Notes on *Abstract Algebra*

John Peloquin

Fall 2007

Abstract

Notes on *Abstract Algebra* by Dummit and Foote.

Exercises

Chapter 0

Section 0.3

EXERCISE 12–14. Let $n \in \mathbb{Z}$, $n \geq 1$. Then

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}$$

We first note that the set on the right is well defined. For suppose $a, b \in \mathbb{Z}$ and $a \equiv b$ mod n, so $a = b + nk$ for some $k \in \mathbb{Z}$. If $(b,n) = d > 1$, write $b = dk_1$ and $n = dk_2$, where $k_1, k_2 \in \mathbb{Z}$. Then

$$a = b + nk = dk_1 + (dk_2)k = d(k_1 + k_2 k)$$

so $d|a$, and $(a,n) > 1$. Hence if $(a,n) = 1$, then $(b,n) = 1$. Since b was arbitrary, this shows that the set is well defined. Now for the proof.

Proof. The case $n = 1$ is trivial, so we assume $n > 1$.

First, suppose $1 \leq a < n$ and $(a,n) = 1$. Then we know (Euclidean algorithm) that there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. In other words, $ax = 1 + n(-y)$, so $\overline{ax} = \overline{a} \cdot \overline{x} = \overline{1}$. Thus $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Conversely, suppose $1 \leq a < n$ and $(a,n) = d > 1$. Write $a = dk_1$ and $n = dk_2$, where $k_1, k_2 \in \mathbb{Z}$ and $1 \leq k_2 < n$. Then $ak_2 = dk_1k_2 = nk_1$, so $\overline{a} \cdot \overline{k_2} = \overline{0}$. Now $\overline{k_2} \neq \overline{0}$. But if there exists $b \in \mathbb{Z}$ such that $\overline{a} \cdot \overline{b} = \overline{1}$, then

$$\overline{k_2} = \overline{1} \cdot \overline{k_2} = (\overline{a} \cdot \overline{b}) \cdot \overline{k_2} = \overline{b} \cdot (\overline{a} \cdot \overline{k_2}) = \cdot \overline{k_2} = \overline{b} \cdot \overline{0} = \overline{0}$$

—a contradiction. Thus $\overline{a} \notin (\mathbb{Z}/n\mathbb{Z})^\times$. □

It follows from the above proof that $\mathbb{Z}/n\mathbb{Z}$ is partitioned into two subsets, one consisting of all elements with multiplicative inverses and the other consisting of all elements which are zero divisors. (Recall that $a \in \mathbb{Z}/n\mathbb{Z}$ is called a *zero divisor* iff $a \neq 0$ and there exists $b \in \mathbb{Z}/n\mathbb{Z}$, $b \neq 0$ such that $ab = 0$.)

Chapter 1

Section 1

EXERCISE 5. Let $n > 1$. Then $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication.

Proof. Note that $\overline{0}, \overline{1} \in \mathbb{Z}/n\mathbb{Z}$ and $\overline{0} \neq \overline{1}$. If $\mathbb{Z}/n\mathbb{Z}$ were a group under multiplication, then there would exist $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ such that

$$\overline{1} = \overline{0} \cdot \overline{a} = \overline{0 \cdot a} = \overline{0}$$

—a contradiction. □

EXERCISE 25. Let G be a group and suppose $x^2 = 1$ for all $x \in G$. Then G is abelian.

Proof. Let $a, b \in G$. Then

$$ab = (ba)^2 ab = bab(a^2)b = ba(b^2) = ba$$

□

EXERCISE 26. Let G be a group and $x \in G$. Set $H = \{x^n \mid n \in \mathbb{Z}\}$. Then H is a subgroup of G.

Proof. Note that $x^0 = e \in H$. If $x^m, x^n \in H$, then $x^m \cdot x^n = x^{m+n} \in H$, and $x^{-m} \in H$. Thus H is nonempty and closed under products and inverses, and so is a subgroup. □

We call H the *cyclic subgroup generated by* x and write $H = \langle x \rangle$.

EXERCISE 31. Let G be a group of even order. Then G contains an element of order 2.

Proof. Recall for $x \in G$, $|x| = 2$ iff $x \neq 1$ and $x^2 = 1$. Note $x^2 = 1$ iff $x = x^{-1}$. Set

$$A = \{x \in G \mid x = x^{-1}\} \qquad \text{and} \qquad B = \{x \in G \mid x \neq x^{-1}\}$$

Then $G = A \cup B$, where this union is disjoint, so $|G| = |A| + |B|$. Now $|B|$ is even since the elements of B come in pairs. Since $|G|$ is even by hypothesis, $|A|$ must also be even. We know $1 \in A$, hence $|A| \geq 2$ and thus there exists $x \in A$, $x \neq 1$ as desired. □

EXERCISE 32. Let G be a group and $x \in G$ with $|x| = n$. Then $1, x, \ldots, x^{n-1}$ are distinct.

Proof. Suppose there exist $0 \leq i < j \leq n-1$ such that $x^i = x^j$. Then by cancellation, $x^{j-i} = 1$. But $0 < j - i < n$, contradicting that n is least in $\mathbb{Z}^+$ with $x^n = 1$. □

This implies that if $|x| = n$, G contains at least n distinct elements, so $|x| \leq |G|$.

Let $H = \langle x \rangle$ (see Exercise 26). If $x^m \in H$, then write $m = nk + r$ where $0 \leq r < n$. We have

$$x^m = x^{nk+r} = (x^n)^k \cdot x^r = 1 \cdot x^r = x^r$$

Hence $H = \{1, x, \ldots, x^{n-1}\}$. In addition, these elements are distinct by this exercise. Hence $|H| = n$. Since x was arbitrary, we have: *the order of an element in a group is the order of the cyclic subgroup generated by that element.*

Exercise 36. Let $G = \{1, a, b, c\}$ be a group with order 4 and no elements of order 4. Then the group table for G is uniquely determined. In particular G is abelian.

Proof. Note that $1, a, b, c$ are all distinct. By Exercise 31, we may assume $a^2 = 1$. We compute ab by considering possible cases and using the cancellation laws:

- If $ab = 1$, then $b = a^{-1} = a$—a contradiction.
- if $ab = a$, then $b = 1$—a contradiction.
- If $ab = b$, then $a = 1$—a contradiction.

Thus we must have $ab = c$. Similarly $ba = c$ and $ac = b = ca$. Note that

$$c^2 = (ba)(ab) = b(a^2)b = b^2$$

To compute b^2, we first note by Exercise 32 and our hypotheses that $|b| \leq 3$.

- If $b^2 = a$, then $b^3 = ab = c$, so $b, b^2, b^3 \neq 1$—contradicting $|b| \leq 3$.
- If $b^2 = b$, then $b = 1$—a contadiction.
- If $b^2 = c$, then $c^2 = c$ (by the above), so $c = 1$—a contradiction.

Thus we must have $b^2 = 1$. This also implies $c^2 = 1$. Finally this gives $bc = a = cb$.

The group table for G is thus:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

The symmetry about the diagonal shows that G is abelian. (This also follows from Exercise 25 and the fact that $1^2 = a^2 = b^2 = c^2 = 1$.) □

Section 2

Exercise 1(a). We compute the order of each element in D_6. Recall

$$D_6 = \{1, r, r^2, s, sr, sr^2\}$$

where $r^3 = 1$, $s^2 = 1$, and $sr = rs^{-1}$. It is immediate that $|1| = 1$, $|r| = 3$, and $|s| = 2$. Note that $sr \neq 1$, but

$$(sr)^2 = s(rs)r = s(sr^{-1})r = s^2 = 1$$

hence $|sr| = 2$. Similarly, $sr^2 \neq 1$ but

$$(sr^2)^2 = sr(rs)rr = sr(sr^{-1})rr = s(rs)r = s(sr^{-1})r = 1$$

so $|sr^2| = 2$.

EXERCISE 2. Let $x \in D_{2n}$ and suppose x is not a power of r. Then $rx = xr^{-1}$.

Proof. We know we may write $x = s^k r^i$ for some (unique) $0 \leq k \leq 1$ and $0 \leq i \leq n-1$. Since x is not a power of r, we must have $k = 1$, so $x = sr^i$. Thus

$$rx = r(sr^i) = (rs)r^i = (sr^{-1})r^i = (sr^i)r^{-1} = xr^{-1}$$

□

EXERCISE 3. Let $x \in D_{2n}$ and suppose x is not a power of r. Then x has order 2.

Proof. As in the previous exercise, write $x = sr^i$, $0 \leq i \leq n-1$. Note $x \neq 1$, and

$$x^2 = (sr^i)^2 = s(r^i s)r^i = s(sr^{-i})r^i = 1$$

(where $r^i s = sr^{-i}$ follows by induction on i). Hence $|x| = 2$. □

EXERCISE 7. Let $G = \langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$. If $a = s$ and $b = sr$ where $s, r \in D_{2n}$, then G gives a presentation of D_{2n}.

Proof. Since $s = a$ and $r = s^2 r = ab$ and r, s generate D_{2n}, it follows that a, b also generate D_{2n}. Let $\mathscr{R}(G)$ be the set of relations that hold in G and $\mathscr{R}(D_{2n})$ be the set of relations that hold in D_{2n}. We claim that $\mathscr{R}(G) = \mathscr{R}(D_{2n})$.

Indeed, from $(ab)^n = 1$ it follows that $r^n = 1$, from $a^2 = 1$ it follows that $s^2 = 1$, and from $a^2 = b^2$ it follows that $s^2 = (sr)^2 = srsr$, so $s = rsr$, so $sr^{-1} = rs$. Since every relation in D_{2n} follows from these relations in r, s, we have $\mathscr{R}(D_{2n}) \subseteq \mathscr{R}(G)$.

Working these equations backwards and noting that every relation in G follows from the relations in a, b (by hypothesis), we have $\mathscr{R}(G) \subseteq \mathscr{R}(D_{2n})$. □

EXERCISE 8. In D_{2n}, $|\langle r \rangle| = |r| = n$ (see Exercise 1.32).

EXERCISE 12. Let D be a (regular) dodecahedron in $\mathbb{R}^3$. We count the symmetries of D in $\mathbb{R}^3$.

Label a face f on D and a vertex v on the face f. Any symmetry of D in $\mathbb{R}^3$ must take f to one of 12 possible face positions, and must take v to one of 5 possible vertex positions at that face position. Hence there are at most $5 \cdot 12 = 60$ symmetries.

On the other hand, since all of these positions are distinct and can be obtained using (distinct) symmetries, it follows that there are at least 60 symmetries. Hence there are exactly 60 symmetries.

EXERCISE 14. The set $\{1, -1\}$ generates $\mathbb{Z}$.

EXERCISE 15. $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \mid n\cdot\overline{1} = \underbrace{\overline{1}+\cdots+\overline{1}}_{n \text{ times}} = \overline{0}\rangle$

Proof. Recall that $\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\dots,\overline{n-1}\}$. Thus it is clear that $\overline{1}$ generates $\mathbb{Z}/n\mathbb{Z}$.

Suppose $\overline{r},\overline{s} \in \mathbb{Z}/n\mathbb{Z}$ and $\overline{r} = \overline{s}$. We claim that this relation can be derived from $n\cdot\overline{1} = \overline{0}$. Indeed, write $r - s = nk$ for $k \in \mathbb{Z}$. Then we have

$$\overline{r} - \overline{s} = \overline{r-s} = \overline{nk} = k(n\cdot\overline{1}) = k\cdot\overline{0} = \overline{0}$$

from which $\overline{r} = \overline{s}$ follows.

Hence we have a presentation of $\mathbb{Z}/n\mathbb{Z}$. □

Section 3

EXERCISE 1,3. Define the permutations σ,τ by

$$\begin{array}{llllll} \sigma: & 1\mapsto 3 & 2\mapsto 4 & 3\mapsto 5 & 4\mapsto 2 & 5\mapsto 1 \\ \tau: & 1\mapsto 5 & 2\mapsto 3 & 3\mapsto 2 & 4\mapsto 4 & 5\mapsto 1 \end{array}$$

Then we have the following cycle decompositions:

$$\begin{array}{ll} \sigma = (135)(24) & \sigma^2 = (153) \\ \tau = (15)(23) & \tau^2 = 1 \\ \sigma\tau = (2534) & \tau\sigma = (1243) \\ \tau^2\sigma = \sigma & \end{array}$$

And we have the following order calculations:

$$|\sigma| = 6 \quad |\sigma^2| = 3 \quad |\tau| = 2 \quad |\tau^2| = 1 \quad |\sigma\tau| = |\tau\sigma| = 4 \quad |\tau^2\sigma| = 6$$

EXERCISE 8. Let $\Omega = \{1,2,\dots\}$. Then S_Ω is infinite.

Proof. S_Ω contains the infinite subset $S = \{(1m) \mid m = 2,3,\dots\}$ of transpositions. □

EXERCISE 9(B). Let $\sigma = (12345678)$. Then by direct computation we have:

$$\begin{array}{ll} \sigma = (12345678) & \sigma^2 = (1357)(2468) \\ \sigma^3 = (14725836) & \sigma^4 = (15)(26)(37)(48) \\ \sigma^5 = (16385274) & \sigma^6 = (1753)(2864) \\ \sigma^7 = (18765432) & \sigma^8 = 1 \end{array}$$

If $i \in \mathbb{Z}$, let $k = i \mod 8$. Then $0 \le k < 8$ and there exists $j \in \mathbb{Z}$ such that $i = 8j + k$. Thus we have

$$\sigma^i = \sigma^{8j+k} = (\sigma^8)^j\sigma^k = 1^j\sigma^k = \sigma^k$$

It follows that σ^i is an 8-cycle iff i is congruent to one of $1,3,5,7 \pmod 8$.

EXERCISE 10. Let $\sigma = (a_0 a_2 \cdots a_{m-1})$ be an m-cycle. Then $|\sigma| = m$.

Proof. Note that $\sigma^i(a_j) = a_{j+i \mod m}$ (by induction on i). Since all of the a_j are distinct in the cycle notation, it follows that $\sigma^i(a_j) \neq a_j$ for $0 < i < m$, so $\sigma^i \neq 1$ for $0 < i < m$. But $\sigma^m(a_j) = a_j$ for all j—that is, $\sigma^m = 1$. Hence $|\sigma| = m$. □

EXERCISE 11. Let $\sigma = (1\ 2\ \cdots\ m)$, $m \in \mathbb{Z}$, $m \geq 1$. Then σ^i is an m-cycle iff $(i, m) = 1$.

Proof. For notational convenience we work with $\sigma = (0\ 1\ \cdots\ m-1)$. Note then

$$\sigma^i(k) = k + i \mod m \qquad (0 \leq k \leq m-1)$$

First suppose $(i, m) = d > 1$. Let $j = m/d$, $l = i/d$. Note $j < m$, and

$$(\sigma^i)^j = \sigma^{ij} = \sigma^{ml} = (\sigma^m)^l = 1^l = 1$$

Thus $|\sigma^i| < m$, so σ^i is not an m-cycle by Exercise 10.

Conversely, suppose $(i, m) = 1$. Fix $0 \leq k \leq m-1$, and suppose that there exists $0 < j < m$ such that $(\sigma^i)^j(k) = k$. Then by the first identity above, there must exist $l \in \mathbb{Z}$ such that

$$k + ij = ml + k$$

that is, $ij = ml$. But this is a contradiction since $j < m$ and i has no factors from m. On the other hand,

$$(\sigma^i)^m = \sigma^{im} = \sigma^{mi} = (\sigma^m)^i = 1^i = 1$$

hence in particular $(\sigma^i)^m(k) = k$. Since k was arbitrary, it is clear that σ^i is an m-cycle as desired, completing the proof. □

EXERCISE 15. Let $\sigma \in S_n$ and let m be the least common multiple of the lengths of the cycles in the cycle decomposition of σ. Then $|\sigma| = m$.

Proof. Let $\sigma = \sigma_1 \cdots \sigma_k$ be the cycle decomposition of σ. Observe that σ may be regarded as the product (or composite) in S_n of the cycles σ_i. Since these cycles are pairwise disjoint by hypothesis, they commute. Hence

$$\sigma^m = (\sigma_1 \cdots \sigma_k)^m = \sigma_1^m \cdots \sigma_k^m$$

by Exercise 1.24. Now $|\sigma_i|$ is just the length of σ_i, for all $1 \leq i \leq k$, by Exercise 10 above. Hence since m is a common multiple of these lengths by hypothesis, we have $\sigma_i^m = 1$ for $1 \leq i \leq k$. Thus $\sigma^m = 1$.

On the other hand, since m is the least common multiple, if $0 < j < m$, then there exists some cycle, say σ_i, such that j is not a multiple of $|\sigma_i|$. We claim that $\sigma_i^j \neq 1$. Indeed, let $p = |\sigma_i|$ and write $j = pq + r$ where $0 \leq r < p$. Then

$$\sigma_i^j = \sigma_i^{pq+r} = (\sigma_i^p)^q \sigma_i^r = 1^q \sigma_i^r = \sigma_i^r$$

If $\sigma_i^j = 1$, then $\sigma_i^r = 1$, so $r = 0$ and j is multiple of $|\sigma_i|$—contradicting our hypothesis. Hence $\sigma_i^j \neq 1$ as claimed.

Now by the pairwise disjointness of the cycles in σ, this implies that $\sigma \neq 1$. Hence we have shown that m is the least positive integer with $\sigma^m = 1$, that is, $|\sigma| = m$. □

One might conjecture, based on the above exercise, that for any group G and any arbitrary elements $x, y \in G$ with $|x| = m$ and $|y| = n$, that $|xy| = \operatorname{lcm}(m, n)$. But this is false. For example, let $G = S_3$, and set $x = (13)$ and $y = (12)$. Then $|x| = 2$ and $|y| = 2$, so $\operatorname{lcm}(|x|, |y|) = 2$. But $xy = (123)$, so $|xy| = 3 \neq 2$.

The key in the case of cycle decompositions is that the cycles are *disjoint*, so the action of one factor cannot 'alter' the action of another factor.

EXERCISE 18. We find all numbers n such that S_5 contains an element of order n.

Note that every permutation in S_5 must take one of the following forms:

$$(a_1)(a_2)(a_3)(a_4)(a_5) \quad (a_1)(a_2)(a_3)(a_4a_5) \quad (a_1)(a_2)(a_3a_4a_5)$$
$$(a_1)(a_2a_3a_4a_5) \quad (a_1)(a_2a_3)(a_4a_5) \quad (a_1a_2)(a_3a_4a_5) \quad (a_1a_2a_3a_4a_5)$$

where a_i, $1 \leq i \leq 5$, are distinct elements of $\{1,2,3,4,5\}$. Also elements of each of these forms exist in S_5. By Exercise 15 above, then, it follows that the orders of the elements in S_5 are precisely $n = 1,2,3,4,5,6$.

Note that this exercise demonstrates how useful cycle decompositions are. There are $5! = 120$ permutations in S_5. It would be extremely tedious to solve this problem by considering the permutations individually.

EXERCISE 20. We find a set of generators and relations for S_3.

It can be verified that $\sigma = (123)$ and $\tau = (12)$ generate S_3. Also it can be verified that the relations $\sigma^3 = 1$, $\tau^2 = 1$, and $\sigma\tau = \tau\sigma^{-1}$ hold and allow one to write any element of S_3 in the form $\tau^i\sigma^j$ where $0 \leq i \leq 1$ and $0 \leq j \leq 2$. Hence any equality relation is derivable from these relations, so

$$S_3 = \langle \sigma, \tau \mid \sigma^3 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$$

Section 4

EXERCISE 1. $|GL_2(\mathbb{F}_2)| = 6$

Proof. Let $a, b, c, d \in \mathbb{F}_2$. Then

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = 1 \iff \begin{array}{l} a = d = 1 \text{ and } (b = 0 \text{ or } c = 0), \text{ or} \\ b = c = 1 \text{ and } (a = 0 \text{ or } d = 0) \end{array}$$

This allows for six possible distinct configurations, hence $|GL_2(\mathbb{F}_2)| = 6$. □

EXERCISE 4. Let $n \geq 0$. Then $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.

Proof. Cases $n = 0, 1$ are trivial, so we assume $n > 1$.

Recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ denotes the subset of elements in $\mathbb{Z}/n\mathbb{Z}$ with multiplicative inverses. By Proposition 0.4, we know

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$$

where we may choose representatives $0 \leq a \leq n - 1$. The result follows by observing that n is prime iff $(a, n) = 1$ for all $0 < a \leq n - 1$. □

EXERCISE 5. Let F be a field. Then $GL_n(F)$ is finite iff F is finite.

Proof. If F is finite, then there are only finitely many $n \times n$ matrices over F, hence in particular only finitely many such matrices with inverses, so $GL_n(F)$ is finite.

If F is infinite, then there exist infinitely many matrices in $GL_n(F)$ of the form

$$\begin{pmatrix} a & & \\ & \ddots & \\ & & a \end{pmatrix} = a \cdot I_{n\times n}$$

with $a \in F$. □

EXERCISE 8. Let F be a field and $n \geq 2$. Then $GL_n(F)$ is nonabelian.

Proof. Let $0, 1 \in F$ denote the additive and multiplicative identities in F, respectively. Recall that $0 \neq 1$ by the field axioms. Set

$$A = \begin{pmatrix} 1 & \cdots & 1 \\ & \ddots & \vdots \\ & & 1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$$

(where a blank entry indicates a 0). Then

$$AB_{(1,1)} = 1\cdot 0 + \cdots + 1 \cdot 0 + 1 \cdot 1 = 1 \neq 0 = 0 \cdot 1 + 0 \cdot 0 + \cdots + 0 \cdot 0 + 1 \cdot 0 = BA_{(1,1)}$$

So $AB \neq BA$ and hence $GL_n(F)$ is nonabelian. □

Section 6

EXERCISE 1. Let G, H be groups and $\varphi : G \to H$ be a homomorphism. Then for all $x \in G$ and for all $n \in \mathbb{Z}$, $\varphi(x^n) = \varphi(x)^n$.

Proof. Fix $x \in G$. Note that

$$\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G) \cdot \varphi(1_G)$$

hence $\varphi(1_G) = 1_H$ by cancellation in H. This establishes the result for $n = 0$.

Note in addition that

$$\varphi(x) \cdot \varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1_G) = 1_H$$

Thus $\varphi(x^{-1}) = \varphi(x)^{-1}$ by uniqueness of inverses, so the result holds for $n = -1$.

For $n > 0$, proceed by induction. If the result holds for $n \geq 0$, then

$$\begin{aligned} \varphi(x^{n+1}) &= \varphi(x^n \cdot x) \\ &= \varphi(x^n) \cdot \varphi(x) \\ &= \varphi(x)^n \cdot \varphi(x) \\ &= \varphi(x)^{n+1} \end{aligned}$$

And hence the result holds for $n+1$. Finally, if the result holds for $n<0$, then

$$\begin{aligned}\varphi(x^{n-1}) &= \varphi(x^n \cdot x^{-1})\\ &= \varphi(x^n)\cdot\varphi(x^{-1})\\ &= \varphi(x)^n\cdot\varphi(x)^{-1}\\ &= \varphi(x)^{n-1}\end{aligned}$$

Hence the result holds for $n-1$.

