|G/C_G(H)| = 1$. Therefore, $G = C_G(H)$, so that $H \leq Z(G)$. ■

Exercise 4.4.13

Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G then $H \leq Z(G)$. Deduce that G is abelian in this case.

Solution. Note that $203 = 7 \cdot 29$. The proof of showing that $H \leq Z(G)$ is similar to the previous exercise. To see that G is abelian, consider the quotient group G/H. Since $|G/H| = 29$ is prime, then G/H is cyclic. By Exercise 3.1.36, we have that G is abelian. ■

Exercise 4.4.14

Let G be a group of order 1575. Prove that if H is a normal subgroup of order 9 in G then $H \leq Z(G)$.

Solution. This exercise is similar to the previous two. Following the proofs, we will find that $|G/C_G(H)|$ divides $|\operatorname{Aut}(H)| = 6$ or 48. However, $1575 = 3^2 \cdot 5^2 \cdot 7$ results in $(|G|, |\operatorname{Aut}(H)|) = 1$ or 3. If the latter is true, then $|C_G(H)| = 525$. However, this is impossible since $H \leq C_G(H)$ and $|H| = 9$ does not divide 525. Therefore, we must have $|G/C_G(H)| = 1$, so that $G = C_G(H)$ and hence $H \leq Z(G)$. ■

Exercise 4.4.15

Prove that each of the following (multiplicative) groups is cyclic: $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/9\mathbb{Z})^\times$, and $(\mathbb{Z}/18\mathbb{Z})^\times$.

Solution. Since $|(\mathbb{Z}/5\mathbb{Z})^\times| = 4$, then $(\mathbb{Z}/5\mathbb{Z})^\times$ is isomorphic to either Z_4 or V_4. However, $\bar{2} \in (\mathbb{Z}/5\mathbb{Z})^\times$ has order 4, so that $(\mathbb{Z}/5\mathbb{Z})^\times \cong Z_4$ is cyclic.

Observe that $|(\mathbb{Z}/9\mathbb{Z})^\times| = |(\mathbb{Z}/18\mathbb{Z})^\times| = 6$. By Exercise 4.2.10, groups of order 6 are isomorphic to either Z_6 or S_3. However, both groups are abelian, so that $(\mathbb{Z}/9\mathbb{Z})^\times$ and $(\mathbb{Z}/18\mathbb{Z})^\times$ must be isomorphic to Z_6. Therefore, both groups are cyclic. ■

(∗) Exercise 4.4.16

Prove that $(\mathbb{Z}/24\mathbb{Z})^\times$ is an elementary abelian group of order 8. (We shall see later that $(\mathbb{Z}/n\mathbb{Z})^\times$ is an elementary abelian group if and only if $n \mid 24$.)

Solution. We first prove the lemma: let $a, b, m, n \in \mathbb{Z}$ such that $(m, n) = 1$. If $a \equiv b \bmod m$ and $a \equiv b \bmod n$, then $a \equiv b \bmod mn$. Indeed, we have that

$$a - b = xm \quad \text{and} \quad a - b = yn$$

for some $x, y \in \mathbb{Z}$. Therefore, $xm = yn$, so that $m \mid yn$. Since $(m, n) = 1$, then $m \mid y$. Letting $y = km$ for some $k \in \mathbb{Z}$, we have

$$a - b = yn = kmn,$$

so that $a \equiv b \bmod mn$.

Let $x \in (\mathbb{Z}/24\mathbb{Z})^\times$. Note that x is always odd. Then $\gcd(x, 24) = 1$, hence $(x, 3) = (x, 8) = 1$. Since $(x, 3) = 1$, then $x \equiv 1$ or $2 \bmod 3$. Then $x^2 \equiv 1 \bmod 3$. Since $(x, 8) = 1$, let $x = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

Since one of k or $k + 1$ is even, then $4k(k + 1)$ is divisible by 8, so that $x^2 \equiv 1 \bmod 8$. By the lemma above, we have $x^2 \equiv 1 \bmod 24$. Therefore, every element of $(\mathbb{Z}/24\mathbb{Z})^\times$ has order dividing 2, so that $(\mathbb{Z}/24\mathbb{Z})^\times$ is an elementary abelian group. ■

Exercise 4.4.17

Let $G = \langle x \rangle$ be a cyclic group of order n. For $n = 2, 3, 4, 5, 6$ write out the elements of $\mathrm{Aut}(G)$ explicitly (by Proposition 16 above we know $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, so for each element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, write out explicitly what the automorphism ψ_a does to the elements $\{1, x, x^2, \ldots, x^{n-1}\}$ of G).

Solution.