This establishes the result for all $n \in \mathbb{Z}$. □

EXERCISE 2. Let $\varphi : G \to H$ be an isomorhism. Then $|\varphi(x)| = |x|$ for all $x \in G$. In addition, G and H have the same number of elements of each order n, for all $n > 0$.

Proof. Fix $x \in G$ and let $n = |x|$. Then

$$\varphi(x)^n = \varphi(x^n) = \varphi(1_G) = 1_H$$

by Exercise 1. On the other hand, if $0 < m < n$, then $x^m \neq 1_G$, and hence $\varphi(x)^n \neq 1_H$ by injectivity of φ. So $|\varphi(x)| = n$ as desired.

For each $n > 0$, let

$$X_n = \{x \in G \mid |x| = n\} \qquad \text{and} \qquad Y_n = \{y \in H \mid |y| = n\}$$

Note $\varphi|_{X_n}$ is an injection from X_n into Y_n. Moreover $\varphi|_{X_n}$ is a surjection since φ is a surjection. Thus $|X_n| = |Y_n|$. This establishes the second part of the result. □

EXERCISE 3. Let $\varphi : G \to H$ be an isomorphism. Then G is abelian iff H is abelian.

Proof. Suppose G is abelian. Let $a', b' \in H$ and set $a = \varphi^{-1}(a')$ and $b = \varphi^{-1}(b')$. Then

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = b'a'$$

Hence H is abelian.

Interchanging the roles of G and H establishes the converse. □

EXERCISE 4. $\mathbb{R}^\times \not\cong \mathbb{C}^\times$

Proof. Recall that $i \in \mathbb{C}^\times$ and $|i| = 4$. We claim that $\mathbb{R}^\times$ has no elements of order 4.

Indeed, if $r \in \mathbb{R}$ and $r^4 = 1$, then $(r^2)^2 = 1^2$, so $r^2 = 1$ by the uniqueness of nonnegative (square) roots in $\mathbb{R}$. Hence $|r| \leq 2$.

The result follows from Exercise 4. □

EXERCISE 5. $\mathbb{R} \not\cong \mathbb{Q}$

Proof. Immediate since $|\mathbb{R}| > |\mathbb{Q}|$. □

EXERCISE 6. $\mathbb{Q} \ncong \mathbb{Z}$

Proof. Suppose $\varphi : \mathbb{Q} \cong \mathbb{Z}$. Set $m = \varphi(1)$ and fix $n > 0$. Then

$$m = \varphi(1) = \varphi(n \cdot (1/n)) = n \cdot \varphi(1/n)$$

hence $\varphi(1/n) = m/n \in \mathbb{Z}$. But this is impossible as $n \to \infty$. □

EXERCISE 9. $D_{24} \ncong S_4$

Proof. We know that D_{24} has an element of order 12. However, by looking at cycle decompositions (cf. Exercise 3.18), we see that S_4 only has elements of orders $m = 1,2,3,4$. Thus the result follows from Exercise 4. □

EXERCISE 10. Let Δ, Ω be sets and suppose $|\Delta| = |\Omega|$. Then $S_\Delta \cong S_\Omega$.

Proof. Let $\pi : \Omega \to \Delta$ be a bijection. Define $\Phi : S_\Delta \to S_\Omega$ by

$$\Phi : \sigma \mapsto \pi^{-1} \circ \sigma \circ \pi$$

Note that Φ is well defined since if $\sigma \in S_\Delta$, then $\Phi(\sigma) \in S_\Omega$ (clearly $\Phi(\sigma) : \Omega \to \Omega$, and $\Phi(\sigma)$ is a bijection since the composite of bijections is a bijection).

Note that Φ is a homomorphism since if $\sigma, \tau \in S_\Delta$, then

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

Also Φ is injective by cancellation. Finally, if $\theta \in S_\Omega$, set $\sigma = \pi\theta\pi^{-1}$. Then $\sigma \in S_\Delta$ and $\Phi(\sigma) = \theta$, so Φ is surjective. □

Note how conjugation captures a type of ‘translation’ process.

For the next problem we need a definition: if $\varphi : G \to H$ is a homomorphism, define

$$\ker\varphi = \{x \in G \mid \varphi(x) = 1_H\}$$

called the *kernel* of φ. It is immediate that $\ker\varphi \le G$.

EXERCISE 14. Let $\varphi : G \to H$ be a homomorphism. Then φ is injective iff $\ker\varphi = 1$.

Proof. Suppose $\ker\varphi = 1$. If $\varphi(a) = \varphi(b)$, then

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1$$

hence $ab^{-1} \in \ker\varphi$. By hypothesis, then, $ab^{-1} = 1$, so $a = b$. Thus φ is injective.

Conversely, suppose φ is injective. We know $\varphi(1) = 1$, hence if $a \in \ker\varphi$, then we must have $a = 1$. Thus $\ker\varphi = 1$. □

EXERCISE 19. Let $G = \{ z \in \mathbb{C} \mid (\exists n > 0)[z^n = 1] \}$ and fix $k > 1$. Then the map $z \mapsto z^k$ is a surjective homomorphism from G to G, but is not an isomorphism.

Proof. Indeed, $(z_1 z_2)^k = z_1^k z_2^k$. If $z \in G$ with $z^n = 1$, let $w \in \mathbb{C}$ be any k-th root of z. Then $w^k = z$, and since $z^n = (w^k)^n = w^{kn} = 1$, we have $w \in G$.

But the map is not injective since the kernel consists of the k-th roots of unity, and there are k of these. □

EXERCISE 25. Let $n > 0$ and set $\theta = 2\pi/n$. Recall from linear algebra that the matrices

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

in $GL_2(\mathbb{R})$ represent in $\mathbb{R}^2$ a counterclockwise rotation about the origin by θ radians, and a reflection about the line $y = x$, respectively. Let r, s generate D_{2n} as usual.

We claim that $\varphi : D_{2n} \to GL_2(\mathbb{R})$ defined on the generators by $r \mapsto R$ and $s \mapsto S$ extends uniquely to an injective homomorphism.

Proof. Indeed, we define φ on D_{2n} by

$$r^{k_1} s^{k_2} \cdots r^{k_m} s^{k_{m+1}} \mapsto R^{k_1} S^{k_2} \cdots R^{k_m} S^{k_{m+1}}$$

This map is defined on all of D_{2n} since r, s generate D_{2n}. Moreover it is well defined and injective since R, S satisfy precisely the same relations in $GL_2(\mathbb{R})$ as r, s satisfy in D_{2n}. This map clearly extends the definition given on generators above, and it is the unique extension since any homomorphism mapping the generators that way must agree with it. □

Note that the map is not surjective since there are more elements in $GL_2(\mathbb{R})$ than those generated by R, S. We note that the map φ provides a *matrix representation* of the dihedral group (cf. permutation representations).

Section 7

EXERCISE 3. The additive group $\mathbb{R}$ acts on the plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Proof. For $x, y \in \mathbb{R}$, $0 \cdot (x, y) = (x + 0y, y) = (x, y)$, so the identity property holds. Also, if $r, s \in \mathbb{R}$,

$$\begin{aligned} (r+s) \cdot (x, y) &= (x + (r+s)y, y) \\ &= (x + ry + sy, y) \\ &= (x + sy + ry, y) \\ &= r \cdot (x + sy, y) = r \cdot (s \cdot (x, y)) \end{aligned}$$

Hence associativity holds as well. □

Note that this action is just a horizontal shear. The geometric fact that horizontal shears accumulate additively is reflected in the fact that the action is given by $\mathbb{R}$. (To compare, see that the action is not given by $\mathbb{R}^\times$, for example.)

EXERCISE 8(A). Let A be a nonempty set. Fix $k \in \mathbb{Z}$, $0 < k \leq |A|$, and let $\mathscr{A}$ be the set of all subsets of A of cardinality k. Then S_A acts on $\mathscr{A}$ by

$$\sigma \cdot \{a_1, \ldots, a_k\} \mapsto \{\sigma(a_1), \ldots, \sigma(a_k)\}$$

Proof. The identity and associativity properties hold trivially. □

We include this problem because it illustrates how a group of permutations of one type of object (in this case, elements of a set A) may naturally give rise to a group of permutations of another type of object. This is also seen, for example, in the regular action of S_A on itself.

EXERCISE 11. Let D_8 act on the vertices of a square. Label the vertices consecutively $1,2,3,4$, starting from a fixed vertex and moving in a clockwise manner. We write cycle decompositions of the elements in S_4 corresponding to the elements of D_8 under this action.

Proof. We have the following representation:

$$\begin{aligned}
1 &\mapsto 1 \\
r &\mapsto (1234) \\
r^2 &\mapsto (13)(24) \\
r^3 &\mapsto (1423) \\
s &\mapsto (24) \\
sr &\mapsto (24)(1234) = (14)(23) \\
sr^2 &\mapsto (24)(13)(24) = (13) \\
sr^3 &\mapsto (24)(1423) = (12)(34)
\end{aligned}$$

□

Note that this map is injective, hence we have obtained a faithful representation of D_8 in S_4. In other words, D_8 is isomorphic to a subgroup of S_4 (though note this must be a proper subgroup, since $|D_8| = 8$ and $|S_4| = 24$). Compare this with the faithful (matrix) representation obtained in Exercise 6.25.

EXERCISE 12. Let $n \in \mathbb{Z}^+$ be even, and label the vertices of a regular n-gon as above with labels from $V = \{1, \ldots, n\}$. Set

$$P = \{\{a, b\} \mid a, b \in V \text{ and } a, b \text{ label opposite vertices}\}$$

Then D_{2n} acts on P.

Proof. For convenience we identify V with the set of vertices of the n-gon, and P with the set of pairs of opposite vertices.

Let $\phi : D_{2n} \to S_V$ be the representation of D_{2n} given by the usual action of D_{2n} on V. Define $\psi : D_{2n} \to S_P$ as follows: for $\alpha \in D_{2n}$, set

$$\begin{aligned}\psi(\alpha) &: P \to P\\ \{a,b\} &\mapsto \{\phi(\alpha)(a), \phi(\alpha)(b)\}\end{aligned}$$

Note that $\psi(\alpha)$ is a well defined permutation of P, hence ψ is well defined. Also ψ is a homomorphism since ϕ is. Thus ψ defines an action of D_{2n} on P. □

We calculate the kernel of this action by cases:

1. If $n = 2$, then direct computation reveals that the action is trivial (that is, the kernel is all of D_4).

2. If $n = 4$, then direct computation reveals that

   $$\ker\psi = \{1, r^2, s, sr^2\}$$

   where r is the usual clockwise rotation through $\theta = \pi/2$, and s the reflection in the line passing through opposing vertices 1 and 3.

3. If $n > 4$, write $n = 2m$. Then we claim $\ker\psi = \{1, r^m\}$, where r is a clockwise rotation through $\theta = 2\pi/n$.

   Indeed, clearly $\{1, r^m\} \subseteq \ker\psi$. For the converse, first note that there are no other orientation preserving symmetries (powers of r) in $\ker\psi$. Suppose now, towards a contradiction, that $\alpha \in \ker\psi$ is orientation reversing. We may write $\alpha = r^k s$, where s is the reflection in the line passing through vertex 1 and its opposing vertex. Let $p_1, p_2, p_n \in P$, where $1 \in p_1$, $2 \in p_2$, and $n \in p_n$. Note that (the action of) s preserves p_1, but interchanges p_2 and p_n. Thus, since $\alpha \in \ker\psi$, r^k must interchange p_2 and p_n again, while fixing p_1. But this is impossible. Hence there are no orientation reversing symmetries in $\ker\psi$. It follows that $\ker\psi = \{1, r^m\}$ as claimed.

EXERCISE 16. Let G be a group. Then G acts on itself by conjugation, where

$$g \cdot x = gxg^{-1}$$

for all $g, x \in G$.

Proof. Clearly the identity property holds. If $g', g_2, x \in G$, then

$$\begin{aligned}(g'g_2)\cdot x &= (g'g_2)x(g'g_2)^{-1}\\ &= (g'g_2)x(g_2^{-1}g'^{-1})\\ &= g'(g_2xg_2^{-1})g'^{-1}\\ &= g'(g_2\cdot x)g'^{-1} = g'\cdot(g_2\cdot x)\end{aligned}$$

Hence associativity holds as well. □

EXERCISE 17. Let G be a group and fix $g \in G$. Then the operation of conjugation by g is an automorphism of G.

Proof. Indeed, let $x, y \in G$. Then

$$g(xy)g^{-1} = g(x(g^{-1}g)y)g^{-1} = (gxg^{-1})(gyg^{-1})$$

Hence conjugation by g is a homomorphism. We know that it is a bijection by the previous exercise. Hence it is an automorphism as desired. □

The previous two exercises show that conjugation in a group G is a very special group action, since from each group element we obtain not merely a permutation but an automorphism of G.

As an example, consider $G = GL_2(\mathbb{R})$, which for convenience we identify with the group of invertible linear transformations on $\mathbb{R}^2$. Each element $g \in G$ gives rise to a transformation of $\mathbb{R}^2$. Now if $x \in G$, and we view x as an operation on the pre-transformed space, then the transformation naturally corresponding to x in the g-transformed space is simply gxg^{-1}. Thus the operation of g on all of G produces a 'translated version' of G, where every $x \in G$ is 'relativized' to g. This 'translated version' of G is structurally identical to G.

EXERCISE 18. Let H be a group acting on a set A. Define a relation $\sim$ on A by

$$a \sim b \iff (\exists h \in H)(a = hb)$$

Then $\sim$ is an equivalence relation on A.

Proof. Let $a, b, c \in A$ be arbitrary. Then $a \sim a$ since $a = 1 \cdot a$ by the identity property of the action. If $a \sim b$, choose $h \in H$ with $a = hb$. We have

$$b = 1 \cdot b = (h^{-1}h)b = h^{-1}(hb) = h^{-1}a$$

hence $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, choose $h, g \in H$ with $a = hb$ and $b = gc$. Then

$$a = hb = h(gc) = (hg)c$$

hence $a \sim c$. Since a, b, c were arbitrary, this shows that reflexivity, symmetry, and transitivity hold for $\sim$, hence $\sim$ is an equivalence relation on A. □

The equivalence class of a is called the *orbit* of a under the action of H.

EXERCISE 19 (LAGRANGE). Let G be a finite group and H a subgroup of G. Then $|H|$ divides $|G|$.

Proof. Let H act on G by the left regular action. By the previous exercise, and the assumption that G is finite, we may partition G into finitely many orbits under H:

$$G = O(x_1) \cup \cdots \cup O(x_n)$$

But note that $O(x_i)$ is merely the image of H under the permutation (in G) of right multiplication by x_i. Hence $|O(x_i)| = |H|$ for all $1 \leq i \leq n$. Since G is partitioned, $|G| = n \cdot |H|$, so the result holds. □

EXERCISE 23. Let G be the group of rotations of a cube, and let G act on the set $A = \{p_1, p_2, p_3\}$ of three pairs of opposite faces of the cube. Then the kernel of this action is the subgroup H of G generated by $\{1, r_1, r_2, r_3\}$, where r_i is the rotation by π radians about the line passing through the centers of the two faces in p_i.

Proof. It is immediate that the kernel contains all of H, since it contains $\{1, r_1, r_2, r_3\}$.

To prove the converse, let ρ be any rotation in the kernel, and consider the effect of ρ on p_1. Either ρ swaps the two faces in p_1 or it does not. In the non-swapping case, either $\rho = 1$ or $\rho = r_1$. In the swapping case, it is easy to see that either $\rho = r_2$ or $\rho = r_3$. Hence H contains the kernel.

This shows that H is the kernel. □

In fact we see from the above proof that $H = \{1, r_1, r_2, r_3\}$. In addition we see that the action's representation of G is not faithful.

Note that the above proof could be simplified by just arguing directly that any element in the kernel is one of 1, r_1, r_2, or r_3. We leave the above proof as it is to illustrate the technique of using a subgroup generated by particular elements; in more complex cases, it might not be as easy to obtain an explicit list of the elements in the kernel.

Chapter 2

Section 1

EXERCISE 1.

(b) Let $G = \mathbb{C}^\times$ and $H = \{z \in G \mid |z| = 1\}$. Then $H \leq G$. *Proof:* $1 \in H$. If $z, w \in H$, then $|zw| = |z||w| = 1 \cdot 1 = 1$, so $zw \in H$. Similarly $|1/z| = 1/|z| = 1$, so $1/z \in H$.

(e) Let $G = \mathbb{R}^\times$ and $H = \{r \in G \mid r^2 \in \mathbb{Q}\}$. Then $H \leq G$. *Proof:* $1 \in H$. If $r, s \in H$, then $r^2 = m'/n_1$ and $s^2 = m''/n_2$ for some $m_i, n_i \in \mathbb{Z} - \{0\}$. But then

$$(rs)^2 = r^2 \cdot s^2 = \left(\frac{m'}{n_1}\right)\left(\frac{m''}{n_2}\right) = \frac{m'm''}{n_1 n_2} \in \mathbb{Q}$$

hence $rs \in H$. Similarly $(1/r)^2 = 1/r^2 = n_1/m' \in \mathbb{Q}$, so $1/r \in H$.

EXERCISE 2.

(a) Fix $n \geq 3$, set $G = S_n$ and let S be the set of 2-cycles in G. Then $S \not\leq G$. *Proof:* Note that $(12), (13) \in S$, but $(13)(12) = (123) \notin S$.

(e) Let $G = \mathbb{R}$ and let $S = \{r \in G \mid r^2 \in \mathbb{Q}\}$. Then $S \not\leq G$. *Proof:* Note $\sqrt{2}, \sqrt{3} \in S$, but

$$(\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 = 5 + \sqrt{6}$$

which is not rational since $\sqrt{6}$ is not rational. Hence $(\sqrt{2} + \sqrt{3}) \notin S$.

EXERCISE 4. Let $G = \mathbb{Z}$ and let $\mathbb{N}$ be the subset of nonnegative integers. Then $\mathbb{N}$ is infinite and closed under the group operation, but $\mathbb{N}$ is not a subgroup since it does not contain additive inverses.

Alternately let $G = \mathbb{Q}^\times$. Then $\mathbb{Z}$ is an infinite subset and is closed under the group operation, but it is not a subgroup since it does not contain multiplicative inverses.

EXERCISE 5. Let G be a group suppose $n = |G| > 2$. Then G does not have a subgroup of order $n-1$.

Proof. Suppose $H \le G$ and $|H| = n-1$. Since $|H| > 1$, we may choose $h \in H$, $h \neq 1$. Let g be the unique element of $G - H$. Now $hg \neq g$, hence $hg \in H$. But then since $h \in H$, we have $h^{-1} \in H$ and

$$h^{-1}(hg) = (h^{-1}h)g = 1 \cdot g = g \in H$$

—contradicting the fact that $g \not\in H$. □

EXERCISE 6. Let G be an abelian group and define

$$H = \{g \in G \mid |g| < \infty\}$$

Then H is a subgroup of G (called the *torsion subgroup* of G).

Proof. Clearly $1 \in H$. Suppose $x, y \in H$, and let $m = |x|$ and $n = |y|$. Then

$$(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = 1^n \cdot 1^m = 1 \cdot 1 = 1$$

Thus $|xy| < \infty$, so $xy \in H$. Similarly $(x^{-1})^m = (x^m)^{-1} = 1^{-1} = 1$, so $x^{-1} \in H$. □

EXERCISE 7. Fix $n \in \mathbb{Z}$, $n > 1$ and let $G = \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Then G is an abelian group, and it is clear that the torsion subgroup of G is $\{(0, a) \mid a \in \mathbb{Z}/n\mathbb{Z}\}$.

The subset of G consisting of the elements of infinite order (together with 0) is not a subgroup. Indeed, $(-1,0)$ and $(1,1)$ have infinite order, but $(-1,0)+(1,1) = (0,1)$ has finite order (and is not 0).

EXERCISE 8. Let $H, K \le G$. Then $H \cup K \le G$ iff $H \subseteq K$ or $K \subseteq H$.

Proof. One direction is trivial.

Suppose $H \not\subseteq K$ and $K \not\subseteq H$. Choose $h \in H - K$ and $k \in K - H$. Then $h, k \in H \cup K$, but $hk \not\in H \cup K$. Indeed, if $hk \in H$, then $h^{-1}(hk) = (h^{-1}h)k = k \in H$—a contradiction—and if $hk \in K$, then $(hk)k^{-1} = h(kk^{-1}) = h \in K$—a contradiction. Thus $H \cup K$ is not a subgroup of G. □

EXERCISE 9. Let $G = GL_n(F)$, F an arbitrary field. Define

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

Then $SL_n(F) \le GL_n(F)$ (called the *special linear group*).

Proof. Clearly $1 \in SL_n(F)$. If $A, B \in SL_n(F)$, then $AB \in SL_n(F)$ since

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$$

Similarly $A^{-1} \in SL_n(F)$ since $\det(A^{-1}) = 1$. □

EXERCISE 10(B). Let G be a group and $\mathscr{H}$ be an arbitrary nonempty collection of subgroups of G. Then $\bigcap\mathscr{H} \le G$.

Proof. Note that $\bigcap\mathscr{H} \subseteq G$ since $\mathscr{H}$ is nonempty. Now $1 \in \bigcap\mathscr{H}$ since $1 \in H$ for all $H \in \mathscr{H}$. Suppose $x, y \in \bigcap\mathscr{H}$. If $H \in \mathscr{H}$ is arbitrary, then $x, y \in H$, so $xy \in H$ since $H \le G$. Since H was arbitrary, $xy \in \bigcap\mathscr{H}$. Similarly $x^{-1} \in \bigcap\mathscr{H}$. Thus $\bigcap\mathscr{H} \le G$. □

EXERCISE 13. Let $0 < H \le \mathbb{Q}$ and suppose $1/x \in H$ for all nonzero $x \in H$. Then $H = \mathbb{Q}$.

Proof. Fix $x \in H$, $x \ne 0$. Write $x = m/n$ where $m, n \in \mathbb{Z}$, $m \ne 0$ and $n > 0$. Note that

$$m = n \cdot \left(\frac{m}{n}\right) = n \cdot x = \underbrace{x + \cdots + x}_{n \text{ times}} \in H$$

Hence $m \in H$, and since $m \ne 0$, $1/m \in H$. But then, as above, $m \cdot (1/m) = 1 \in H$.

Now let $y \in \mathbb{Q}$ be arbitrary. Write $y = m'/n'$, with $m', n' \in \mathbb{Z}$ and $n' > 0$. We have $n' = n' \cdot 1 \in H$ since $1 \in H$. Since $n' > 0$, $1/n' \in H$. Finally, $m'/n' = m' \cdot (1/n') \in H$. Thus, since y was arbitrary, $H = \mathbb{Q}$. □

This result shows, in particular, that $\mathbb{Q}$ is the smallest additive subgroup containing $\mathbb{Z}$ and closed under multiplicative inverses.

EXERCISE 15. Let G be a group and $\mathscr{H}$ be a nonempty chain of subgroups of G. Then $\bigcup\mathscr{H} \le G$.

Proof. Fix $H \in \mathscr{H}$. Then $1 \in H \subseteq \bigcup\mathscr{H}$. Suppose $x, y \in \bigcup\mathscr{H}$. Then $x \in H$ and $y \in K$ for some $H, K \in \mathscr{H}$. Since $\mathscr{H}$ is a chain, either $H \subseteq K$ or $K \subseteq H$, so $H \cup K$ is a subgroup equal to one of them (cf. Exercise 8). Now $x, y \in H \cup K$, so $xy \in H \cup K \subseteq \bigcup\mathscr{H}$. Also $x^{-1} \in H \subseteq \bigcup\mathscr{H}$. It follows that $\bigcup\mathscr{H} \le G$. □

Section 2

EXERCISE 6. Let $H \le G$. Then $H \le N_G(H)$, and $H \le C_G(H)$ iff H is abelian.

Proof. For the first claim, let $h \in H$. Then $hHh^{-1} \subseteq H$. If $h' \in H$, then $h^{-1}h'h \in H$, so $h' = h(h^{-1}h'h)h^{-1} \in hHh^{-1}$. Thus $hHh^{-1} = H$. Since h was arbitrary, $H \le N_G(H)$.

The second claim is immediate from definitions. □

EXERCISE 7. Let $n \in \mathbb{Z}$, $n \ge 3$. If n is odd, $Z(D_{2n}) = 1$, and if n is even, $Z(D_{2n}) = \{1, r^k\}$, where $n = 2k$.

Proof. Note that $Z(D_{2n}) = C(r) \cap C(s)$ since r, s generate D_{2n}. Now we know that $C(r) = \langle r \rangle = \{1, r, \ldots, r^{n-1}\}$. We also know $\{1, s\} \le C(s)$. We claim that $r^i \in C(s)$ for some $0 < i < n$ iff n is even, and in this case $n = 2i$.

Indeed, suppose $r^i \in C(s)$ for $0 < i < n$. Then $sr^i = r^i s = sr^{-i}$, so by cancellation $r^i = r^{-i}$, or $r^{2i} = 1$. It follows that $n|2i$. Now if n is odd, then $n|i$—contradicting that $0 < i < n$. Hence n must be even. In addition, since $2i < 2n$, we must have $2i = n$. The converse claim is trivial.

Now if n is odd, then $C(s) = \{1, s\}$, hence we must have $Z(D_{2n}) = 1$. If n is even, then $C(s) = \{1, r^k, s, sr^k\}$, where $n = 2k$. Hence $Z(D_{2n}) = \{1, r^k\}$. □

In the above proof, we see an instance of the general result that if G is a group, $S \subseteq G$, and $G = \langle S \rangle$, then $Z(G) = \bigcap\{C_G(s) \mid s \in S\}$. In particular, $|Z(G)|$ divides $|C_G(s)|$ for all $s \in S$ (by Lagrange's Theorem).

The following result is also useful in the computation of centralizers: if G is a group and $g \in G$, then $C_G(g) = C_G(\langle g \rangle)$. In particular, if $|g| = n$, and $(m, n) = 1$, then $C_G(g^m) = C_G(g)$ since $\langle g^m \rangle = \langle g \rangle$.

EXERCISE 13. Fix $n \in \mathbb{Z}$, $n > 0$ and let R be the set (ring) of all polynomials in $x_1, \dots, x_n$ over $\mathbb{Z}$. For each $\sigma \in S_n$, define the map $\sigma : R \to R$ by

$$\sigma : p(x_1, \dots, x_n) \mapsto p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

This mapping defines a (left) action of S_n on R.

Proof. The identity and associativity properties are immediate. □

From this exercise we see that the permutations in S_n naturally induce permutations on polynomials in n variables.

Section 3

NOTE. Let $G = \langle x \rangle$. Then

(a) If $|x| = n$, $\langle x^a \rangle \le \langle x^b \rangle$ iff $(b, n) | (a, n)$.

Proof. If $\langle x^a \rangle \le \langle x^b \rangle$, then $|x^a|$ divides $|x^b|$ by Lagrange and Proposition 2. By Proposition 5, this means

$$\frac{n}{(a,n)} \cdot k = \frac{n}{(b,n)}$$

for some $k \in \mathbb{Z}$. In other words, $(b, n) \cdot k = (a, n)$, so $(b, n) | (a, n)$ as desired.

Conversely, if $(a, n) = k \cdot (b, n)$ for some $k \in \mathbb{Z}$, then

$$x^{(a,n)} = x^{k \cdot (b,n)} = (x^{(b,n)})^k \in \langle x^{(b,n)} \rangle$$

Hence $\langle x^{(a,n)} \rangle \le \langle x^{(b,n)} \rangle$. But $\langle x^a \rangle = \langle x^{(a,n)} \rangle$ and $\langle x^b \rangle = \langle x^{(b,n)} \rangle$ by Theorem 7(3). This completes the proof. □

(b) If $|x| = \infty$, $\langle x^a \rangle \le \langle x^b \rangle$ iff $b | a$.

Proof. If $x^a \in \langle x^b \rangle$, then $x^a = (x^b)^k = x^{bk}$ for some $k \in \mathbb{Z}$. This gives $x^{a-bk} = 1$, so we must have $a - bk = 0$ since $|x| = \infty$. Thus $a = bk$, or $b | a$ as desired.

The converse is immediate. □

It follows from these results that for $G = \langle x \rangle$, if $|G| = n$, then $\langle x^b \rangle = G$ iff $(b, n) = 1$; and if $|G| = \infty$, then $\langle x^b \rangle = G$ iff $b = \pm 1$ (cf. Proposition 6).

We also obtain the following specific case (cf. p. 59): if $n \ge 1$ and $1 \le a, b \le n$, then $\langle \overline{a} \rangle \le \langle \overline{b} \rangle$ in $\mathbb{Z}/n\mathbb{Z}$ iff $(b, n) | (a, n)$.

EXERCISE 1. We determine the subgroup structure (lattice) of $Z_{45} = \langle x \rangle$.

Note that $45 = 3 \cdot 3 \cdot 5$, with positive divisors $1, 3, 5, 9, 15, 45$. Hence by Theorem 7, the subgroups of Z_{45} are

$$\langle 1 \rangle \quad \langle x^{15} \rangle \quad \langle x^9 \rangle \quad \langle x^5 \rangle \quad \langle x^3 \rangle \quad \langle x \rangle$$

By the result above, we see that $\langle x^a \rangle \leq \langle x^b \rangle$ iff $(b, 45) | (a, 45)$ for $1 \leq a, b \leq 45$.

EXERCISE 5. Let $G = \mathbb{Z}/49000\mathbb{Z}$. Note that $49000 = 2^3 \cdot 5^3 \cdot 7^2$, hence by Proposition 6, the number of generators in G is given by

$$\begin{aligned} \varphi(49000) &= \varphi(2^3) \cdot \varphi(5^3) \cdot \varphi(7^2) \\ &= 2^2(1) \cdot 5^2(4) \cdot 7(6) \\ &= 4 \cdot 100 \cdot 42 \\ &= 16800 \end{aligned}$$

EXERCISE 12. The following groups are noncyclic: $Z_2 \times Z_2$, $Z_2 \times \mathbb{Z}$, and $\mathbb{Z} \times \mathbb{Z}$.

Proof. Note that each element in $Z_2 \times Z_2$ has order at most 2, hence the group cannot be cyclic (for this requires an element of order 4).

If (a, b) generates $Z_2 \times \mathbb{Z}$, then we must have $b = \pm 1$ by Proposition 6. Clearly we cannot have $a = 1$, for $\langle (1, b) \rangle = 1 \times \mathbb{Z} < Z_2 \times \mathbb{Z}$. But we also cannot have $a = x$, because for example $(1, 1) \notin \langle (x, b) \rangle$. Since these possibilities are exhaustive, there is no generator for the group.

Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Define

$$x = \begin{cases} (1, -1) & \text{if } a \text{ and } b \text{ have the same sign} \\ (1, 1) & \text{if not} \end{cases}$$

Then $x \notin \langle (a, b) \rangle$. Since (a, b) was arbitrary, there is no generator for the group. □

EXERCISE 13. Note that $\mathbb{Z} \times Z_2$ is not isomorphic to $\mathbb{Z}$ since $\mathbb{Z}$ is cyclic but $\mathbb{Z} \times Z_2$ is not (cf. Exercise 12).

We claim that $\mathbb{Q} \times Z_2$ is not isomorphic to $\mathbb{Q}$. Indeed, if $\varphi : \mathbb{Q} \times Z_2 \to \mathbb{Q}$ is an injective homomorphism, then $\varphi(0, x) = q \neq 0$. But then

$$\varphi((0, x) \cdot (0, x)) = \varphi(0, 1) = 0 \neq q + q = \varphi(0, x) + \varphi(0, x)$$

—a contradiction.

EXERCISE 15. Note that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic by Theorem 7 since $1 \times \mathbb{Q} \leq \mathbb{Q} \times \mathbb{Q}$ but $1 \times \mathbb{Q} \cong \mathbb{Q}$ is not cyclic (see Exercise 4.14(d) below).

EXERCISE 16. Let G be a group and suppose $x, y \in G$ commute. Set $m = |x|$ and $n = |y|$. Then $|xy|$ divides $\operatorname{lcm}(m,n)$.

Proof. Indeed, write $\alpha = \operatorname{lcm}(m,n)$. Since $m|\alpha$ and $n|\alpha$, $x^\alpha = 1$ and $y^\alpha = 1$. Then since x and y commute, $(xy)^\alpha = x^\alpha \cdot y^\alpha = 1$. The result follows from Proposition 3. □

Note that $|xy|$ need not equal $\operatorname{lcm}(m,n)$. Indeed, let $G = S_3$ and set $x = y = (12)$. Then $m = n = 2$, so $\operatorname{lcm}(m,n) = 2$, but $xy = 1$ so $|xy| = 1 < 2$.

Also the result need not hold if x, y do not commute. Again in S_3, set $x = (12)$ and $y = (13)$. Then $\operatorname{lcm}(m,n) = 2$. But $xy = (132)$, so $|xy| = 3$, which does not divide 2.

EXERCISE 23. The group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is noncyclic for $n \geq 3$.

Proof. Fix $n \geq 3$ and let $G = (\mathbb{Z}/2^n\mathbb{Z})^\times$. We claim that $x = 2^{n-1} - 1$ and $y = 2^{n-1} + 1$ are two distinct elements of order 2 in G, from which it follows that G cannot be cyclic by Theorem 7(3).

Note that $0 < x < y < 2^n$. Thus if $x = 1$ (in G), then $2^{n-1} - 1 = 1$ (in $\mathbb{Z}$), which implies $2^{n-2} = 1$—a contradiction since $n \geq 3$. On the other hand,

$$x^2 = (2^{n-1} - 1)^2 = (2^{n-1})^2 - 2 \cdot 2^{n-1} + 1 = (2^n)^2 \cdot 2^{-2} - 2^n + 1 = 1$$

Hence $|x| = 2$. Similarly $y \neq 1$ but since $y = -x$, $y^2 = (-x)^2 = x^2 = 1$, so $|y| = 2$. It is easy to check that $x \neq y$, hence x and y are two distinct elements of order 2, establishing our claim. □

EXERCISE 25. Let G be a cyclic group of order n and let k be relatively prime to n. Then the map $\varphi : g \mapsto g^k$ is an automorphism of G.

Proof. Write $G = \langle x \rangle$. Then φ is a homomorphism since

$$\begin{aligned} \varphi(x^a \cdot x^b) &= \varphi(x^{a+b}) \\ &= (x^{a+b})^k \\ &= x^{(a+b)k} \\ &= x^{ak} \cdot x^{bk} \\ &= \varphi(x^a) \cdot \varphi(x^b) \end{aligned}$$

Now $\langle x^k \rangle = G$ since $(k,n) = 1$ by Proposition 6. Hence for any $x^a \in G$, there exists m such that $x^a = (x^k)^m = x^{km} = (x^m)^k$, so $\varphi(x^m) = x^a$. Therefore φ is a surjective homomorphism. But since G is finite, this means φ is an automorphism. □

If G is an arbitrary group of order n and $(k,n) = 1$, then the map $\varphi : g \to g^k$ may not be a homomorphism. For example, let $G = D_6$ (so $n = 6$) and let $k = 5$. Then $(k,n) = 1$, but

$$\varphi(rs) = (rs)^5 = rs \neq r^2 s = r^5 \cdot s^5 = \varphi(r) \cdot \varphi(s)$$

However, in general the map is still surjective. Indeed, for G arbitrary and $g \in G$, let $H = \langle g \rangle$ and let $m = |g|$. Then by Lagrange's Theorem, $m|n$, hence $(k,m) = 1$. Note that $\varphi|_H : H \to H$. Hence by the above exercise there exists $h \in H$ such that $\varphi(h) = g$.

On the other hand, if $(k,n) > 1$, then by Cauchy's Theorem (Section 3.2) there exists $x \in G$ with $|x| = d > 1$ and $d|k$. Then $x \neq 1$ but $x^k = 1$, so the the map $g \mapsto g^k$ is not injective, and hence not surjective since G is finite. Thus we obtain: for G of order n, the map $g \mapsto g^k$ is surjective iff $(k,n) = 1$.

EXERCISE 26. Let Z_n be a cyclic group of order n. For $a \in \mathbb{Z}$, define

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

(a) σ_a is an automorphism of Z_n iff $(a,n) = 1$. (*Proof:* previous exercise).

(b) $\sigma_a = \sigma_b$ iff $a \equiv b \pmod n$.

Proof. If $a \equiv b$, then $a = b + nk$ for some $k \in \mathbb{Z}$, hence

$$\sigma_a(x) = x^a = x^{b+nk} = x^b \cdot (x^n)^k = x^b = \sigma_b(x)$$

for all $x \in Z_n$, that is, $\sigma_a = \sigma_b$. Conversely, if $\sigma_a = \sigma_b$ and $Z_n = \langle y \rangle$, then $y^a = y^b$, so $y^{a-b} = 1$, so $n|(a-b)$, so $a \equiv b$. □

(c) Every automorphism of Z_n is of the form σ_a for some $a \in \mathbb{Z}$.

Proof. Let σ be an automorphism of Z_n and write $Z_n = \langle y \rangle$. Then $\sigma(y) = y^a$ for some $a \in \mathbb{Z}$. If $x \in Z_n$, then $x = y^b$ for some $b \in Z$, hence

$$\sigma(x) = \sigma(y^b) = \sigma(y)^b = (y^a)^b = y^{ab} = (y^b)^a$$

Thus $\sigma = \sigma_a$. □

(d) $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(Z_n)$

Proof. We claim the map $\overline{a} \mapsto \sigma_a$ witnesses the isomorphism. Indeed, by part (b) this map is well defined and injective. By parts (a)–(c), the map is surjective. And the map satisfies the homomorphism property since

$$\sigma_{ab}(x) = x^{ab} = (x^b)^a = \sigma_a \circ \sigma_b(x)$$

for all $x \in Z_n$, hence $\sigma_{ab} = \sigma_a \circ \sigma_b$. □

Note that this result shows that $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$. By Theorem 4, this result actually gives the structure of the automorphism group for any finite cyclic group of order n.

Section 4

EXERCISE 3. Suppose $H \leq G$ is abelian. Then $\langle H, Z(G)\rangle$ is abelian.

Proof. Let $x, y \in \langle H, Z(G)\rangle$. Then by Proposition 9, x and y are both finite products of elements all of which commute with each other. Hence $xy = yx$. □

Note this result does not hold in general for the centralizer of an abelian subgroup. Let $G = S_5$ and $H = \langle(12)\rangle$. Then H is abelian, and $(34), (45) \subseteq C(H)$, but $\langle H, C(H)\rangle$ is nonabelian since $(34)(45) = (345) \neq (354) = (45)(34)$.

EXERCISE 5. Suppose $x, y \in S_3$ with $x \neq y$ and $|x| = 2 = |y|$. Then $\langle x, y\rangle = S_3$.

Proof. Note that $\{1, x, y, xy\} \subseteq \langle x, y\rangle$. It is easily verified using cancellation that these elements are distinct, hence $|\langle x, y\rangle| \geq 4$. But then by Lagrange's Theorem, we must have $|\langle x, y\rangle| = 6$, that is, $\langle x, y\rangle = S_3$. □

EXERCISE 6. Let $x = (12)$ and $y = (12)(34)$ (in S_4). Then $\langle x, y\rangle$ is noncyclic of order 4.

Proof. It is easily verified that $\langle x, y\rangle = \{1, x, y, xy\}$, where these elements are distinct. Hence $|\langle x, y\rangle| = 4$. But there are no elements in this group of order 4, hence it is noncyclic (and isomorphic to the Klein Four group by Exercise 1.1.36). □

EXERCISE 13. Let $G = (\mathbb{Q}^+)^\times$. Then $G = \langle 1/p \mid p \text{ prime}\rangle$.

Proof. Write $S = \{1/p \mid p \text{ prime}\}$ and $H = \langle S\rangle$. We require $H = G$.

Let $q \in G$. Then $q = m/n$ for some $m, n \in \mathbb{Z}^+$. By prime factorization, write $n = p_1 \cdots p_j$. Note that $1/p_1, \ldots, 1/p_j \in S$, hence the product

$$\left(\frac{1}{p_1}\right)\cdots\left(\frac{1}{p_j}\right) = \frac{1}{p_1 \cdots p_j} = \frac{1}{n} \in H$$

Similarly $1/m \in H$, and hence $1/(1/m) = m \in H$. But then $m \cdot (1/n) = m/n = q \in H$. Since q was arbitrary, $H = G$. □

EXERCISE 14.

(c) Let $H \leq \mathbb{Q}$ be finitely generated. Then H is cyclic.

Proof. Write $H = \langle A\rangle$ where $A = \{m'/n_1, \ldots, m_k/n_k\}$. Set $q = 1/(n_1 \cdots n_k)$. Then $A \subseteq \langle q\rangle$, since

$$\frac{m_i}{n_i} = (m_i n_1 \cdots n_{i-1} n_{i+1} \cdots n_k) \cdot q$$

Hence $H \leq \langle q\rangle$. By Theorem 2.3.7, H is cyclic. □

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

Proof. This follows from (c) and the fact that $\mathbb{Q}$ is not cyclic: for $q = m/n > 0$ arbitrary, note that

$$-kq < 0 < \frac{m}{n+1} < \frac{m}{n} \leq kq \qquad (k \in \mathbb{Z}, k > 0)$$

Hence $\langle q\rangle < \mathbb{Q}$. Since q was arbitrary, $\mathbb{Q}$ is noncyclic. □

EXERCISE 16.

(a) Let H be a proper subgroup of a finite group G. Then there exists a maximal subgroup of G containing H.

Proof. Since G is finitely generated, this follows from the proof of Exercise 17 by setting $H_0 = H$. □

(b) Let $G = D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ and set $H = \langle r \rangle$. Then H is maximal.

Proof. We have $H \neq G$ since $s \notin H$. Suppose $H < H'$. Choose $x \in H' - H$ and write $x = sr^k$ where $0 \leq k < n$. Then since $r^{n-k} \in H$,

$$x \cdot r^{n-k} = (sr^k) \cdot r^{n-k} = s \cdot (r^k r^{n-k}) = s \cdot r^n = s \in H'$$

Hence $r, s \in H'$, so $H' = G$. Since H' was arbitrary, H is maximal. □

(c) Let $G = \langle x \rangle$ be cyclic of order n. Then $H \leq G$ is maximal iff $H = \langle x^p \rangle$ for some prime p dividing n.

Proof. Suppose $H \leq G$ is maximal. Write $H = \langle x^d \rangle$ where $d \geq 1$ and $d|n$ (by Theorem 2.3.7). Since $H \neq G$, we have $d > 1$. Suppose $d = ab$ with $1 < a, b < d$. Then $\langle x^d \rangle < \langle x^a \rangle < G$ by the above note, contradicting the maximality of H. Therefore d is prime.

Conversely, suppose $H = \langle x^p \rangle$ for some $p|n$. Then $H \neq G$ since $(p, n) = p > 1$. Suppose $H < H' < G$. Then $H' = \langle x^d \rangle$ for some $d > 1$ such that $d|p$ but not $p|d$—contradicting that p is prime. Therefore H is maximal. □

EXERCISE 17. Let G be a nontrivial finitely generated group. Then G has a maximal subgroup.

Proof. Let $\mathscr{G}$ be the set of all subgroups of G. Define a relation R from $\mathscr{G}$ to G by

$$H\,R\,g \iff H < \langle H \cup \{g\} \rangle < G$$

Let F be a choice function for R. Note that for $H \in \mathscr{G}$, $H \notin \mathrm{dom}(F)$ iff either $H = G$ or H is maximal in G.

Let Ω denote the class of all ordinals and construct a recursion $H : \Omega \to \mathscr{G}$ as follows:

$$H_\alpha = \begin{cases} 1 & \text{if } \alpha = 0 \\ \langle H_\beta \cup \{F(H_\beta)\} \rangle & \text{if } \alpha = \beta^+ \text{ and } H_\beta \in \mathrm{dom}(F) \\ H_\beta & \text{if } \alpha = \beta^+ \text{ and } H_\beta \notin \mathrm{dom}(F) \\ \bigcup_{\beta < \alpha} H_\beta & \text{if } \alpha \text{ is a limit ordinal} \end{cases}$$

It is easily verified by induction that $\alpha < \beta$ implies $H_\alpha \subseteq H_\beta$ for all $\alpha, \beta \in \Omega$, and hence by induction again that $H_\alpha \in \mathscr{G}$ for all $\alpha \in \Omega$.

Let γ be the Hartogs number of $\mathscr{G}$. Since $H|_\gamma : \gamma \to \mathscr{G}$ cannot be injective, there must exist ordinals $\delta < \varepsilon < \gamma$ such that $H_\delta = H_\varepsilon$. Note that $\delta < \delta^+ \leq \varepsilon$, hence

$$H_\delta \subseteq H_{\delta^+} \subseteq H_\varepsilon \subseteq H_\delta$$

so $H_\delta = H_{\delta^+}$. By the definition of our recursion above, this implies that $H_\delta \notin \operatorname{dom}(F)$, which means either $H_\delta = G$ or H_δ is maximal in G.