- $n = 2$: $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$. Then $\psi_1 : x^k \mapsto x^{1\cdot k} = x^k$ for $k = 0, 1$. Therefore, $\mathrm{Aut}(G) = \{\mathrm{id}\}$.
- $n = 3$: $(\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}, \bar{2}\}$. Then
$$\psi_1 : x^k \mapsto x^{1\cdot k} = x^k, \quad \psi_2 : x^k \mapsto x^{2\cdot k}$$
for $k = 0, 1, 2$. Therefore, $\mathrm{Aut}(G) = \{\psi_1, \psi_2\}$.
- $n = 4$: $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$. Then
$$\psi_1 : x^k \mapsto x^{1\cdot k} = x^k, \quad \psi_3 : x^k \mapsto x^{3\cdot k}$$
for $k = 0, 1, 2, 3$. Therefore, $\mathrm{Aut}(G) = \{\psi_1, \psi_3\}$.
- $n = 5$: $(\mathbb{Z}/5\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Then
$$\psi_1 : x^k \mapsto x^{1\cdot k}, \quad \psi_2 : x^k \mapsto x^{2\cdot k}, \quad \psi_3 : x^k \mapsto x^{3\cdot k}, \quad \psi_4 : x^k \mapsto x^{4\cdot k}$$
for $k = 0, 1, 2, 3, 4$. Therefore, $\mathrm{Aut}(G) = \{\psi_1, \psi_2, \psi_3, \psi_4\}$.
- $n = 6$: $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$. Then
$$\psi_1 : x^k \mapsto x^{1\cdot k} = x^k, \quad \psi_5 : x^k \mapsto x^{5\cdot k}$$
for $k = 0, 1, 2, 3, 4, 5$. Therefore, $\mathrm{Aut}(G) = \{\psi_1, \psi_5\}$. ■

Exercise 4.4.18

This exercise shows that for $n \neq 6$ every automorphism of S_n is inner. Fix an integer $n \geq 2$ with $n \neq 6$.

(a) Prove that the automorphism group of a group G permutes the conjugacy classes of G, i.e. for each $\sigma \in \mathrm{Aut}(G)$ and each conjugacy class $\mathcal{K}$ of G, the set $\sigma(\mathcal{K})$ is also a conjugacy class of G.

(b) Let $\mathcal{K}$ be the conjugacy class of transpositions in S_n and let $\mathcal{K}'$ be the conjugacy class of any element of order 2 in S_n that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$. Deduce that any automorphism of S_n sends transpositions to transpositions. (See Exercise 33 in Section 3.)

(c) Prove that for each $\sigma \in \mathrm{Aut}(S_n)$,
$$\sigma : (1\,2) \mapsto (a\,b_2), \qquad \sigma : (1\,3) \mapsto (a\,b_3), \qquad \ldots, \qquad \sigma : (1\,n) \mapsto (a\,b_n),$$
for some distinct integers $a, b_2, b_3, \ldots, b_n \in \{1, 2, \ldots, n\}$.

(d) Show that $(1\,2), (1\,3), \ldots, (1\,n)$ generate S_n and deduce that any automorphism of S_n is uniquely determined by its action on these elements. Use (c) to show that S_n has at most $n!$ automorphisms and conclude that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ for $n \neq 6$.

Exercise 4.4.19

This exercise shows that $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| \leq 2$ (Exercise 10 in Section 6.3 shows that equality holds by exhibiting an automorphism of S_6 that is not inner).

(a) Let $\mathcal{K}$ be the conjugacy class of transpositions in S_6 and let $\mathcal{K}'$ be the conjugacy class of any element of order 2 in S_6 that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$ unless $\mathcal{K}'$ is the conjugacy class of products of three disjoint transpositions. Deduce that $\mathrm{Aut}(S_6)$ has a subgroup of index at most 2 which sends transpositions to transpositions.

(b) Prove that $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| \leq 2$. (Follow the same steps as in (c) and (d) of the preceding exercise to show that any automorphism that sends transpositions to transpositions is inner.)

Exercise 4.4.20

For any finite group P let $d(P)$ be the minimum number of generators of P (so, for example, $d(P) = 1$ if and only if P is a nontrivial cyclic group and $d(Q_8) = 2$). Let $m(P)$ be the maximum of the integers $d(A)$ as A runs over all abelian subgroups of P (so, for example, $m(Q_8) = 1$ and $m(D_8) = 2$). Define

$$J(P) = \langle A \mid A \text{ is an abelian subgroup of } P \text{ with } d(A) = m(P) \rangle.$$

($J(P)$ is called the *Thompson subgroup* of P.)

(a) Prove that $J(P)$ is a characteristic subgroup of P.

(b) For each of the following groups P, list all abelian subgroups A of P that satisfy $d(A) = m(P)$: Q_8, D_8, D_{16}, and QD_{16} (where QD_{16} is the quasidihedral group of order 16 defined in Exercise 11 of Section 2.5). (Use the lattices of subgroups for these groups in Section 2.5.)

(c) Show that $J(Q_8) = Q_8$, $J(D_8) = D_8$, $J(D_{16}) = D_{16}$, and $J(QD_{16})$ is a dihedral subgroup of order 8 in QD_{16}.

(d) Prove that if $Q \leq P$ and $J(P)$ is a subgroup of Q, then $J(P) = J(Q)$. Deduce that if P is a subgroup (not necessarily normal) of the finite group G and $J(P)$ is contained in some subgroup Q of P such that $Q \trianglelefteq G$, then $J(P) \trianglelefteq G$.