To rule out the first case, we prove (by induction) that $H_\alpha < G$ for all $\alpha \in \Omega$. Fix α and suppose the result holds for all $\beta < \alpha$. If $\alpha = 0$, the result holds since $H_0 = 1$ and $1 < G$ by hypothesis. If $\alpha = \beta^+$, then both possible cases in our recursion yield $H_\alpha < G$. Finally, if α is a limit ordinal, suppose towards a contradiction that

$$G = H_\alpha = \bigcup_{\beta<\alpha} H_\beta$$

Since G is finitely generated, we have $G = \langle g', \ldots, g_n \rangle$ for some $g', \ldots, g_n \in G$. Choose $\beta_1, \ldots, \beta_n < \alpha$ such that $g_i \in H_{\beta_i}$ for $1 \leq i \leq n$. Since these subgroups form a chain, we have $H = \bigcup H_{\beta_i} = H_{\beta_j}$ for some $1 \leq j \leq n$. Now $g', \ldots, g_n \in H$, so $G \leq H$—but this contradicts the supposition that $H < G$. Thus $H_\alpha < G$.

By induction then, our claim holds for all $\alpha \in \Omega$. In particular, H_δ is maximal in G, so G has a maximal subgroup as desired. □

Note that we present this direct proof instead of using Zorn's Lemma because it well illustrates both the principle behind Zorn's Lemma as well as the natural way in which the ordinals can be used to extend the counting process beyond the finite (cf. the proof of this result for a finite group G).

Exercise 19.

(a) $\mathbb{Q}$ is divisible. *Proof:* For $q \in \mathbb{Q}$ and $k \neq 0$ arbitrary, set $r = q/k$, so $r \cdot k = q$.

(b) No finite group is divisible.

Proof. Let G be an arbitrary nontrivial finite group. Write $G = \{g', \ldots, g_n\}$ and set $N = |g'| \cdots |g_n|$. Then $N > 0$, and for all $g \in G$, $g^N = 1$, so no nontrivial element of G has an N-th root. It follows that G is not divisible. □

Section 5

Exercise 3. Let $H = \langle s, r^2 \rangle$ in D_8. Then $H \cong V_4$.

Proof. Note $V_4 = \langle\, a, b \mid a^2 = 1 = b^2, ab = ba \,\rangle$ and $H = \langle\, s, r^2 \mid s^2 = 1 = (r^2)^2, sr^2 = r^2 s \,\rangle$. Hence there is a natural isomorphism from V_4 to H mapping $a \mapsto s$ and $b \mapsto r^2$. □

EXERCISE 6. We compute the centralizers of each element in the following groups G:

(a) Let $G = D_8 = \langle s, r \mid s^2 = 1 = r^4, sr = r^{-1}s\rangle = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$. Using the group lattice and some computations, we have

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

(c) Let $G = S_3 = \langle(12), (123)\rangle = \{1, (12), (13), (23), (123), (132)\}$. We have

$$C(1) = S_3$$
$$C((12)) = \langle(12)\rangle \quad C((13)) = \langle(13)\rangle \quad C((23)) = \langle(23)\rangle$$
$$C((123)) = C((132)) = \langle(123)\rangle$$

EXERCISE 8. We compute the normalizers of each element in the following groups G:

(a) Let $G = S_3$ as above. Then

$$N(1) = N(\langle 123\rangle) = N(S_3) = S_3$$
$$N(\langle(12)\rangle) = \langle(12)\rangle \quad N(\langle(13)\rangle) = \langle(13)\rangle \quad N(\langle(23)\rangle) = \langle(23)\rangle$$

EXERCISE 10 (GROUPS OF ORDER 4). If $|G| = 4$, then $G \cong Z_4$ or $G \cong V_4$.

Proof. Suppose $|G| = 4$ but $G \ncong Z_4$. Then by Theorem 2.3.4(1), G is noncyclic, and hence G contains no element of order 4. By Exercise 1.1.36 then, $G \cong V_4$. □

EXERCISE 15. The group D_{16} has three subgroups of order 8: $H_1 = \langle r\rangle$, $H_2 = \langle s, r^2\rangle$, and $H_3 = \langle sr, r^2\rangle$. Trivially $H_1 \cong Z_8$. By examining the subgroup lattice of D_{16}, it seems reasonable to guess that both H_2 and H_3 are isomorphic to D_8.

Indeed, note that $s^2 = 1 = (r^2)^4$, and $s(r^2) = (r^{-1})^2 s = (r^2)^{-1}s$, and these relations determine the structure of H_2, hence there is a natural isomorphism from D_8 to H_2.

Similarly, $(sr)^2 = 1 = (r^2)^4$ and $(sr)r^2 = (r^{-1})^2(sr) = (r^2)^{-1}(sr)$, so there is also a natural isomorphism from D_8 to H_3.

Chapter 3

Section 1

EXERCISE 1. Let $\varphi : G \to H$ be a homomorphism and let $E \leq H$. Then $\varphi^{-1}(E) \leq G$. If E is normal, so is $\varphi^{-1}(E)$.

Proof. Write $F = \varphi^{-1}(E)$. Note $1_G \in F$ since $1_H \in E$ and $\varphi(1_G) = 1_H$. Suppose $x, y \in F$ and write $x' = \varphi(x)$ and $y' = \varphi(y)$. By definition of F, $\{x', y'\} \subseteq E$. Now

$$\begin{aligned} \varphi(xy^{-1}) &= \varphi(x)\varphi(y^{-1}) \\ &= \varphi(x)\varphi(y)^{-1} \\ &= x'y'^{-1} \in E \end{aligned}$$

It follows that $F \leq G$.

Suppose now that $E \trianglelefteq H$. Let $g \in G$ be arbitrary and $x \in F$. Then

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in E$$

since $\varphi(x) \in E$ and E is normal. Thus $gxg^{-1} \in F$. Since g was arbitrary, $F \trianglelefteq G$. □

EXERCISE 3. Let A be an abelian group and $B \leq A$. Then A/B is abelian.

Proof. The natural projection $\pi : A \to A/B$ is a surjective homomorphism. □

Let $G = D_6$ and $N = \langle r \rangle$. Then G is non-abelian and $N \trianglelefteq G$. Since $|G/N| = 2$, G/N is cyclic and hence abelian.

EXERCISE 4. Let G be a group and $N \trianglelefteq G$. Then in G/N, $(gN)^\alpha = g^\alpha N$ for all $g \in G$ and $\alpha \in \mathbb{Z}$.

Proof. Fix $g \in G$ and $\alpha \in \mathbb{Z}$. Let $\pi : G \to G/N$ be the natural projection. Then

$$g^\alpha N = \varphi(g^\alpha) = \varphi(g)^\alpha = (gN)^\alpha$$

□

EXERCISE 7. Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi(x, y) = x + y$. Then π is a surjective homomorphism. The fibers of π are the lines $y = c - x$ for $c \in \mathbb{R}$. In particular, the kernel of π is the line $y = -x$.

Proof. Trivial. □

EXERCISE 14. Let $G = \mathbb{Q}/\mathbb{Z}$.

(a) Every coset in G contains exactly one representative $q \in \mathbb{Q}$ with $0 \le q < 1$.

Proof. Let $r + \mathbb{Z} \in G$ where $r \in \mathbb{Q}$, $r \ge 0$. Let $m \in \mathbb{Z}$ be largest such that $m \le r$ and set $q = r - m$. Then $0 \le q < 1$ and

$$\begin{aligned} r + \mathbb{Z} &= (q + m) + \mathbb{Z} \\ &= q + (m + \mathbb{Z}) \\ &= q + \mathbb{Z} \end{aligned}$$

Thus q is a desired representative for $r + \mathbb{Z}$.

Suppose $q + \mathbb{Z} = q' + \mathbb{Z}$ where $q, q' \in \mathbb{Q}$ and $0 \le q, q' < 1$. Then $q = q' + m$ for some $m \in \mathbb{Z}$, that is, $m = q - q'$. But we have $0 \le q - q' < 1$, hence $m = 0$ and $q = q'$. Thus the representative above is unique. □

(b) All elements in G have finite order, but there exist elements of arbitrarily large order.

Proof. Let $q + \mathbb{Z} \in G$ where $q = m/n$ with $m, n \in \mathbb{Z}$ and $n > 0$. Then

$$n \cdot (q + \mathbb{Z}) = nq + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}$$

Hence $|q + \mathbb{Z}| \le n$.

Note if $(m, n) = 1$, then $|q + \mathbb{Z}| = n$. Thus for $m = 1$, $|q + \mathbb{Z}| \to \infty$ as $n \to \infty$. □

(c) G is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$.

Proof. By (b), every element in $\mathbb{Q}/\mathbb{Z}$ has finite order. Suppose $\alpha + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ and $|\alpha + \mathbb{Z}| = n$. Then

$$n \cdot (\alpha + \mathbb{Z}) = n\alpha + \mathbb{Z} = \mathbb{Z}$$

In particular, $n\alpha = m$ for some $m \in \mathbb{Z}$, so $\alpha = m/n \in \mathbb{Q}$. Thus $\alpha + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. This establishes the claim. □

(d) G is isomorphic to the multiplicative group of roots of unity in $\mathbb{C}^\times$.

Proof. Define $\varphi : G \to \mathbb{C}^\times$ by

$$\varphi : \frac{m}{n} + \mathbb{Z} \mapsto e^{\frac{2m\pi i}{n}}$$

It is verified that this a well defined, injective, surjective homomorphism. □

EXERCISE 15. Let G be a divisible abelian group and $N < G$. Then G/N is divisible.

Proof. Since G is abelian, so is G/N, and since $N \neq G$, $G/N \neq 1$. Let $gN \in G/N$ be arbitrary and $k \in \mathbb{Z}$, $k \neq 0$. Since G is divisible, there exists $a \in G$ such that $a^k = g$. But then $(aN)^k = a^k N = gN$, hence gN has a k-th root in G/N. □

EXERCISE 16. Let $G = \langle S \rangle$ and $N \trianglelefteq G$. Then $\overline{G} = \langle \overline{S} \rangle$, where $\overline{S} = \{\overline{s} \mid s \in S\}$.

Proof. Let $\overline{g} \in \overline{G}$ be arbitrary. Then since $g \in \langle S \rangle$, there exist $s_1, \ldots, s_n \in S$ such that

$$g = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \quad (\varepsilon_i = \pm 1)$$

Therefore, since the natural projection from G to $\overline{G}$ is a homomorphism,

$$\begin{aligned} \overline{g} &= \overline{s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}} \\ &= \overline{s_1}^{\varepsilon_1} \cdots \overline{s_n}^{\varepsilon_n} \in \langle \overline{S} \rangle \end{aligned}$$

Since $\overline{g}$ was arbitrary, this shows $\overline{G} \leq \langle \overline{S} \rangle$ as desired. □

EXERCISE 22. Let G be a group and $\mathscr{B}$ be a nonempty set of normal subgroups of G. Then $\bigcap \mathscr{B} \trianglelefteq G$.

Proof. We know $\bigcap \mathscr{B} \leq G$. Suppose $x \in \bigcap \mathscr{B}$ and let $g \in G$ be arbitrary. Then for any $N \in \mathscr{B}$, $x \in N$, and hence $gxg^{-1} \in N$ since N is normal. Since N was arbitrary, $gxg^{-1} \in \bigcap \mathscr{B}$. Since g and x were arbitrary, $\bigcap \mathscr{B}$ is normal. □

EXERCISE 23. Let G be a group and $\mathscr{B}$ be a nonempty set of normal subgroups of G. Then $\langle \mathscr{B} \rangle \trianglelefteq G$. (Here $\langle \mathscr{B} \rangle$ denotes the join over $\mathscr{B}$, that is, the smallest subgroup of G which includes $\bigcup \mathscr{B}$.)

Proof. Suppose $x \in \langle \mathscr{B} \rangle$ and let $g \in G$ be arbitrary. Choose $N \in \mathscr{B}$ such that $x \in N$. Then $gxg^{-1} \in N$ since N is normal. But $N \subseteq \bigcup \mathscr{B} \subseteq \langle \mathscr{B} \rangle$, hence $gxg^{-1} \in \langle \mathscr{B} \rangle$. It follows that $\langle \mathscr{B} \rangle \trianglelefteq G$. □

EXERCISE 24. Let G be a group, $N \trianglelefteq G$ and $H \leq G$. Then $N \cap H \trianglelefteq H$.

Proof. We know $N \cap H \leq H$. If $x \in N \cap H$ and $h \in H$, then $hxh^{-1} \in N$ since N is normal in G, and $hxh^{-1} \in H$ since H is a subgroup, hence $hxh^{-1} \in N \cap H$. □

EXERCISE 25.

(a) Let G be a group and $N \leq G$. Then $N \trianglelefteq G$ iff $gNg^{-1} \subseteq N$ for all $g \in G$.

Proof. The forward direction is trivial. If $gNg^{-1} \subseteq N$ for all $g \in G$, then for all $g \in G$ we have

$$N = (gg^{-1})N(gg^{-1}) = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$$

Hence g normalizes N for all $g \in G$, so $N \trianglelefteq G$. □

(b) Let $G = GL_2(\mathbb{Q})$, and define the subgroup and element

$$N = \left\{ \begin{pmatrix} 1 & n \\ & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\} \qquad g = \begin{pmatrix} 2 & \\ & 1 \end{pmatrix}$$

Note that for all $n \in \mathbb{Z}$,

$$\begin{aligned} g \begin{pmatrix} 1 & n \\ & 1 \end{pmatrix} g^{-1} &= \begin{pmatrix} 2 & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \\ & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2n \\ & 1 \end{pmatrix} \in N \end{aligned}$$

Hence $gNg^{-1} \subseteq N$. But note that g does not normalize N, since not every element in N has an even integer in entry $(1,2)$.

EXERCISE 26.

(a),(b) Recall that conjugation is an automorphism.

(c) Let G be a group, $S \subseteq G$, and $N = \langle S \rangle$. Then $N \trianglelefteq G$ iff $gSg^{-1} \subseteq N$ for all $g \in G$.

Proof. The forward direction is trivial. Suppose $gSg^{-1} \subseteq N$ for all $g \in G$. Let $x \in N$ be arbitrary. Then there exist $s_1, \ldots, s_n \in S$ such that

$$x = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \quad (\varepsilon_i = \pm 1)$$

Since conjugation is a homomorphism, for any $g \in G$ we have

$$gxg^{-1} = (gs_1g^{-1})^{\varepsilon_1} \cdots (gs_ng^{-1})^{\varepsilon_n} \in N$$

Thus $gNg^{-1} \subseteq N$ for all $g \in G$, so $N \trianglelefteq G$. □

(d) It follows immediately that if $N = \langle x \rangle$ is cyclic in G, then N is normal iff for all $g \in G$, $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$.

(e) Let G be a group, $n \in \mathbb{Z}$, $n > 0$, and let N be the subgroup generated by all elements in G of order n. Then N is normal.

Proof. Since conjugation is an automorphism, the conjugate of any element of order n has order n. It follows from (c) that N is normal. □

EXERCISE 29. Let $G = \langle T \rangle$. Suppose $S \subseteq G$, $N = \langle S \rangle$, and N is finite. Then $N \trianglelefteq G$ iff $tSt^{-1} \subseteq N$ for all $t \in T$.

Proof. The forward direction is trivial. Suppose $tSt^{-1} \subseteq N$ for all $t \in T$. Since N is finite, $N_G(N) = \{g \in G \mid gSg^{-1} \subseteq N\}$ (Exercise 28). By hypothesis then, $T \subseteq N_G(N)$. Thus $N_G(N)$ is a subgroup of G containing T, so $G \subseteq N_G(N)$ and $N \trianglelefteq G$. □

EXERCISE 33. Write $D_8 = \langle\, r, s \mid r^4 = 1 = s^2, rs = sr^{-1} \,\rangle$. Using the lattice of subgroups for D_8 and doing some computations (using Exercise 29), we find that the normal subgroups of D_8 are 1, $\langle r^2 \rangle$, $\langle r \rangle$, $\langle s, r^2 \rangle$, $\langle rs, r^2 \rangle$, and D_8. The following isomorphisms are easily verified:

$$\begin{aligned} D_8/1 &\cong D_8 \\ D_8/\langle r^2 \rangle &\cong V_4 \quad (\text{or } D_4) \\ D_8/\langle r \rangle &\cong Z_2 \quad (\text{or } D_2) \\ D_8/\langle s, r^2 \rangle &\cong Z_2 \\ D_8/\langle rs, r^2 \rangle &\cong Z_2 \end{aligned}$$

EXERCISE 34. Write $D_{2n} = \langle\, r, s \mid r^n = 1 = s^2, rs = sr^{-1} \,\rangle$ and let k be a positive integer dividing n. Then $\langle r^k \rangle \trianglelefteq D_{2n}$ and $D_{2n}/\langle r^k \rangle \cong D_{2k}$.

Proof. Write $D_{2k} = \langle \rho, \sigma \mid \rho^k = 1 = \sigma^2, \rho\sigma = \sigma\rho^{-1} \rangle$. Define

$$\begin{aligned} \varphi : D_{2n} &\to D_{2k} \\ s^\alpha r^\beta &\mapsto \sigma^\alpha \rho^\beta \quad (\alpha, \beta \in \mathbb{Z}) \end{aligned}$$

Since ρ, σ satisfy in D_{2k} all of the relations satisfied by r, s in D_{2n} (note $\rho^n = (\rho^k)^{n/k} = 1^{n/k} = 1$), it follows that φ is a well defined map from D_{2n} to D_{2k}. It is easily seen that φ is a surjective homomorphism.

If $\sigma^\alpha \rho^\beta = 1$, then $2|\alpha$ and $k|\beta$, and conversely. Thus $\ker\varphi = \langle r^k \rangle$. It follows that $\langle r^k \rangle \trianglelefteq G$ and $G/\langle r^k \rangle \cong D_{2k}$. □

EXERCISE 36. If $G/Z(G)$ is cyclic, then G is abelian.

Proof. Write $Z = Z(G)$. Suppose G/Z is cyclic and fix $g \in G$ such that $G/Z = \langle gZ \rangle$. Then for all $x \in G$, there exists $\alpha \in \mathbb{Z}$ such that $x \in (gZ)^\alpha = g^\alpha Z$. In other words, for all $x \in G$ there exists $\alpha \in \mathbb{Z}$ and $z \in Z$ such that $x = g^\alpha z$.

Let $x, y \in G$ be arbitrary, and write $x = g^\alpha w$ and $y = g^\beta z$ where $\alpha, \beta \in \mathbb{Z}$ and $w, z \in Z$. Then we have

$$xy = (g^\alpha w)(g^\beta z) = g^\alpha g^\beta wz = g^\beta g^\alpha zw = (g^\beta z)(g^\alpha w) = yx$$

since w, z commute with all elements, and powers of g commute with each other. Since x, y were arbitrary, it follows that G is abelian. □

Another way to state this result is that $G/Z(G)$ cannot be nontrivially cyclic (since, when G is abelian, $Z(G) = G$ so $G/Z(G) \cong 1$).

EXERCISE 40. Let G be a group, $N \trianglelefteq G$, and write $\overline{G} = G/N$. For $x, y \in G$, $\overline{x}, \overline{y}$ commute in $\overline{G}$ iff $x^{-1}y^{-1}xy \in N$. (Note $x^{-1}y^{-1}xy$ is called the *commutator* of x and y.)

Proof.

$$\begin{aligned} \overline{x}\,\overline{y} = \overline{y}\,\overline{x} &\iff \overline{x}^{-1}\overline{y}^{-1}\overline{x}\,\overline{y} = \overline{1} \\ &\iff \overline{x^{-1}y^{-1}xy} = \overline{1} \\ &\iff x^{-1}y^{-1}xy \in N \end{aligned}$$

□

EXERCISE 41. Let G be a group and set $N = \langle x^{-1}y^{-1}xy \mid x, y \in G\rangle$. Then $N \trianglelefteq G$ and G/N is abelian. (Note N is called the *commutator subgroup* of G.)

Proof. For all $x, y, g \in G$,

$$\begin{aligned} g^{-1}(x^{-1}y^{-1}xy)g &= (g^{-1}x^{-1}g)(g^{-1}y^{-1}g)(g^{-1}xg)(g^{-1}yg) \\ &= (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) \in N \end{aligned}$$

It follows from Exercise 26(c) that $N \trianglelefteq G$. Since N contains all commutator elements in G, it follows from Exercise 40 that G/N is abelian. □

EXERCISE 43. Let G be a group and suppose $\mathscr{A} = \{A_i \mid i \in I\}$ is a partition of G which forms a group under the following operation: for $A_i, A_j \in \mathscr{A}$, the product A_iA_j is the element of $\mathscr{A}$ containing the product a_ia_j, for any $a_i \in A_i$ and $a_j \in A_j$.

Then the identity A in $\mathscr{A}$ is a normal subgroup of G, and $\mathscr{A} \cong G/A$.

Proof. Define $\pi : G \to \mathscr{A}$ by mapping $g \to A_i$ iff $g \in A_i$. Then π is a well defined, surjective homomorphism by the assumptions on $\mathscr{A}$. Also $\ker\pi$ just consists of the elements of A. Hence $A \trianglelefteq G$ and $G/A \cong \mathscr{A}$. □

This exercise shows that the quotient construction is in a certain sense ‘unique’. It is the only construction on a partition of a group whose operation may be induced by the operation of the group elements in the above manner.

Section 2

EXERCISE 2. We prove that the lattice of subgroups for S_3 in Section 2.5 is correct.

Proof. We first claim that the lattice is exhaustive. Indeed, if H is any subgroup of S_3, then by Lagrange’s Theorem we know the order of H is one of 1, 2, 3, or 6. Cases $|H| = 1$ and $|H| = 6$ are trivial. If $|H| = 2$, then H is cyclic and generated by one of the three elements of order 2, that is, H is one of

$$\langle(12)\rangle \qquad \langle(13)\rangle \qquad \langle(23)\rangle$$

Similarly if $|H| = 3$, then H must be cyclic and equal to $\langle(123)\rangle$. This shows that the lattice is exhaustive.

Clearly any two of the distinct subgroups of order 2 have trivial intersection. Also, by Lagrange's Theorem, each of these subgroups have trivial intersection with the subgroup of order 3 since $(2,3) = 1$. This shows that the intersections on the lattice are correct.

Finally, it is easily verified that any two distinct nontrivial subgroups join to all of S_3. Hence the joins on the lattice are correct. □

EXERCISE 4. Suppose $|G| = pq$, with p, q prime. Then $Z(G) = 1$ or G is abelian.

Proof. Let $H = G/Z(G)$ and suppose $Z(G) > 1$. If $Z(G) = G$, then trivially G is abelian. If $Z(G) \neq G$, then by Lagrange's Theorem, $|Z(G)|$ is either p or q, and thus the same is true of $|H|$. But then H is cyclic, so again G is abelian by Exercise 3.1.36. □

EXERCISE 6. Suppose $H \leq G$, $g \in G$, and the right coset Hg is equal to *some* left coset of H. Then $gH = Hg$.

Proof. Suppose $Hg = g'H$ for some $g' \in G$. Then gH and $g'H$ both contain g, hence $gH = g'H = Hg$. □

EXERCISE 8. Suppose H and K are finite subgroups of G whose orders are relatively prime. Then $H \cap K = 1$

Proof. By Lagrange's Theorem since $|H \cap K|$ must divide both $|H|$ and $|K|$. □

EXERCISE 9 (CAUCHY'S THEOREM). Let G be a finite group and suppose p is a prime dividing $|G|$. Then there exists an element in G of order p.

Proof. First define

$$\mathscr{P} = \{(x_1, \dots, x_p) \mid x_i \in G \wedge x_1 \cdots x_p = 1\}$$

(a) Note that $|\mathscr{P}| = |G|^{p-1}$ since, when constructing a tuple $(x_1, \dots, x_p)$, we have $|G|$ possible choices for each x_i where $1 \leq i \leq p-1$, but once those elements are chosen, we must choose $x_p = (x_1 \cdots x_{p-1})^{-1}$. Thus p divides $|\mathscr{P}|$.

Define a relation $\sim$ on $\mathscr{P}$ by letting $\alpha \sim \beta$ iff α is a cyclic permutation of β.

(b) Note $\mathscr{P}$ is closed under cyclic permutations. Indeed, if $(x_1, \dots, x_p) \in \mathscr{P}$, then $(x_1 \cdots x_{p-1})x_p = 1$, so $x_p(x_1 \cdots x_{p-1}) = 1$, so $(x_p, x_1, \dots, x_{p-1}) \in \mathscr{P}$. The general case now follows by induction.

(c) Note $\sim$ is reflexive since the identity permutation is cyclic; it is symmetric since the inverse of a cyclic permutation is also cyclic; and it is transitive since the composite of two cyclic permutations is also cyclic. Therefore $\sim$ forms an equivalence relation.

(d) We claim that an equivalence class contains a single element iff that element is of the form $(x, \dots, x)$, with $x^p = 1$. Indeed, if $x^p = 1$, then $(x, \dots, x)$ is in $\mathscr{P}$, and it is preserved under any cyclic permutation. Conversely, if $(x_1, \dots, x_p)$ is in $\mathscr{P}$ and is preserved under any cyclic permutation, then by applying powers of the permutation (of indices) $(1 \cdots p)$, it follows that $x_1 = \cdots = x_p$. So the tuple is of the desired form with $x = x_1$, and $x^p = 1$.

(e) We claim that each equivalence class has order 1 or p. To see this, let E be an arbitrary equivalence class and note that the set of cyclic permutations of elements of E forms a group H of order p under composition. Moreover, this group acts on E. Now fix a tuple $t \in E$ and consider the stabilizer S of t in H. By Lagrange's Theorem, since p is prime, either $S = 1$ or $S = H$. If $S = H$, then E has order 1. If $S = 1$, then distinct cyclic permutations give rise to distinct images of t. So H is in bijective correspondence with E, and E has order p.

It follows now that $|G|^{p-1} = k + pd$, where k is the number of 1-element classes and d is the number of p-element classes.

(f) Since p divides $|G|^{p-1}$, p divides $k + pd$, and so p divides k. We know $k > 0$ since $\{(1,\dots,1)\}$ is a 1-element equivalence class. But this means $k > 1$, so there must exist a nonidentity element $x \in G$ with $x^p = 1$, and $|x| = p$.

□

Note that this theorem is a generalization of Exercise 1.1.31, and the proof is in some ways a generalization of the proof used in that exercise.

EXERCISE 11. Suppose $H \leq K \leq G$. Then $|G:H| = |G:K||K:H|$.

Proof. If $|K:H| = \infty$, then there are infinitely many cosets of H in K, and hence in G, so $|G:H| = \infty$ and equality holds.

If $|G:K| = \infty$, then there are infinitely cosets of K in G. Note that for all $g \in G$, $gH \subseteq gK$, that is, each coset of K contains a G-coset of H. Since the cosets of K are pairwise disjoint, these G-cosets of H are pairwise distinct (and disjoint). Hence $|G:H| = \infty$ and equality holds in this case as well.

Suppose now that $|G:K|$ and $|K:H|$ are both finite. We claim that the number of G-cosets of H contained in each coset of K is equal to $|K:H|$. Indeed, let $g \in G$ be arbitrary and define the map

$$\pi : kH \mapsto gkH \quad (k \in K)$$

Note for all $k \in K$, $kH \subseteq K$, so $gkH \subseteq gK$. Thus π maps cosets of H in K to cosets of H contained in gK. This map is injective, since if $gkH = gk'H$, then $kH = k'H$. Also, if $g'H \subseteq gK$, then in particular $g' \in gK$, so $g' = gk^*$ for some $k^* \in K$ and $g'H = gk^*H = \pi(k^*H)$. Thus π witnesses a bijection between the set of K-cosets of H and the set of G-cosets of H contained in gK. Since g was arbitrary, this proves our claim.

It now follows that $|G:H|$ is finite, and indeed the above equality holds. □

Note if we write this equality as

$$|G:K| = \frac{|G:H|}{|K:H|}$$

this suggests that the quotient G/K might be isomorphic to the quotient $(G/H)/(K/H)$. Indeed, this is so (see the Third Isomorphism Theorem).

EXERCISE 15. Let $G = S_n$, fix $i \in \{1,\dots,n\}$, and let G_i be the stabilizer of i. Then $G_i \cong S_{n-1}$.

Proof. Define $\sigma = (i\,n)$. Then

$$G_i \cong \sigma G_i \sigma^{-1} = G_n \cong S_{n-1}$$

where the first isomorphism is obtained by conjugation and the second is obtained by restriction. □

EXERCISE 21. Neither $\mathbb{Q}$ nor $\mathbb{Q}/\mathbb{Z}$ have proper subgroups of finite index.

Proof. Recall that if G is divisible, then G cannot be finite (Exercise 2.4.19(b)). Also if G is divisible and H is a proper normal subgroup of G, then G/H is also divisible (Exercise 3.1.15). Thus a divisible group cannot have proper normal subgroups of finite index.

The result now follows from the fact that $\mathbb{Q}$ is abelian and divisible (Exercise 2.4.19(a)). □

EXERCISE 22 (EULER'S THEOREM). Fix n and let $a \in \mathbb{Z}$ be relatively prime to n. Then $a^{\varphi(n)} \equiv 1 \mod n$.

Proof. Consider $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Recall $\overline{a} \in G$ since $(a,n) = 1$, and $|G| = \varphi(n)$. Hence by Lagrange's Theorem, $|\overline{a}|$ divides $\varphi(n)$, so $\overline{a}^{\varphi(n)} = \overline{1}$—that is, $a^{\varphi(n)} \equiv 1 \mod n$. □

EXERCISE 23. We compute the last two digits of $3^{3^{100}}$ using Euler's Theorem. Note that this is equivalent to computing $3^{3^{100}} \mod 100$. By Euler's Theorem, note that $3^{\varphi(100)} \mod 100 = 1$, hence we need only compute $3^{3^{100} \mod \varphi(100)} \mod 100$.

Write $r = 3^{100} \mod \varphi(100)$. Note $\varphi(100) = \varphi(2^2 \cdot 5^2) = 2(1) \cdot 5(4) = 40$. Thus to compute r, we may use Euler's Theorem again to note $r = 3^{100 \mod \varphi(40)} \mod 40$. Now $\varphi(40) = \varphi(2^3 \cdot 5) = 2^2(1) \cdot 1(4) = 16$, and $100 \mod 16 = 4$. So $r = 3^4 \mod 40 = 1$.

Thus our answer is $3^1 \mod 100 = 3$–that is, the last two digits are 03.

Section 3

EXERCISE 2 (LATTICE THEOREM). Let G be a group and $N \trianglelefteq G$. For any $A \leq G$, let

$$\overline{A} = A/N = \{\, aN \mid a \in A\}$$

Then the map $A \mapsto \overline{A}$ forms a bijective correspondence between the set of subgroups of G containing N and the set of subgroups of $\overline{G} = G/N$. Moreover, this bijection preserves lattice structure: for $A, B \leq G$ with $N \leq A \cap B$,

(1) $A \leq B$ iff $\overline{A} \leq \overline{B}$

(2) if $A \leq B$ then $|B : A| = |\overline{B} : \overline{A}|$

(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$

(5) $A \trianglelefteq G$ iff $\overline{A} \trianglelefteq \overline{G}$

Proof. Let $\pi : G \to \overline{G}$ be the natural projection. Then for $N \leq A \leq G$,

$$\overline{A} = \pi[A] \leq \pi[G] = \overline{G}$$

Hence $\overline{A} \leq \overline{G}$, so the map is defined on the desired sets.

Fix $A, B \leq G$ with $N \leq A \cap B$. Note that if $aN = bN$ for any $a \in A$ and $b \in B$, then in particular $a \in B$ (since $N \leq B$) and $b \in A$ (since $N \leq A$). Hence if $\overline{A} = \overline{B}$, then $A = B$. In other words, the mapping above is injective.

Finally, the mapping is surjective. If $A^* \leq \overline{G}$ is arbitrary, set $A = \pi^{-1}[A^*]$. Then $A \leq G$, and $N \leq A$ since $N \in A^*$. Also $\overline{A} = A^*$ by definition of π^{-1}.

Properties (1) and (3)–(5) are immediate by direct computation with elements. To prove (2), suppose $N \leq A \leq B$ and define a map from the coset space B/A to the coset space $(B/N)/(A/N)$ as follows:

$$\begin{aligned} f : B/A &\to (B/N)/(A/N) \\ bA &\mapsto bN(A/N) \end{aligned}$$

By definition

$$bN(A/N) = \{(bN)(aN) \mid a \in A\} = \{baN \mid a \in A\}$$

Note f is well-defined. Indeed, if $bA = b'A$, then $b = b'a'$ for some $a' \in A$, hence $baN = b'(a'a)N$ for all $a \in A$, and so $bN(A/N) \subseteq b'N(A/N)$. The converse follows by symmetry.

Also f is injective. If $bN(A/N) = b'N(A/N)$, then $bN = b'aN \subseteq b'A$ for some $a \in A$. In particular $b \in bA \cap b'A$, hence $bA = b'A$.

Clearly f is surjective. Hence f is a bijection and $|B : A| = |\overline{B} : \overline{A}|$. □

EXERCISE 3. Suppose $H \trianglelefteq G$ and $|G : H| = p$ for some prime p. Then for all $K \leq G$, either $K \leq H$ or else $G = HK$ and $|K : K \cap H| = p$.

Proof. Let $K \leq G$ be arbitrary. Note $H \leq HK \leq G$, hence

$$p = |G : H| = |G : HK||HK : H|$$

Suppose $K \nleq H$. Then $|HK : H| > 1$, hence $|HK : H| = p$ and $|G : HK| = 1$ (since p is prime), and thus $G = HK$.

Now by the Diamond Isomorphism Theorem, $G/H \cong K/(K \cap H)$, so in particular $|K : K \cap H| = |G : H| = p$. □

EXERCISE 4. Let A and B be groups, $C \trianglelefteq A$ and $D \trianglelefteq B$. Then $C \times D \trianglelefteq A \times B$ and

$$(A \times B)/(C \times D) \cong (A/C) \times (B/D)$$

Proof. Define the mapping

$$\begin{aligned} \varphi : (A \times B) &\to (A/C) \times (B/D) \\ (a, b) &\mapsto (aC, bD) \end{aligned}$$

Then it is immediate that φ is a surjective homomorphism with $\ker\varphi = C \times D$. The desired result now follows from the First Isomorphism Theorem. □

EXERCISE 7. Suppose $G = MN$ where $M \trianglelefteq G$ and $N \trianglelefteq G$. Then

$$G/(M \cap N) \cong (G/M) \times (G/N)$$

Proof. Define the map

$$\begin{aligned} \varphi : G &\to (G/M) \times (G/N) \\ g &\mapsto (gM, gN) \end{aligned}$$

It is immediate that φ is a homomorphism with $\ker \varphi = M \cap N$.

We claim that φ is surjective. Indeed, since $G = MN = NM$, we have $G/M = N/M$ (coset space) and $G/N = M/N$ (coset space). Thus values

$$\varphi(mn) = \varphi(m)\varphi(n) = (M, mN)(nM, N) = (nM, mN)$$

exhaust $(G/M) \times (G/N)$ as m and n vary.

The desired result now follows from the First Isomorphism Theorem. □

Note that this result can be seen visually by looking at the (partial) subgroup lattice. The 'diamond' formed by $G/(M \cap N)$ is reobtained by taking the cross product of the 'lines' G/M and G/N.

EXERCISE 9 (RESTRICTING SYLOW p-SUBGROUPS). Let G be a group with $|G| = p^\alpha m$ where p does not divide m. Suppose P is a Sylow p-subgroup of G (that is, $|P| = p^\alpha$) and $N \trianglelefteq G$ with $|N| = p^\beta n$ where p does not divide n. Then $P \cap N$ is a Sylow p-subgroup of N (that is, $|P \cap N| = p^\beta$) and $|PN/N| = p^{\alpha-\beta}$.

Proof. Note that if $|P \cap N| = p^\beta$, then by the Diamond Isomorphism Theorem and Lagrange's Theorem, we have

$$|PN/N| = |P/(P \cap N)| = \frac{|P|}{|P \cap N|} = \frac{p^\alpha}{p^\beta} = p^{\alpha-\beta}$$

Hence it suffices to prove $|P \cap N| = p^\beta$.

Let $\kappa = |P \cap N|$. By Lagrange's Theorem, $\kappa | p^\alpha$ and $\kappa | p^\beta n$, hence $\kappa | p^\beta$. Now let $\lambda = |PN|$. Recall

$$\lambda = \frac{|P||N|}{|P \cap N|} = \frac{p^\alpha p^\beta n}{\kappa}$$

But $\lambda | p^\alpha m$ by Lagrange's Theorem. Since p cannot divide m, we must have $p^\beta | \kappa$. Hence $\kappa = p^\beta$ as desired. □

Section 4

EXERCISE 1. Let G be an abelian simple group. Then $G \cong Z_p$ for some prime p.

Proof. By definition $|G| > 1$. Fix $x \in G$, $x \neq 1$ and set $N = \langle x \rangle$. Since G is abelian, any subgroup is normal and so $1 < N \trianglelefteq G$. But this implies $N = G$ since G is simple, so G is cyclic. By Theorem 2.3.7, G cannot have infinite or finite composite order because it does not have any nontrivial proper subgroups. Therefore $G \cong Z_p$ for some prime p. □

EXERCISE 4. Let G be a finite abelian group and suppose $n > 0$ divides the order of G. Then G has a subgroup of order n.

Proof. If n is prime then the result follows from Cauchy's Theorem.

If n is composite, write $n = pm$ for a prime p and $m > 0$. By Cauchy's Theorem choose a subgroup N with $|N| = p$. Note that $N \trianglelefteq G$ since G is abelian. Set $\overline{G} = G/N$. By Lagrange's Theorem, $|\overline{G}| = |G|/p$, hence $|\overline{G}| < |G|$, and since n divides $|G|$, m must divide $|\overline{G}|$. By induction choose a subgroup $\overline{H} \leq \overline{G}$ with $|\overline{H}| = m$. Let $H = \pi^{-1}[\overline{H}]$ where $\pi : G \to \overline{G}$ denotes the natural projection. By the Lattice Isomorphism Theorem and Lagrange's Theorem, $N \leq H \leq G$ and

$$|H| = |N||H : N| = |N||\overline{H}| = pm = n$$

Therefore H is a subgroup of G of order n, as desired. □

EXERCISE 5. Let G be a solvable group. If $H \leq G$, then H is solvable. If $N \trianglelefteq G$, then G/N is solvable.

Proof. Let $1 = G_0 \trianglelefteq \cdots \trianglelefteq G_n = G$ be a chain of subgroups in G such that G_{i+1}/G_i is abelian for $0 \leq i < n$. Suppose $H \leq G$. Define $H_i = G_i \cap H$ for $0 \leq i \leq n$. Then trivially

$$1 = H_0 \trianglelefteq \cdots \trianglelefteq H_n = H$$

Let $0 \leq i < n$. We claim H_{i+1}/H_i is abelian. Indeed, let $A = H_{i+1}$ and $B = G_i$. Then $A \leq N_G(B)$ since $G_i \trianglelefteq G_{i+1}$, $A \cap B = H_i$, and $AB \leq G_{i+1}$. Therefore by the Diamond Isomorphism Theorem,

$$H_{i+1}/H_i = A/(A \cap B) \cong AB/B \leq G_{i+1}/G_i$$

Therefore H_{i+1}/H_i is abelian. Since i was arbitrary, H is solvable.

Now suppose $N \trianglelefteq G$. For $H \leq G$, set $\overline{H} = \pi[H]$, where $\pi : G \to G/N$ is the natural projection. Then by the Lattice Isomorphism Theorem, we have

$$\overline{1} = \overline{G_0} \trianglelefteq \cdots \trianglelefteq \overline{G_n} = \overline{G}$$

By the proof of the Third Isomorphism Theorem, for all $0 \leq i < n$, $\overline{G_{i+1}}/\overline{G_i} \cong G_{i+1}/G_i$ and hence is abelian. □

EXERCISE 6,7 (JORDAN-HÖLDER THEOREM PART I). Let G be a nontrivial finite group. Then G has a composition series.

Proof. If G has no nontrivial proper normal subgroups, then G is simple and $1 \trianglelefteq G$ is a composition series for G.

If not, choose $1 < N \triangleleft G$. Since $|N| < |G|$, by induction we may assume N has a composition series $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_j = N$. Set $\overline{G} = G/N$. Then $|\overline{G}| < |G|$, so again by induction we may assume $\overline{G}$ has a composition series $\overline{1} = \overline{G_0} \trianglelefteq \cdots \trianglelefteq \overline{G_k} = \overline{G}$.

Set $G_i = \pi^{-1}[\overline{G_i}]$ for $0 \leq i \leq k$, where $\pi : G \to \overline{G}$ is the natural projection. By the Lattice Isomorphism Theorem, we have $N = G_0 \trianglelefteq \cdots \trianglelefteq G_k = G$, and by the Third

Isomorphism Theorem, $G_{i+1}/G_i \cong \overline{G_{i+1}}/\overline{G_i}$, and hence is simple, for $0 \le i < k$. Thus we have a composition series for G given by

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_j = N = G_0 \trianglelefteq \cdots \trianglelefteq G_k = G$$

□

Note that this proof also shows that if $H \trianglelefteq G$, there exists a composition series for G containing H as a term. Indeed, if $H = 1$ or $H = G$, this is trivial. Otherwise, combine a composition series for H with the preimage of a composition series for G/H under the natural projection to obtain a composition series for G which includes H.

An analogous note also holds for solvable groups.

Section 5

NOTE.Every permutation in S_n can be written as a product of transpositions. To prove this, first claim that this holds for any m-cycle:

$$(a_1 \cdots a_m) = (a_1\, a_m) \cdots (a_1\, a_2)$$

Indeed, this follows by induction. For $m = 1$ the result is trivial. If the result holds for fixed $m \ge 1$, note that

$$\begin{aligned} (a_1 \cdots a_{m+1}) &= (a_1\, a_{m+1})(a_1 \cdots a_m) && \text{by direct verification} \\ &= (a_1\, a_{m+1})[(a_1\, a_m) \cdots (a_1\, a_2)] && \text{by induction} \\ &= (a_1\, a_{m+1}) \cdots (a_1\, a_2) \end{aligned}$$

Thus the result holds for $m+1$. By induction the result holds for all m.

Now for any $\sigma \in S_n$, σ may be written as a product of cycles (cycle decomposition algorithm). Since each of these cycles may be written as a product of transpositions by the above, the result holds for σ.

EXERCISE 3. $S_n = \langle (i\, i+1) \mid 1 \le i < n \rangle$

Proof. Let S denote the set on the right. Claim that for any $1 \le i < j \le n$, $(i\, j) \in S$. Indeed, this follows by induction on j. For $j = 1$ the result is trivial. If the result holds for $j < n$, note that $(i\, j+1) = (i\, j)(j\, j+1)(i\, j) \in S$.

Since any element of S_n is a product of transpositions, the result follows. □

EXERCISE 4. $S_n = \langle (12), (1 \cdots n) \rangle$ for $n \ge 2$.

Proof. Let S denote the set on the right. By assumption $(12) \in S$. Suppose $1 < i < n$. Set $\rho = (1 \cdots n)^{i-1}$. Then $(i\, i+1) = \rho(12)\rho^{-1} \in S$.

The result now follows from Exercise 3. □

EXERCISE 7. The group of rigid motions (rotations) of a regular tetrahedron in 3-space is isomorphic to A_4.

Proof. Let G be the group of rigid motions. By letting G act on numbered faces of the tetrahedron, we obtain a permutation representation $\varphi : G \to S_4$. Note $|\varphi[G]| \leq 12$ since any rigid motion must take face 1 to one of four possible faces, and at any one of these must put it in one of three possible positions. And $|\varphi[G]| \geq 12$ since each one of these configurations is distinct and is realized by a rigid motion in G. Hence we must have $|\varphi[G]| = 12$.

We claim that $\varphi[G] \subseteq A_4$. First note that G is generated by two rotations ρ_1 and ρ_2 through $2\pi/3$ radians about axes passing through any two distinct vertices and the centers of their respective opposing faces. Therefore since φ is a homomorphism, it suffices to observe that $\varphi(\rho_1)$ and $\varphi(\rho_2)$ can be written as even permutations.

Since $\varphi[G] \subseteq A_4$ and $|\varphi[G]| = 12 = |A_4|$, $\varphi[G] = A_4$ and so $\varphi : G \cong A_4$. □

NOTE.Recall that groups of rigid motions of 2-dimensional regular n-gons in 3-space are not in general isomorphic to subgroups of A_n (e.g. $D_6 \cong S_3$). Intuitively it makes sense that the groups of rigid motions of a 3-dimensional object in 3-space (acting on a set of n elements) might be, since it does not contain reflections.

EXERCISE 8,9,14. The lattice of subgroups for A_4 in Figure 8 is correct.

Proof. We first prove exhaustiveness. Note $|A_4| = 12 = 2 \cdot 2 \cdot 3$, hence by Lagrange's Theorem the only possible subgroup orders are $1, 2, 3, 4, 6, 12$. Orders 1 and 12 are trivial. There are no subgroups of order 6 by Exercise 7 and the remarks on p. 92.

If a subgroup has order 2, it must be cyclic and generated by one of the even permutations in S_4 of order 2: $(12)(34)$, $(13)(24)$, or $(14)(23)$. Similarly if a subgroup has order 3, then it must be cyclic and generated by one of these (even) 3-cycles in S_4: (123), (124), (134), or (234). If a subgroup has order 4, it cannot contain an element of order 4 (since a 4-cycle is odd). Hence it must contain, and be generated by, at least two distinct even permutations of order 2. However, it is easily checked that any of the two distinct even permutations above generate the same subgroup. Hence there is just one subgroup of order 4, namely $\langle (12)(34), (13)(24) \rangle$. This establishes exhaustiveness of the lattice.

We now establish (nontrivial) intersections. Clearly any two distinct subgroups of order 2 have trivial intersection, and similarly for the subgroups of order 3. By Lagrange's Theorem, the intersection of a subgroup of order 2 or 4 with a subgroup of order 3 is trivial since $(2,3) = (4,3) = 1$. Finally, the intersection of the subgroup of order 4 with any subgroup of order 2 follows from the inclusions noted above.

The joins are established similarly. Hence the lattice is correct. □

Note that the subgroup of order 4 is isomorphic to V_4 since it has no element of order 4. Also it must be normal since it is the only subgroup of order 4. It is thus immediate that

$$1 \trianglelefteq \langle (12)(34) \rangle \trianglelefteq \langle (12)(34), (13)(24) \rangle \trianglelefteq A_4$$

By the lattice, the factors in this chain are cyclic of orders 2 or 3, and hence are abelian simple. It follows that this is a composition series for A_4 and moreover that A_4 is solvable.

Chapter 4

Section 1

NOTE.If G acts on A and $a \in A$, then by Lagrange's Theorem and Proposition 2,

$$|G| = |G : G_a||G_a| = |O_a||G_a|$$

where O_a is the orbit of a under G, and G_a is the stabilizer of a in G. This result is sometimes called the *Orbit-Stabilizer Theorem*.

EXERCISE 1. Let G act on A and suppose $b = g \cdot a$ for some $a, b \in A$ and $g \in G$. Then $G_b = gG_ag^{-1}$. If G is transitive on A, then the kernel of the action is $\bigcap_{g\in G} gG_ag^{-1}$

Proof. If $x \in G_a$, then for $g \in G$,

$$(gxg^{-1})(b) = (gx)(g^{-1}(b)) = (gx)(a) = g(xa) = g(a) = b$$

hence $gxg^{-1} \in G_b$. Thus $gG_ag^{-1} \subseteq G_b$.

Conversely, if $x \in G_b$, then by the above (with g^{-1}), $g^{-1}xg \in G_a$, hence

$$x = g(g^{-1}xg)g^{-1} \in gG_ag^{-1}$$

Therefore $G_b = gG_ag^{-1}$ as desired. The second claim is then immediate since the kernel of the action is just the intersection of the stabilizers. □

EXERCISE 3. Let G be an abelian, transitive subgroup of S_A. Then for all $\sigma \in G - 1$, $\sigma(a) \neq a$ for all $a \in A$.

Proof. If $a \in A$, then $gG_ag^{-1} = G_a$ for all $g \in G$ since G is abelian. By Exercise 1 then, $g(a) = a$ implies that g is in the kernel of the action, that is, $g = 1$. □

EXERCISE 7. Let G be a transitive permutation group on A. Call $B \subseteq A$ a *block* iff B is nonempty and for all $\sigma \in G$, $\sigma[B] = B$ or $\sigma[B] \cap B = \emptyset$ (where $\sigma[B] = \{\sigma(b) \mid b \in B\}$). Call G *primitive* on A iff the only blocks in A are the trivial ones (the singletons, and the entire set).

(a) If B is a block and $b \in B$, then $G_b \leq G_B \leq G$, where $G_B = \{\sigma \in G \mid \sigma[B] = B\}$.

Proof. Clearly $1 \in G_B$, and if $\sigma, \tau \in G_B$, then $\tau^{-1}[B] = B$, hence $(\sigma\tau^{-1})[B] = \sigma[\tau^{-1}[B]] = \sigma[B] = B$. Thus $G_B \leq G$. If $\sigma \in G_b$, then $b = \sigma(b) \in B \cap \sigma[B]$, hence $\sigma[B] = B$ (since B is a block) and $\sigma \in G_B$. Thus $G_b \leq G_B$. □

(b) If B is a block, then the set $\mathscr{B} = \{\sigma[B] \mid \sigma \in G\}$ partitions A.

Proof. Each set in $\mathscr{B}$ is nonempty since B is nonempty. Fix $b \in B$. Since G is transitive, for any $a \in A$ there exists $\sigma \in G$ such that $a = \sigma(b) \in \sigma[B]$. Hence $A = \bigcup \mathscr{B}$. We claim that $\sigma[B] \neq \tau[B]$ implies $\sigma[B] \cap \tau[B] = \emptyset$. Indeed, suppose $a \in \sigma[B] \cap \tau[B]$, so $a = \sigma(b) = \tau(b')$ for some $b, b' \in B$. Then

$$b' = \tau^{-1}(a) = \tau^{-1}(\sigma(b)) = (\tau^{-1}\sigma)(b) \in (\tau^{-1}\sigma)[B]$$

Thus $b' \in B \cap (\tau^{-1}\sigma)[B]$, so $B = (\tau^{-1}\sigma)[B]$ and $\tau[B] = \sigma[B]$. □

(c) S_4 is primitive on $A = \{1,2,3,4\}$, but D_8 is not primitive on the vertices of the square.

Proof. Suppose $X \subseteq A$ is nontrivial (in the above sense). Choose $x \in X$ and $y \in A - X$. Let $\sigma = (xy) \in S_4$. Then $\sigma[X] \neq X$ but $\sigma[X] \cap X$ is nonempty. Thus X is not a block. Since X was arbitrary, S_4 is not primitive.

On the contrary, if we let A label the vertices of the square in clockwise order, then the pair $X = \{1,3\}$ of diagonally opposing vertices is a block under D_8. □

(d) G is primitive iff G_a is maximal for all $a \in A$.

Proof. If G is not primitive, there exists a nontrivial block B in A. Fix $b, b' \in B$ with $b \neq b'$ and $a \in A - B$. We know $G_b \leq G_B \leq G$. Since G is transitive, there exists $\sigma \in G$ with $\sigma(b) = b'$. Note $\sigma \in G_B - G_b$, hence $G_b < G_B$. Similarly there exists $\tau \in G$ with $\tau(b) = a$, so $\tau \notin G_B$ and $G_B < G$. It follows that G_b is not maximal.

If G_a is not maximal, then there exists $G_a < H < G$. Let B be the orbit of a under H. Since $G_a < H$, B contains elements other than a. Fix $\sigma \in G - H$. If $\sigma(a) = \tau(a)$ for some $\tau \in H$, then $\tau^{-1}\sigma \in G_a \subseteq H$, so $\sigma \in H$, contradicting the choice of σ. Hence $\sigma(a) \in A - B$ and $B \neq A$. We claim that B is a block. Indeed, suppose $\sigma[B] \cap B$ is nonempty, so there exist $b, b' \in B$ with $b' = \sigma(b)$. Choose $\tau, \tau' \in H$ with $b = \tau(a)$ and $b' = \tau'(a)$. Then $\tau'(a) = \sigma(\tau(a)) = (\sigma\tau)(a)$, so $\tau'^{-1}(\sigma\tau) = \tau'^{-1}\sigma\tau \in G_a \subseteq H$. But this implies that $\sigma \in H$ and $\sigma[B] = B$. It follows that B is a block as claimed. Since B is nontrivial, it follows that G is not primitive. □

Informally, a block may be thought of as a set of related elements which always 'move together' as a unit under the action of a group. Hence the elements of a block may be 'identified' to induce a natural action of the group on the blocks themselves. In general, stabilizers under the induced action will be larger than corresponding stabilizers under the original action because the stabilizer of a block includes the stabilizers of the individual elements in the block *as well as* any permutations which permute the elements of the block amongst each other. Also, by the Orbit-Stabilizer Theorem above, this means orbits generally get smaller.

EXERCISE 9 (ORBIT-STABILIZER). Let G act transitively on the finite set A and $H \trianglelefteq G$. Let $O_1, \ldots, O_r$ denote the distinct orbits of H on A.

(a) G acts transitively on the orbits where $g \cdot O_i = \{g \cdot a \mid a \in O_i\}$, and all the orbits have the same cardinality.

Proof. Write $O_i = \{h \cdot a \mid h \in H\}$. Then

$$\begin{aligned} g \cdot O_i &= \{g \cdot (h \cdot a) \mid h \in H\} \\ &= \{gh \cdot a \mid h \in H\} \\ &= \{hg \cdot a \mid h \in H\} && \text{since } gH = Hg \\ &= \{h \cdot (g \cdot a) \mid h \in H\} = O_j \end{aligned}$$

where O_j is the orbit of $g \cdot a$ under H. It follows that G acts transitively on the orbits since G acts transitively on A.

Since g is a permutation of A, all the orbits have the same cardinality. □

(b) Suppose $a \in O_1$. Then $|O_1| = |H : H \cap G_a|$ and $r = |G : HG_a|$.

Proof. The first claim follows from the Orbit-Stabilizer Theorem (Proposition 2) since $H_a = H \cap G_a$. The second claim follows similarly by noting that HG_a is precisely the stabilizer of O_1 in the action of G on the orbits. □

Section 2

EXERCISE 8. Suppose $H \leq G$ and $|G : H| = n$. Then there exists $K \leq H$ with $K \trianglelefteq G$ and $|G : K| \leq n!$.

Proof. Let G act on the coset space $A = G/H$, let $\pi : G \to S_A$ be the permutation representation and set $K = \ker \pi$. Then $K \leq H$, $K \trianglelefteq G$, and by the First Isomorphism Theorem,

$$|G : K| = |G/K| = |\varphi[G]| \leq |S_A| = n!$$

□

EXERCISE 10 (GROUPS OF ORDER 6). If $|G| = 6$, then $G \cong Z_6$ or $G \cong S_3 (\cong D_6)$.

Proof. Since $|G| = 3 \cdot 2$, by Cauchy's Theorem there exist elements $r, s \in G$ with $|r| = 3$ and $|s| = 2$. Set $H = \langle rs \rangle$. If G is abelian, then H contains the distinct elements 1, $r = (rs)^4$, $s = (rs)^3$, and rs. By Lagrange's Theorem then, $|H| = 6$, so $H = G$, which means G is cyclic and $G \cong Z_6$.

If G is not abelian, set $K = \langle s \rangle$ and let G act on the coset space G/K. Note that this gives a permutation representation into S_3 since by Lagrange's Theorem $|G/K| = 3$. We claim that this representation is faithful. Indeed, note G/K is given by

$$\langle s \rangle = \{1, s\} \qquad r\langle s \rangle = \{r, rs\} \qquad r^2\langle s \rangle = \{r^2, r^2 s\}$$

If g is in the kernel of the action, then in particular g must stabilize $\langle s \rangle$, so $g = 1$ or $g = s$. But s does not stabilize $r\langle s \rangle$ since $sr \neq r$ ($s \neq 1$) and $sr \neq rs$ (G is not cyclic). So we must have $g = 1$. Therefore the kernel of the action is trivial, and $G \cong S_3$. □

EXERCISE 11. Let G be a finite group and $\pi_G : G \to S_G$ denote the left regular action of G. If $x \in G$ with $|x| = n$ and $|G| = mn$, then $\pi(x)$ is a product of m n-cycles. Hence $\pi(x)$ is an odd permutation iff $|x|$ is even and $|G|/|x|$ is odd.

Proof. Set $X = \langle x \rangle$. Then $|G : X| = m$, hence there exist elements $g_1, \cdots, g_m \in G$ with $g_1 = 1$ such that the n-element right cosets $X, Xg_2, \cdots, Xg_m$ partition G. But these are just the orbits under the left action of X on G. In particular, we may write

$$\pi(x) = (1\, x \cdots x^{n-1})(g_2\, xg_2 \cdots x^{n-1}g_2) \cdots (g_m\, xg_m \cdots x^{n-1}g_m)$$

which is a product of m n-cycles as claimed.

Recall an n-cycle is even iff n is odd. Hence $\pi(x)$ is even iff n is odd or else m is even, or equivalently $\pi(x)$ is odd iff n is even and m is odd. This completes the proof. □

EXERCISE 12. Let G be a finite group and $\pi : G \to S_G$ be the left regular action. If $\pi[G]$ contains an odd permutation, then G has a subgroup of index 2.

Proof. Recall $|S_G : A_G| = 2$. Since $\pi[G]$ contains an odd permutation, $\pi[G] \not\leq A_G$. Hence $S_G = \pi[G]A_G$ and by the Diamond Isomorphism Theorem,

$$|\pi[G] : \pi[G] \cap A_G| = |S_G : A_G| = 2$$

(See Exercise 3.3.3.) Therefore $\pi^{-1}[\pi[G] \cap A_G]$ has index 2 in G. □

EXERCISE 13. Let G be a group with $|G| = 2k$ where k is odd. Then G has a subgroup of index 2.

Proof. Since G has even order, there exists $x \in G$ of order 2. But then by Exercise 11, $\pi_G(x)$ is an odd permutation (where π_G denotes the left regular representation of G). Hence G has a subgroup of index 2 by Exercise 12. □

Note that the previous three exercises illustrate a recurring use of group actions: pulling information about elements and subgroups of S_n back into arbitrary groups. In this case we have used information about the existence of A_n in S_n to obtain information about more general groups.

EXERCISE 14. Let $|G| = n$ with n composite. Suppose for each positive $k|n$ there exists a subgroup of G of order k. Then G is not simple.

Proof. Note $n > 1$. Let p be the smallest prime dividing n and write $k = n/p$. Then $1 < k < n$. By assumption there exists a subgroup K with $|K| = k$, and $1 < K < G$. By Lagrange's Theorem, $|G : K| = p$, so $K \trianglelefteq G$ by Corollary 5. It follows that G is not simple. □

Section 3

EXERCISE 2. We find conjugacy class decompositions.

(a) Let $G = D_8 = \langle r, s \mid s^2 = 1 = r^4, sr = r^{-1}s\rangle$. We know that $Z(D_8) = \langle r^2\rangle$, hence two conjugacy classes are $\{1\}$ and $\{r^2\}$. Now $\langle r\rangle \leq C(r)$, but $C(r) \neq D_8$ since $s \notin C(r)$ $(srs = r^3)$, so $C(r) = \langle r\rangle$. Since $|\langle r\rangle| = 4$, by Lagrange's Theorem we have $|G : \langle r\rangle| = 2$, so by the Orbit-Stabilizer Theorem the conjugacy class of r consists of the two elements $\{r, r^3\}$. It is similarly verified that $C(s) = \langle s, r^2\rangle$, so the conjugacy class of s contains the two elements $\{s, sr^2\}$, and $C(sr) = \langle rs, s^2\rangle$, so the conjugacy class of sr contains the two elements $\{sr, sr^3\}$. This gives a complete partition. The class equation for D_8 is $8 = 1 + 1 + 2 + 2 + 2$.

(b) Let $G = A_4$. Trivially $Z(A_4) = 1$. Using the lattice and the fact that groups of order 4 are abelian, it is easily checked that $C((12)(34)) = \langle (12)(34), (13)(24)\rangle$. Thus, as above, the conjugacy class of $(12)(34)$ consists of 3 elements. Since conjugates must have the same cycle shape, the only possible conjugates are $(12)(34)$, $(13)(24)$, and $(14)(23)$. Hence these are exhaustive.

Similarly $C((123)) = \langle (123)\rangle$, hence the conjugacy class containing (123) has 4 elements. These must be 3-cycles. It is checked by direct computation that these are (123), (142), (134), and (243). This leaves the elements (132), (124), (143), and (234) in the remaining conjugacy class.

Thus the class equation for A_4 is $12 = 1 + 3 + 4 + 4$.

NOTE.For the following exercise we first observe the following result: If A and B are groups, then the conjugacy classes in $A \times B$ are precisely the direct products of the conjugacy classes of A with the conjugacy classes of B.

Proof. Trivial since multiplication in $A \times B$ is coordinate-wise. □

EXERCISE 3. We find conjugacy class decompositions.

(a) Let $G = Z_2 \times S_3$. Write $Z_2 = \{\pm 1\}$. Then the conjugacy classes of Z_2 are $\{1\}$ and $\{-1\}$. The conjugacy classes in S_3 are $\{1\}$, $\{(12), (13), (23)\}$, and $\{(123), (132)\}$. Hence by the above note, the conjugacy classes in G are

$$\begin{array}{ccc} \{1\} \times \{1\} & \{1\} \times \{(12), (13), (23)\} & \{1\} \times \{(123), (132)\} \\ \{-1\} \times \{1\} & \{-1\} \times \{(12), (13), (23)\} & \{-1\} \times \{(123), (132)\} \end{array}$$

(b) Let $G = S_3 \times S_3$. The conjugacy classes in G are just the direct products of the conjugacy classes in S_3 with each other.

(c) Let $G = Z_3 \times A_4$. The conjugacy classes in G are just the direct products of the conjugacy classes in Z_3 ($\{1\}$, $\{x\}$, and $\{x^2\}$) with the conjugacy classes in A_4.

EXERCISE 5. Let G be finite and suppose $|G : Z(G)| = n$. Then every conjugacy class in G has at most n elements.

Proof. Let $g \in G$. Note that $Z(G) \le C_G(g) \le G$, hence

$$n = |G : Z(G)| = |G : C_G(g)||C_G(g) : Z(G)| \ge |G : C_G(g)|$$

Therefore by the Orbit-Stabilizer Theorem, the conjugacy class containing g has at most n elements. Since g was arbitrary this establishes the claim. □

EXERCISE 6. Let G be a nonabelian group of order 15. Then there is only one possible class equation for G.

Proof. We must have $Z(G) = 1$, since otherwise $G/Z(G)$ is of prime order and hence cyclic, contradicting that G is nonabelian. Thus there is only the trivial singleton conjugacy class. The other conjugacy classes must have orders 3 or 5. It is easy to check that the only possibility is $15 = 1+3+3+3+5$. □

EXERCISE 13. Let G be a finite group with two conjugacy classes. Then $G \cong Z_2$.

Proof. Let $n = |G|$. Then we must have $n = 1+k$ where k is the order of the nontrivial conjugacy class. But $k|n$ by the Orbit-Stabilizer Theorem. Hence there exists m with $mk = n = k+1$. Now $m \ge 1$, but since $k \ge 1$, $m \ne 1$. Also $2k > 1$, so $3k > k+1$, and hence we have $m < 3$. This leaves $m = 2$, in which case $k = 1$, $n = 2$, and $G \cong Z_2$. □

EXERCISE 17. Let A be a nonempty set and $X \subseteq S_A$. Then

$$F(X) = \{a \in A \mid (\forall \sigma \in X)(\sigma(a) = a)\}$$

is called the *fixed set* of X and $M(X) = A - F(X)$ is called the *moved set* of X.

Set $D = \{\sigma \in S_A \mid M(\sigma) < \infty\}$. Then $D \trianglelefteq S_A$.

Proof. Trivially $1 \in D$. Suppose $\sigma, \tau \in D$, so that $M(\sigma)$ and $M(\tau)$ are finite. Note that $M(\tau^{-1}) = \tau[M(\tau)] = M(\tau)$, and $M(\sigma\tau^{-1}) \subseteq M(\sigma) \cup M(\tau^{-1})$, hence $M(\sigma\tau^{-1})$ is finite and $\sigma\tau^{-1} \in D$. This shows that $D \le S_A$.

Suppose now $\sigma \in D$ and $\tau \in S_A$. Note that $M(\tau\sigma\tau^{-1}) = \tau[M(\sigma)]$, hence

$$|M(\tau\sigma\tau^{-1})| = |\tau[M(\sigma)]| = |M(\sigma)| < \infty$$

since τ is a permutation. Thus $\tau\sigma\tau^{-1} \in D$. Since σ, τ were arbitrary, $D \trianglelefteq S_A$. □

EXERCISE 18. Let A be a nonempty set, $H \le S_A$, and $F(H)$ the fixed set of H. Then $N_{S_A}(H)$ stabilizes $F(H)$ and its complement $M(H)$.

Proof. Suppose $\tau \in N(H)$. We claim that $\tau[F(H)] = F(H)$. Note that $\tau H = H\tau$, hence if $a \in F(H)$ and $\sigma \in H$, there exists $\sigma' \in H$ such that

$$\sigma(\tau(a)) = (\sigma\tau)(a) = (\tau\sigma')(a) = \tau(\sigma'(a)) = \tau(a)$$

Thus $\tau(a) \in F(H)$. Since a was arbitrary, $\tau[F(H)] \subseteq F(H)$.

By symmetry, $\tau^{-1}[F(H)] \subseteq F(H)$, so $F(H) \subseteq \tau[F(H)]$, and hence $\tau[F(H)] = F(H)$ as claimed. Since τ is a bijection, it follows that $\tau[M(H)] = M(H)$ as well. □

EXERCISE 19. Let G be a group, $H \trianglelefteq G$, and K be a conjugacy class of G such that $K \subseteq H$. Then K is a union of k conjugacy classes of equal size in H, where for any $x \in K$, $k = |G : HC_G(x)|$.

Proof. This follows from the proof of Exercise 1.9. Note that under conjugation, G acts transitively on K, hence K is partitioned into H-orbits of equal cardinality. Now G acts transitively on the set of H-orbits. Hence k is just the size of the one orbit under this action. The stabilizer of this action is precisely $HC_G(x)$, hence by the Orbit-Stabilizer Theorem we have $k = |G : HC_G(x)|$ as desired. □

Recall $A_n \trianglelefteq S_n$ and $|S_n| = 2\cdot|A_n|$ (hence A_n is maximal for $n \geq 2$). It follows from this result that any conjugacy class in S_n which is contained in A_n consists either of one conjugacy class in A_n or else two conjugacy classes in A_n of equal size.

EXERCISE 22. Suppose $n \geq 3$ is odd. Then the set of all n-cycles forms two conjugacy classes of equal size in A_n.

Proof. Since n is odd, the n-cycles are even and hence are contained in A_n. Define $\sigma = (123\cdots n)$, $\tau = (12)$, and $\sigma^* = \tau\sigma\tau^{-1} = (213\cdots n)$. We claim that σ and σ^* are not conjugate in A_n. Indeed, if $\rho \in S_n$ and $\rho\sigma\rho^{-1} = \sigma^*$, then by Proposition 10 and the fact that the only alternate representations of the cycle for σ^* are obtained by cyclically permuting its elements, we must have $\rho = (\sigma^*)^k\tau$ for some k, which is an odd permutation. Hence there is not one conjugacy class of n-cycles in A_n, and the desired result follows from Exercise 19. □

EXERCISE 25. Let $G = GL_2(\mathbb{C})$ and let H be the subgroup of upper triangular matrices in G. Then every element in G is conjugate to some element in H.

Proof. Let A be a matrix in G and let T be the corresponding linear transformation under the standard basis. We know T has an eigenvalue because its characteristic polynomial must have a complex root. By changing to a basis whose first element is an eigenvector of T, we obtain an upper triangular matrix representation A^* for T. But A^* is obtained by conjugating A, hence A is a conjugate of A^*. Since A was arbitrary, this completes the proof. □

EXERCISE 29. Let G be a group of order p^α. Then G has a subgroup of order p^β for all $0 \leq \beta \leq \alpha$.

Proof. We proceed by induction on α. For $\alpha = 0$ and $\alpha = 1$ the result is trivial.

Suppose $\alpha > 1$ and the result holds for all groups of order p^γ with $\gamma < \alpha$. By Theorem 8, $Z(G) \neq 1$, hence $|Z(G)| = p^\delta$ for $0 < \delta \leq \alpha$. Since $Z(G)$ is normal, we may define $\overline{G} = G/Z(G)$. Then $|\overline{G}| = p^{\alpha-\delta}$ by Lagrange's Theorem and $\alpha - \delta < \alpha$, so by the induction hypothesis we may assume the result holds for $\overline{G}$.

Now let $0 \leq \beta \leq \alpha$ be arbitrary. If $\beta \leq \delta$, then $p^\beta | p^\delta$, hence by Exercise 4.4 in Chapter 3 there exists a subgroup of $Z(G)$ of order p^β. If $\beta > \delta$, then $\rho = \beta - \delta$ satisfies $0 < \rho \leq \alpha - \delta$, so there exists a subgroup $\overline{H}$ of $\overline{G}$ with $|\overline{H}| = p^\rho$. But we know by the Lattice Theorem that $\overline{H} = H/Z$ for some subgroup $Z \trianglelefteq H \leq G$, and hence

$$|H| = |\overline{H}||Z| = p^\rho p^\delta = p^{\beta-\delta} p^\delta = p^\beta$$

Thus in either case there exists a subgroup of G of order p^β, as desired. □

EXERCISE 30. Let G be a group of odd order. Then for all nonidentity elements $x \in G$, x is not conjugate to x^{-1}.

Proof. Suppose $x \in G$, $x \neq 1$ and x is conjugate to x^{-1}. We cannot have $x = x^{-1}$, lest $x^2 = 1$ so x has order 2 and 2 divides $|G|$ by Lagrange's Theorem—contradicting that $|G|$ is odd. We claim that x has an even number of conjugates. Indeed, each element axa^{-1} in the conjugacy class of x can be paired off with its distinct inverse element $(axa^{-1})^{-1} = ax^{-1}a^{-1}$, which is also in the conjugacy class of x. But then by the Orbit-Stabilizer Theorem, the order of the conjugacy class divides the order of G, so 2 divides $|G|$—again a contradiction. It follows that our initial assumption cannot be correct, so there is no nonidentity element conjugate to its inverse. □

EXERCISE 33. Let $\sigma \in S_n$, let $m_1, \dots, m_s$ be the distinct cycle lengths in the (complete) cycle decomposition of σ, and for each $1 \leq i \leq s$ let k_i be the number of m_i-cycles in the decomposition (so $n = \sum_{i=1}^s k_i m_i$). Then the number of conjugates of σ is

$$n! \prod_{i=1}^{s} \frac{1}{k_i!\, m_i^{k_i}}$$

Proof. Recall that the number of conjugates of σ is precisely the number of elements in S_n with the same cycle type as σ, hence we need only count the number of ways to form a permutation in S_n with this cycle type.

We give a combinatorial argument. To obtain any such permutation we may start with any linear arrangement of the numbers $1, \dots, n$ and then partition the numbers into cycles, by drawing parentheses, according to the cycle type of σ. Now there are $n!$ distinct linear arrangements of the numbers $1, \dots, n$. However, for any such permutation formed, for each $1 \leq i \leq s$, the m_i-cycles may be permuted amongst each other in any of $k_i!$ ways, and the elements in each m_i-cycle may be cyclically permuted in m_i ways, while still preserving identity and form. Thus each linear arrangement of $1, \dots, n$ is in an equivalence class of $\prod_{i=1}^s k_i!\, m_i^{k_i}$ (including itself), all of which give the same permutation. Thus the number of distinct permutations with the cycle type of σ is as above. □

EXERCISE 36. Let G be a group. Let $\pi : G \to S_G$ be the left regular representation of G, and write $\pi(g) = \sigma_g$, so $\sigma_g(x) = gx$ for all $x \in G$. Similarly let $\lambda : G \to S_G$ be the right regular representation of G, and write $\lambda(h) = \tau_h$, so $\tau_h(x) = xh^{-1}$ for all $h \in G$.[1]

(a) $C_{S_G}(\pi(G)) = \lambda(G)$ and $C_{S_G}(\lambda(G)) = \pi(G)$. In particular, σ_g and τ_h commute for all $g, h \in G$.

[1] Note that under our definitions, the right regular *representation* λ of G is not associated with a right *action* of G, but a left action $h \cdot x = xh^{-1}$, for otherwise λ would fail to be a homomorphism under our usual left-based functional notation.

Proof. We prove the first equality; the other follows by symmetry. Note that $\lambda(G) \subseteq C_{S_G}(\pi(G))$ since for $g, h \in G$,

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

for all $x \in G$. Conversely, suppose $\tau \in C_{S_G}(\pi(G))$, so $\tau\sigma_g = \sigma_g\tau$ for all $g \in G$. We claim that there exists some $h \in G$ such that $\tau = \tau_h$. Indeed, let $h = \tau(1)^{-1}$, so $\tau(1) = h^{-1}$. Then

$$\tau(x) = \tau(\sigma_x(1)) = (\tau\sigma_x)(1) = (\sigma_x\tau)(1) = \sigma_x(\tau(1)) = \sigma_x(h^{-1}) = xh^{-1} = \tau_h(x)$$

for all $x \in G$. Hence $\tau = \tau_h$, satisfying the claim.

Thus $C_{S_G}(\pi(G)) = \lambda(G)$ as desired. □

(b) $\sigma_g = \tau_g$ iff $g \in Z(G)$ and $|g|$ equals 1 or 2. *Proof:* part (c).

(c) $\sigma_g = \tau_h$ iff $g, h \in Z(G)$ and $g = h^{-1}$. Thus $\pi(G) \cap \lambda(G) = \pi(Z(G)) = \lambda(Z(G))$.

Proof. Note $\sigma_g = \tau_h$ iff for all $x \in G$, $gx = \sigma_g(x) = \tau_h(x) = xh^{-1}$, which is true iff $g = h^{-1}$ (taking $x = 1$) and hence $gx = xg$ for all $x \in G$, which is true iff $g = h^{-1}$ and $g, h \in Z(G)$.

The set identities are now immediate. □

Note this exercise shows in particular that the centralizer of the left or right regular permutation representation of a group is isomorphic to the group itself.

Section 4

EXERCISE 1. Let G be a group, $g \in G$, and let φ_g denote conjugation by g. Then for $\sigma \in \mathrm{Aut}(G)$, $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Hence $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Proof. Let $\varphi^* = \sigma\varphi_g\sigma^{-1}$. Then for $x \in G$,

$$\varphi^*(x) = (\sigma\varphi_g\sigma^{-1})(x) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)x\sigma(g)^{-1}$$

Hence $\varphi^* = \varphi_{\sigma(g)}$ as desired. □

The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G.

EXERCISE 2. Let G be an abelian group, $|G| = pq$ where $p \neq q$ are prime. Then G is cyclic.

Proof. By Cauchy's Theorem, there exist $x, y \in G$ with $|x| = p$ and $|y| = q$. Set $z = xy$. Note that

$$z^{pq} = (xy)^{pq} = x^{pq}y^{pq} = (x^p)^q(y^q)^p = 1 \cdot 1 = 1$$

Hence $|z|$ divides pq. We claim $|z| = pq$.

If $|z|$ divides p, then $1 = (xy)^p = x^p \cdot y^p = y^p$. But this implies $q|p$, which is a contradiction since $p \neq q$. Similarly $|z|$ does not divide q since p does not divide q.

Hence $|z| = pq$ as claimed, and G is cyclic. □

Recall from the text that if $|G| = pq$ with $p \leq q$ and p does not divide $q - 1$, then G is abelian. Combining this with the above result we obtain the following classification theorem: *if $|G| = pq$ with $p < q$ and p does not divide $q - 1$, then G is cyclic.*

As an example, if $|G| = 15 = 3 \cdot 5$, then G is cyclic.

EXERCISE 3. $|\mathrm{Aut}(D_8)| \leq 8$

Proof. Looking at cycle decompositions (Exercise 1.7.11) of the elements in D_8, we see that under any automorphism, r has at most two images (elements of order 4), and s has at most four images (elements of order 2 which are not in the center). □

EXERCISE 5. $\mathrm{Aut}(D_8) \cong D_8$

Proof. Note $D_8 \trianglelefteq D_{16}$, so D_{16} acts on D_8 by conjugation and $D_{16}/C_{D_{16}}(D_8)$ is isomorphic to a subgroup of $\mathrm{Aut}(D_8)$. Note that $C_{D_{16}}(D_8) = \langle r^4 \rangle$, so since $|\mathrm{Aut}(D_8)| \leq 8$ (by Exercise 3), we have

$$\mathrm{Aut}(D_8) \cong D_{16}/\langle r^4 \rangle \cong D_8$$

where the last isomorphism holds since the groups have an identical presentation. □

This exercise illustrates that if inner automorphisms do not exhaust $\mathrm{Aut}(G)$, then it is useful to look at larger normalizers of G.

EXERCISE 6. If H char G, then $H \trianglelefteq G$.

Proof. Trivial since H is preserved under inner automorphisms. □

EXERCISE 7. If H is the unique subgroup of a given order in G, then H char G.

Proof. Trivial since automorphisms preserve order and map subgroups to subgroups. □

Note it follows that any subgroup of a cyclic group is characteristic.

EXERCISE 8. Suppose $H \leq K \leq G$.

(a) If H char $K \trianglelefteq G$, then $H \trianglelefteq G$.

Proof. If $g \in G$ and φ_g denotes the automorphism in G of conjugation by g, then $\varphi_g|_K \in \mathrm{Aut}(K)$ since $K \trianglelefteq G$. Hence $\varphi_g(H) = \varphi_g|_K(H) = H$ since H char K, that is, $gHg^{-1} = H$. Since g was arbitrary, $H \trianglelefteq G$. □

(b) If H char K char G, then H char G.

Proof. If $\sigma \in \mathrm{Aut}(G)$, then $\sigma(K) = K$ since K char G, hence $\sigma|_K \in \mathrm{Aut}(K)$. But then $\sigma(H) = \sigma|_K(H) = H$ since H char K. Since σ was arbitrary, H char G. □

Note that V_4 char S_4.

(c) It is not true in general that $H \trianglelefteq K$ char G implies $H \trianglelefteq G$. For example, $Z_2 \trianglelefteq V_4$ char S_4, but Z_2 is not normal in S_4.

EXERCISE 9. Let $G = D_{2n}$ and $K = \langle r \rangle$. Then every subgroup of K is normal in G.

Proof. Let $H \leq K$. Note $K \trianglelefteq G$ (by checking generators). Recall that $\mathrm{Aut}(K)$ consists of maps $r \mapsto r^a$ where $0 < a < n$ and $(a, n) = 1$. Hence H is mapped to itself under any automorphism of K, that is, H char K. It follows from Exercise 8(a) that $H \trianglelefteq G$. □

This exercise illustrates another useful way of finding normal subgroups.

EXERCISE 11. Let $G = S_p$, and $P \leq G$ with $|P| = p$. Then $N_G(P)/C_G(P) \cong \mathrm{Aut}(P)$.

Proof. P is cyclic and generated by a p-cycle x. We know $\mathrm{Aut}(P)$ consists of maps $x \mapsto x^k$ with $0 < k < p$, where the image of x is always a p-cycle. Each of these maps can be obtained via conjugation of x in S_p w ith an element of $N(P)$. Hence $N(P)/C(P)$ is isomorphic to all of $\mathrm{Aut}(P)$. □

EXERCISE 13. If $|G| = 203$ and G has a normal subgroup of order 7, then G is abelian (and hence cyclic).

Proof. Note $|G| = 7 \cdot 29$, where 7 and 29 are both prime. Let $H \trianglelefteq G$ with $|H| = 7$. We know $G/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$, hence $|G|/|C(H)|$ must divide $|\mathrm{Aut}(H)| = \varphi(7) = 6$. This is only possible if $C(H) = G$, that is, $H \leq Z(G)$. This implies G/Z is of prime order and hence cyclic, so G is abelian. It follows that G is cyclic by Exercise 2. □

EXERCISE 15. The groups $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/9\mathbb{Z})^\times$, and $(\mathbb{Z}/18\mathbb{Z})^\times$ are each cyclic.

Proof. The groups are each abelian. The latter two are of orders $\varphi(9) = 3(3-1) = 6$ and $\varphi(18) = (2-1) \cdot 3(3-1) = 6$, respectively, hence cyclic by Exercise 2. The first group is cyclic and generated by the element $\overline{2}$. □

Section 5

NOTE.The proof of Sylow's Theorem illustrates several recurring techniques:

1. It uses induction to prove (part of) an existence claim (cf. Cauchy's Theorem for abelian groups, Exercise 3.29, etc.).
2. It makes use of the Class Equation, combining information about the order of G and an assumption about the order of $Z(G)$ to obtain information about subgroups (centralizers) in G (cf. an example in Section 4.4).
3. To count Sylow subgroups, it restricts the source of a group action to a subgroup about which we have more information, which provides additional information about the original orbits (cf. Exercise 1.9).
4. In using Sylow p-subgroups computationally, it utilizes their maximality in order among p-subgroups.

These techniques are important to keep in mind.

EXERCISE 3 (CAUCHY'S THEOREM). Let G be a group, p a prime dividing $|G|$. Then there exists $g \in G$ with $|g| = p$.

Proof. Let P be a Sylow p-subgroup of G. Since p divides $|G|$, there exists $x \in P$, $x \neq 1$. Set $H = \langle x \rangle$. Then H is a nontrivial cyclic p-subgroup of G, so p divides $|H|$ and hence there exists $g \in H$ with $|g| = p$. □

EXERCISE 5. Let $G = D_{2n}$. If p is an odd prime and $P \in \mathrm{Syl}_p(G)$, then P is cyclic and normal.

Proof. Let $P \in \mathrm{Syl}_p(G)$. Let r, s be the usual generators of G and set $H = \langle r \rangle$. Recall $|H| = n$, hence (since $p \neq 2$) any Sylow p-subgroup of H is also a Sylow p-subgroup of G. By Sylow's Theorem then, all Sylow p-subgroups of G are contained in H, so in particular $P \leq H$. It follows that P is cyclic, and P char $H \trianglelefteq G$ (see Exercise 4.7), hence $P \trianglelefteq G$. □

EXERCISE 6. We find all Sylow 3-subgroups of S_4 and A_4.

Proof. Recall $|S_4| = 4! = 24 = 2^3 \cdot 3$, hence a Sylow 3-subgroup of S_4 is just a subgroup of order 3 generated by an element of order 3. By direct computation it is easily seen that the distinct such subgroups are:

$$\langle(123)\rangle \quad \langle(124)\rangle \quad \langle(134)\rangle \quad \langle(234)\rangle$$

Since these consist of even permutations, they are also the Sylow 3-subgroups of A_4. □

EXERCISE 13. Let G be a group with $|G| = 56$. Then G has a normal Sylow p-subgroup for some prime p dividing $|G|$.

Proof. Note $|G| = 2^3 \cdot 7$. By Sylow's Theorem, $n_7 \equiv 1\ (7)$ and $n_7 | 8$, thus $n_7 = 1$ or $n_7 = 8$. If $n_7 = 1$, then there is a unique normal Sylow 7-subgroup of G. If $n_7 = 8$, then there are $8 \cdot (7-1) = 48$ elements of order 7 in G (since distinct Sylow 7-subgroups must have trivial intersection), leaving 8 remaining elements. These 8 elements must be precisely those in a unique, and hence normal, Sylow 2-subgroup of G. □

EXERCISE 16. Let G be a group with $|G| = pqr$, where p, q, r are prime and $p < q < r$. Then G has a normal Sylow subgroup for one of p, q, r.

Proof. Assume towards a contradiction that none of n_p, n_q, n_r equal 1. We know from Sylow's Theorem that $n_p|qr$, hence $n_p \geq q$. Also $n_q|pr$, but since $n_q \equiv 1$ (q) and $p < q$, we must have $n_q \geq r$. Similarly $n_r|pq$ but $n_r \neq p$ and $n_r \neq q$, so $n_r = pq$. But then by counting elements we must have

$$\begin{aligned} pqr = |G| &\geq q(p-1) + r(q-1) + pq(r-1) \\ &= pqr + qr - (q+r) \\ &> pqr + qr - 2r && \text{since } q < r \\ &> pqr && \text{since } 2 \leq p < q \end{aligned}$$

—a contradiction. Thus one of n_p, n_q, n_r equals 1, establishing the result. □

EXERCISE 17. Let G be a group with $|G| = 105$. Then there exists a normal Sylow 5-subgroup and a normal Sylow 7-subgroup in G.

Proof. Note $|G| = 3 \cdot 5 \cdot 7$. By Sylow's Theorem, $n_7 \equiv 1$ (7) and $n_7|15$, hence $n_7 = 1$ or $n_7 = 15$. Similarly $n_5 = 1$ or $n_5 = 21$. If neither n_5 nor n_7 equals 1, then there exist $15 \cdot (7-1) + 21 \cdot (5-1) = 174 > 105$ elements of orders 7 and 5 in G, contradicting the order of G. Thus at least one of n_7 and n_5 equals 1.

Let $P \in \mathrm{Syl}_7(G)$ and $Q \in \mathrm{Syl}_5(G)$. We know from the above remarks that $P \trianglelefteq G$ or $Q \trianglelefteq G$, so $PQ \leq G$. Now $|P \cap Q| = 1$, hence $|PQ| = |P||Q| = 7 \cdot 5 = 35$. It follows that PQ is cyclic (since $5 < 7$ and 5 does not divide $7-1$), and $PQ \trianglelefteq G$ since $|G : PQ| = 3$ (the smallest prime dividing $|G|$). Hence any subgroup of PQ is normal in G (see Exercises 4.7–8), so in particular $P \trianglelefteq G$ and $Q \trianglelefteq G$. □

Note this proof utilizes the technique of constructing an intermediate cyclic normal subgroup (cf. the example on groups of order 30).

EXERCISE 22. Let G be a group and $|G| = 132$. Then G is not simple.

Proof. Note $|G| = 2^2 \cdot 3 \cdot 11$. By Sylow's Theorem, $n_{11} = 1$ or $n_{11} = 12$. If $n_{11} = 1$, G has a normal Sylow 11-subgroup and we are done. If $n_{11} = 12$, there exist $12 \cdot (11-1) = 120$ elements of order 11 in G, leaving 12 elements remaining.

In this case, if $n_3 = 1$ there exists a normal Sylow 3-subgroup and we are done. Otherwise we must have $n_3 = 4$ and $4 \cdot (3-1) = 8$ elements of order 3, which leaves 4 elements in G to form the unique and hence normal Sylow 2-subgroup of G. □

EXERCISE 24. Let G be a group, $|G| = 231$. Then $Z(G)$ contains a Sylow 11-subgroup and there exists a normal Sylow 7-subgroup.

Proof. Note $|G| = 3 \cdot 7 \cdot 11$. By Sylow's Theorem, $n_7 \equiv 1\ (7)$ and $n_7 | 33$, leaving only the possibility $n_7 = 1$ and a normal Sylow 7-subgroup.

Similarly $n_{11} = 1$. Let P be the unique Sylow 11-subgroup of G. Since P is normal, $N(P) = G$, and hence $G/C(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$. In particular, $|G|/|C(G)|$ divides $|\mathrm{Aut}(P)| = \varphi(11) = 10$. But this is only possible if $|C(P)| = |G|$, that is, $C(P) = G$ so $P \le Z(G)$. □

EXERCISE 26. Let G be a group with $|G| = 105$ and suppose G has a normal Sylow 3-subgroup. Then G is abelian.

Proof. Recall $|G| = 3 \cdot 5 \cdot 7$. Let $P \in \mathrm{Syl}_3(G)$. Then $N(P) = G$, so $G/C(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$. In particular, $|G|/|C(P)|$ divides $|\mathrm{Aut}(P)| = \varphi(3) = 2$. But this is only possible if $C(P) = G$, that is, $P \le Z(G)$.

Set $\overline{G} = G/Z(G)$. The only possibilities for $|\overline{G}|$ are $1, 5, 7, 35 (= 5 \cdot 7)$. In all cases, $\overline{G}$ is cyclic (for case 35, note $5 < 7$ and 5 does not divide $7 - 1$). Hence G is abelian. □

EXERCISE 30. A simple group of order 168 must have 48 elements of order 7.

Proof. Suppose $|G| = 168 = 2^3 \cdot 3 \cdot 7$. By Sylow's Theorem, $n_7 \equiv 1\ (7)$ and $n_7 | 24$, hence $n_7 = 1$ or $n_7 = 8$. But since G is simple, $n_7 \neq 1$. Hence since every element of order 7 lies in a Sylow 7-subgroup, and distinct Sylow 7-subgroups have trivial intersection, there are $8 \cdot (7 - 1) = 48$ elements of order 7 in G. □

EXERCISE 32. Suppose $P \in \mathrm{Syl}_p(H)$ and $P \trianglelefteq H \trianglelefteq K$. Then $P \trianglelefteq K$.

Proof. By Corollary 20, P char $H \trianglelefteq K$, hence $P \trianglelefteq K$ by Exercise 4.8(a). □

Set $H = N(P)$, so $P \trianglelefteq H \trianglelefteq N(H)$. By this exercise, $P \trianglelefteq N(H)$, hence $N(H) \le H$, so $N(H) = H$. In other words, *normalizers of Sylow p-subgroups are self-normalizing.*

EXERCISE 33. Let G be a group, P a normal Sylow p-subgroup of G, and $H \le G$. Then $P \cap H$ is the unique Sylow p-subgroup of H.

Proof. Let P^* be a Sylow p-subgroup of H. Then since P^* is a p-subgroup of G, there exists $g \in G$ with $P^* \le gPg^{-1} = P$. Hence $P^* \le P \cap H$. Now $P \cap H$ is a p-subgroup of H, so by the maximality of P^* we have $P^* = P \cap H$. Since P^* was arbitrary, $P \cap H$ is unique. (Alternately, this follows since $P \cap H \trianglelefteq H$.) □

EXERCISE 34. Let G be a group, P a Sylow p-subgroup of G, and $N \trianglelefteq G$. Then $P \cap N$ is a Sylow p-subgroup of N.

Proof. Let $P^* \in \mathrm{Syl}_p(N)$. Then there exists $g \in G$ such that $P^* \leq gPg^{-1}$, and hence

$$g^{-1}P^*g \leq g^{-1}(gPg^{-1})g = P$$

Set $P^{**} = g^{-1}P^*g$. Then $P^{**} \in \mathrm{Syl}_p(N)$ since $N \trianglelefteq G$, and by counting elements we get $P^{**} = P \cap N$ (cf. Exercise 33). □

Note that

$$|PN/N| = \frac{|PN|}{|N|} = \frac{|P||N|}{|P \cap N||N|} = \frac{|P|}{|P \cap N|}$$

which is the highest power of p dividing $|G|/|N|$. Hence $PN/N \in \mathrm{Syl}_p(G/N)$. (See also Exercise 3.3.9.)

EXERCISE 35. Note that for $P \in \mathrm{Syl}_p(G)$ and $H \leq G$, it is not true in general that $P \cap H \in \mathrm{Syl}_p(H)$. For example, $P = \langle(12)\rangle$ is a Sylow 2-subgroup of S_3, but if $H = \langle(23)\rangle$, $P \cap H = 1$, which is not a Sylow 2-subgroup of H.

EXERCISE 43. Let G be the group of rigid motions in $\mathbb{R}^3$ of a (regular) dodecahedron. Then $G \cong A_5$.

Proof. We know from a counting argument that $|G| = 60$ (see Exercise 1.2.12). Hence by Proposition 23, it suffices to prove that G is simple, and hence by Proposition 21 it suffices to prove that G has more than one Sylow 5-subgroup.

Since $60 = 2^2 \cdot 3 \cdot 5$, any subgroup of G of order 5 is a Sylow 5-subgroup of G. Recall that G acts on the set of 12 faces of the dodecahedron and each such face has a stabilizer of order 5. Clearly there exists more than one distinct such stabilizer. By the above remarks this completes the proof. □

EXERCISE 44. Let G be a group and p be the smallest prime dividing $|G|$. Then if $P \in \mathrm{Syl}_p(G)$ and P is cyclic, $N(P) = C(P)$.

Proof. Write $|P| = p^\alpha$. Since P is cyclic, $P \leq C(P) \leq N(P)$. Let $k = |N(P)|/|C(P)|$. We know k divides $|\mathrm{Aut}(P)| = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. But since p^α divides $|C(P)|$ this implies k divides $p-1$. Also, since p is the smallest prime dividing $|G|$, no nontrivial factor of $|N(P)|$ divides $p-1$, so $k = 1$. This implies $N(P) = C(P)$ as desired. □

EXERCISE 49. Let G be a group of order $2^n m$, where m is odd, and suppose G has a cyclic Sylow 2-subgroup. Then G has a normal subgroup of order m.

Proof. We prove existence of a subgroup of order m by induction on n.

Case $n = 0$ is trivial. If $n > 0$, since G has a cyclic Sylow 2-subgroup, we may fix $x \in G$ with $|x| = 2^n$. Then $|x|$ is even and $|G|/|x|$ is odd. Hence by Exercises 2.11–12, there exists $H \leq G$ with $|G : H| = 2$, that is, $|H| = 2^{n-1}m$. By induction there exists $K \trianglelefteq H$ with $|K| = m$. □

Section 6

EXERCISE 1. For $n \geq 5$, A_n has no proper subgroups with index strictly less than n.

Proof. Suppose towards a contradiction that $A < A_n$ and $|A_n : A| = m < n$.

Recall A_n acts on the coset space A_n/A, affording a permutation representation $\varphi : A_n \to S_m$. Write $K = \ker\varphi$. Then $K \leq A$, and A_n/K is isomorphic to a subgroup of S_m. Since $1 < m < n$, we know $|S_m| = m! < n!/2 = |A_n|$, hence $K \neq 1$. But then $1 < K \leq A < A_n$ and $K \trianglelefteq A_n$ (since K is a kernel), so K is a nontrivial proper normal subgroup of A_n. This contradicts that A_n is simple for $n \geq 5$. □

EXERCISE 5. Let G be a group and suppose $G = \bigcup G_i$ where $G_1 \leq G_2 \leq \cdots \leq G$ and each G_i is simple. Then G is simple.

Proof. Suppose towards a contradiction G is not simple, so there exists $1 < H < G$ with $H \trianglelefteq G$. For all i, set $H_i = G_i \cap H$. Then $H_1 \leq H_2 \leq \cdots \leq H = \bigcup H_i$ and $H_i \trianglelefteq G_i$ for all i. Since $H \neq 1$, there exists a least j with $H_j \neq 1$. If $H_k = G_k$ for all $k \geq j$, then

$$H = \bigcup H_i = \bigcup_{k \geq j} H_k = \bigcup_{k \geq j} G_k = G$$

contradicting that $H < G$. Hence there exists $k \geq j$ such that $1 < H_j \leq H_k < G_k$—in other words, H_k is a nontrivial proper normal subgroup of G_k, contradicting our assumption that G_k is simple. □

Chapter 5

Section 1

EXERCISE 4. Let $G_1, \cdots, G_n$ be finite groups, $G = \prod G_i$, and p a prime. Then

$$\mathrm{Syl}_p(G) = \left\{ \prod P_i \mid P_i \in \mathrm{Syl}_p(G_i) \right\}$$

Hence $n_p(G) = \prod n_p(G_i)$.

Proof. The reverse inclusion is immediate since $|G| = \prod |G_i|$ and $|\prod P_i| = \prod |P_i|$ for any subgroups $P_i \leq G_i$.

To prove the forward inclusion, suppose $P \in \mathrm{Syl}_p(G)$, and set $P_i = P \cap G_i$ for all i so $P = \prod P_i$ (here we are identifying G_i with the naturally corresponding subgroup of G). Then by Lagrange's Theorem, P_i is a p-subgroup of G_i for all i, so there exist subgroups $P_i^* \in \mathrm{Syl}_p(G_i)$ with $P_i \leq P_i^*$. Note $P^* = \prod P_i^* \in \mathrm{Syl}_p(G)$ by the above, and $P \leq P^*$. But $P = P^*$ since $|P| = |P^*|$, hence $P_i = P_i^*$ and $P_i \in \mathrm{Syl}_p(G_i)$ for all i.

The value of $n_p(G)$ follows immediately. □

EXERCISE 5. We exhibit a nonnormal subgroup of $G = Q_8 \times Z_4$. Recall

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \quad \text{where} \quad i^2 = j^2 = k^2 = ijk = -1$$

Write $Z_4 = \langle x \rangle$. Set $H = \langle ix \rangle = \{1, ix, -x^2, -ix^3\}$. Then H is not normal in G, since e.g.

$$j(ix)j^{-1} = j(ix)(-j) = ji(-j)x = j(-k)x = -ix \notin H$$

Note this exercise illustrates the importance of looking at subgroups of products other than the factors in the product. Indeed, all subgroups of Q_8 and Z_4 are normal, hence normal in G, and hence any product obtained from these subgroups is also normal in G. The subgroup H is isomorphic to Z_4 but is not normal in G.

EXERCISE 7. Let $G_1, \cdots, G_n$ be groups and $\pi \in S_n$. Define

$$\begin{aligned} \varphi_\pi : \prod G_i &\to \prod G_{\pi^{-1}(i)} \\ (g_i) &\mapsto (g_{\pi^{-1}(i)}) \end{aligned}$$

Then φ_π is an isomorphism.

Proof. Clearly φ_π is well defined. Also

$$\begin{aligned} \varphi_\pi((g_i)(h_i)) &= \varphi_\pi(g_i h_i) \\ &= (g_{\pi^{-1}(i)} h_{\pi^{-1}(i)}) \\ &= (g_{\pi^{-1}(i)})(h_{\pi^{-1}(i)}) \\ &= \varphi_\pi(g_i)\varphi_\pi(h_i) \end{aligned}$$

So φ_π is a homomorphism. If $(g_{\pi^{-1}(i)}) = (h_{\pi^{-1}(i)})$, then $g_i = g_{\pi(\pi^{-1}(i))} = h_{\pi(\pi^{-1}(i))} = h_i$ for all i, that is, $(g_i) = (h_i)$. If $(g_i^*) \in \prod G_{\pi^{-1}(i)}$, set $(g_i) = (g^*_{\pi(i)})$. Then $(g_i) \in \prod G_i$ and

$$\varphi_\pi(g_i) = (g_{\pi^{-1}(i)}) = (g^*_{\pi(\pi^{-1}(i))}) = (g_i^*)$$

Hence φ_π is a bijection, so φ_π is an isomorphism as desired. □

EXERCISE 8. Let $G_1 = \cdots = G_n$ and $G = \prod G_i$. Then for $\pi \in S_n$ and φ_π as above, $\varphi_\pi \in \text{Aut}(G)$, and the map $\pi \mapsto \varphi_\pi$ is an embedding of S_n into $\text{Aut}(G)$.

Proof. It follows from Exercise 7 that $\varphi_\pi \in \text{Aut}(G)$. If $\sigma, \tau \in S_n$, then

$$\begin{aligned} (\varphi_\sigma \circ \varphi_\tau)(g_i) &= \varphi_\sigma(\varphi_\tau(g_i)) \\ &= \varphi_\sigma(g_{\tau^{-1}(i)}) \\ &= (g_{\tau^{-1}(\sigma^{-1}(i))}) \\ &= (g_{(\sigma\tau)^{-1}(i)}) = \varphi_{\sigma\tau}(g_i) \end{aligned}$$

(Note the third equality follows since if we write $h_i = g_{\tau^{-1}(i)}$, then $\varphi_\sigma(h_i) = (h_{\sigma^{-1}(i)})$ by definition and $h_{\sigma^{-1}(i)} = g_{\tau^{-1}(\sigma^{-1}(i))}$.) Therefore $\pi \mapsto \varphi_\pi$ is a homomorphism. It is clear that the kernel of this homomorphism is trivial, so it is injective. □

EXERCISE 9. Let F be a field, and let H be the set of $n \times n$ matrices over F with only a single 1 in each row and column (and 0's elsewhere). Then $H \leq GL_n(F)$ and $H \cong S_n$.

Proof. Note H acts faithfully on the standard basis vectors $e_1, \ldots, e_n$ in the vector space F^n. Hence $H \leq GL_n(F)$ (since each matrix in H has a natural inverse), and $H \cong S_n$. □

The matrices in H are called *permutation matrices* for the obvious reason.

EXERCISE 11. Let n be a positive integer and p a prime. The number of subgroups of order p in the elementary abelian group E_{p^n} is $(p^n - 1)/(p-1)$.

Proof. Each of the $p^n - 1$ nonidentity elements in E_{p^n} generates, and hence lives in, a subgroup of order p. By Lagrange's Theorem, distinct subgroups of order p have trivial intersection, hence the $p^n - 1$ nonidentity elements are partitioned into sets of $p - 1$ elements, namely the subgroups of order p minus the identity element. It follows that there are $(p^n - 1)/(p-1)$ such subgroups. □

EXERCISE 12,13 (CENTRAL PRODUCTS). Let A and B be groups with $Z_1 \leq Z(A)$ and $Z_2 \leq Z(B)$ such that $Z_1 \cong Z_2$ by the mapping $x_i \mapsto y_i$. Set $Z = \{(x_i, y_i^{-1}) \mid x_i \in Z_1\}$ and define $A * B = (A \times B)/Z$.

(a) Let $\overline{A} = A/Z$ and $\overline{B} = B/Z$ (here identifying A and B with $A \times 1$ and $1 \times B$, respectively). Then $\overline{A} \cong A$ and $\overline{B} \cong B$, and $\overline{A} \cap \overline{B}$ is a central subgroup of $A * B$ isomorphic to Z_1(and Z_2).

Proof. Let π project A onto A/Z. Then $\ker \pi = \{(a, 1) \in Z\}$. But if $(a, 1) \in Z$, $(a, 1) = (x_i, y_i^{-1})$ for some i, that is, $y_i^{-1} = 1$ so $y_i = 1$ and hence $a = x_i = 1$. Thus $\ker \pi = 1$ and $A \cong \overline{A}$ by the First Isomorphism Theorem. Similarly $B \cong \overline{B}$.

If $x \in \overline{A} \cap \overline{B}$, then $x = \overline{a} = \overline{b}$ for some $a \in A$, $b \in B$. In particular, $(a, 1) \in (1, b)Z$, so there exists i with

$$(a, 1) = (1, b)(x_i, y_i^{-1}) = (x_i, b y_i^{-1})$$

That is, $a = x_i$ and $b = y_i$, so $x = \overline{x_i} = \overline{y_i}$. Conversely, any element of the form $\overline{x_i}$ is in $\overline{A} \cap \overline{B}$, since $\overline{x_i} = \overline{y_i}$ in $A * B$. Hence we have

$$\overline{A} \cap \overline{B} = \{\overline{x_i} \mid x_i \in Z_1\} = \overline{Z_1} = \overline{Z_2} = \{\overline{y_i} \mid y_i \in Z_2\}$$

which is isomorphic to Z_1 (and Z_2). This subgroup is central in $A * B$ since Z_1 and Z_2 are central in A and B, respectively. □

(b) Let $Z_4 = \langle x \rangle$ and $D_8 = \langle r, s \rangle$ (r, s as usual). Then we may form $Z_4 * D_8$ under the identification $x^2 \mapsto r^2$. We then have

$$Z_4 * D_8 = \langle \overline{x}, \overline{r}, \overline{s} \mid \overline{x}^4 = 1 = \overline{r}^4 = \overline{s}^2, \overline{r}\,\overline{s} = \overline{s}\,\overline{r}^{-1}, \overline{x}^2 = \overline{r}^2 \rangle$$

The central product illustrates well how quotient groups can be used to 'identify' elements in existing groups. In this case we desire to identify each element x_i in a central subgroup of A with a corresponding element y_i in an isomorphic central subgroup of B. In other words, we desire $x_i = y_i$. We achieve this by taking a quotient to force $\overline{x_i} = \overline{y_i}$. Since

$$\overline{x_i} = \overline{y_i} \iff \overline{x_i}\,\overline{y_i}^{-1} = \overline{1} \iff \overline{x_i y_i^{-1}} = \overline{1}$$

we divide out the elements $x_i y_i^{-1} = (x_i, y_i^{-1})$—that is, the elements in Z.

In the quotient $A * B$, we retain the structures of A and B, but the two distinct central subgroups of A and B have collapsed into one central subgroup of both.

EXERCISE 14. Suppose $B_i \trianglelefteq A_i$ for all i. Then $\prod B_i \trianglelefteq \prod A_i$ and $\prod A_i / \prod B_i \cong \prod(A_i/B_i)$

Proof. Define $\pi : \prod A_i \to \prod(A_i/B_i)$ by the map $(a_i) \mapsto (a_i B_i)$. It is immediate that π is a surjective homomorphism and $\ker\pi = \prod B_i$. Hence $\prod B_i \trianglelefteq \prod A_i$ and the quotient identity follows from the First Isomorphism Theorem. □

Note that even if every subgroup of each A_i is normal, it is not necessarily true that every subgroup of $\prod A_i$ is normal (see Exercise 5).

EXERCISE 18. We exemplify groups satisfying various properties:

(a) $G = \prod_{n=1}^{\infty} Z_2$ is an infinite group, but every element has order 1 or 2.

(b) $G = \mathbb{Q}/\mathbb{Z}$ is an infinite group in which every element has finite order, but there is an element of order n for each positive integer n (cf Exercise 3.1.14).

(c) $G = Z_2 \times \mathbb{Z}$ has an element of order 2 and an element of infinite order.

(d) $G = \prod_{n=1}^{\infty} S_n$ is such that any finite group is isomorphic to a subgroup of G.

(e) $G = \prod_{n=1}^{\infty} Z_2$ is nontrivial and $G \cong G \times G$.

Section 2

EXERCISE 1. For each n, we count the number of isomorphism classes of abelian groups of order n by counting the number of possible lists of elementary divisors.

(a) $n = 100$: Note $n = 2^2 \cdot 5^2$, hence there are $2 \cdot 2 = 4$ classes.

(b) $n = 576$: Note $n = 2^6 \cdot 3^2$, hence since there are 11 possible partitions of 6 elements, there are $11 \cdot 2 = 22$ classes.

EXERCISE 3. For each n, we find all possible elementary divisors and invariant factors for abelian groups of order n.

(a) $n = 270$: Note $270 = 2 \cdot 3^3 \cdot 5$, hence the possible lists of elementary divisors are $\{2, 3^3, 5\}$, $\{2, 3^2, 3, 5\}$, and $\{2, 3, 3, 3, 5\}$. Using the algorithm to obtain invariant factors from elementary divisors, we obtain the corresponding lists $\{2 \cdot 3^3 \cdot 5\}$, $\{2 \cdot 3^2 \cdot 5, 3\}$, and $\{2 \cdot 3 \cdot 5, 3, 3\}$, respectively, of invariant factors.

EXERCISE 4. Let $[a_1, \cdots, a_k]$ denote the group $Z_{a_1} \times \cdots \times Z_{a_k}$. We determine which pairs of groups given are isomorphic.

(a) For groups $[4,9]$, $[6,6]$, $[8,3]$, $[9,4]$, $[6,4]$, and $[64]$, we have the following lists of elementary divisors:

$$\begin{aligned}
[4,9] &\longrightarrow \{2^2, 3^2\}\\
[6,6] &\longrightarrow \{2,2,3,3\}\\
[8,3] &\longrightarrow \{2^3, 3\}\\
[9,4] &\longrightarrow \{2^2, 3^2\}\\
[6,4] &\longrightarrow \{2, 2^2, 3\}\\
[64] &\longrightarrow \{2^6\}
\end{aligned}$$

Hence $[4,9] \cong [9,4]$, but no other pairs of distinct groups above are isomorphic.

EXERCISE 5. Let G be a finite abelian group of type $(n_1, \ldots, n_t)$. Then G contains an element of order m iff $m|n_1$. In particular, G has exponent n_1.

Proof. By assumption $G = Z_{n_1} \times \cdots \times Z_{n_t}$. If $m|n_1$, then there is an element of order m in the subgroup Z_{n_1}, and hence in G. Conversely, if $x = (x_1, \ldots, x_t) \in G$ has order m, then $m = \mathrm{lcm}(|x_1|, \ldots, |x_t|)$. Now $|x_i|$ divides n_i for $1 \le i \le t$, hence since each n_i divides n_1, n_1 is a common multiple of the $|x_i|$. Since m is the least such multiple, $m|n_1$ as desired.

It follows that for all $x \in G$, $x^{n_1} = 1$ since $|x|$ divides n_1. Also G has an element of order n_1 (namely the generator of Z_{n_1}), so no smaller number satisfies this property. Therefore G has exponent n_1. □

EXERCISE 6. A finite group has finite exponent. An infinite group may have finite exponent. A group with exponent m need not contain an element of order m.

Proof. If $|G| = n$, then for all $x \in G$, $|x|$ divides n (Lagrange), hence $x^n = 1$. Let m be the least integer satisfying this property. Then m is the exponent of G.

Let $G = \prod^{\infty} Z_2$. Then G is an infinite group with finite exponent 2.

Let $G = D_6$. Then G has exponent 6, but G contains no element of order 6. □

EXERCISE 7. Let p be a prime. For $1 \le i \le n$, let $A_i = \langle x_i \rangle$ where $|x_i| = p^{\alpha_i} > 1$, and set $A = \prod A_i$. Define $\varphi : A \to A$ by $x \mapsto x^p$ (the *p-th power map*).

(a) φ is a homomorphism. (*Proof:* trivial since each A_i is abelian.)

(b) $\mathrm{im}\varphi = \prod \langle x_i^p \rangle$ and $\ker\varphi = \prod \langle x_i^{p^{\alpha_i - 1}} \rangle$.

Proof. Write $[x_i^{m_i}] = (x_1^{m_1}, \cdots, x_n^{m_n})$. Then

$$\mathrm{im}\varphi = \left\{ [x_i^{m_i}]^p \right\} = \left\{ [(x_i^{m_i})^p] \right\} = \left\{ [(x_i^p)^{m_i}] \right\} = \prod \langle x_i^p \rangle$$

If we let A^p denote $\mathrm{im}\varphi$ on A, then this shows: $\left(\prod A_i\right)^p = \prod A_i^p$. Also

$$\ker\varphi = \left\{ [x_i^{m_i}] \mid [x_i^{m_i}]^p = 1 \right\}$$

Now $[x_i^{m_i}]^p = 1$ iff $x_i^{m_i p} = 1$ for all i, which is true iff $p^{\alpha_i} | m_i p$ for all i, which is true iff $p^{\alpha_i - 1} | m_i$. Hence $\ker\varphi = \prod\langle x_i^{p^{\alpha_i - 1}}\rangle$ as desired. □

(c) $A/\mathrm{im}\varphi \cong E_{p^n} \cong \ker\varphi$, hence in particular $A/\mathrm{im}\varphi$ and $\ker\varphi$ both have rank n.

Proof. By part (b), $|\ker\varphi| = \prod_{i=1}^n p = p^n$, and $x^p = 1$ for all $x \in \ker\varphi$, hence $\ker\varphi \cong E_{p^n}$. Also

$$A/\mathrm{im}\varphi = \left(\prod A_i\right)/\left(\prod A_i^p\right) \cong \prod (A_i/A_i^p) \cong \prod Z_p = E_{p^n}$$

where the second isomorphism follows since $|A_i^p| = p^{\alpha_i - 1}$. □

EXERCISE 8. Let p be a prime and G be a finite abelian group. Let G^p and G_p denote the image and kernel of the p-th power map, respectively.

(a) $G/G^p \cong G_p$.

Proof. Let $n = |G|$. If p does not divide n, the result is trivial since in this case $G^p = G$ and $G_p = 1$. Hence we assume p divides n. Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, with pairwise distinct primes and $p_1 = p$ (so $p_1^{\alpha_1} > 1$). By Theorem 5, we may write $G = \prod A_i$ where $|A_i| = p_i^{\alpha_i}$ for $1 \le i \le k$. Now $G^p = \prod A_i^p$, and it is easily seen that $A_i^p = A_i$ and $(A_i)_p = 1$ for $i > 1$, hence we have

$$\begin{aligned} G/G^p &= \left(\prod A_i\right)/\left(\prod A_i^p\right) \\ &\cong \prod (A_i/A_i^p) \\ &= (A_1/A_1^p) \times 1 \times \cdots \times 1 \\ &\cong (A_1)_p \times 1 \times \cdots \times 1 && \text{by Exercise 7} \\ &= \prod (A_i)_p \\ &= G_p \end{aligned}$$

Note we may appeal to Exercise 7 since A_1 is a nontrivial abelian p-group. □

EXERCISE 13. Let $A = \prod_{i=1}^r \langle x_i\rangle$ where $|x_i| = n_i$ for $1 \le i \le r$. Let G be any group with commuting elements $g_1, \ldots, g_r$ such that $g_i^{n_i} = 1$ for $1 \le i \le r$. Then there is a unique homomorphism from A to G which maps $x_i \mapsto g_i$.

Proof. Define $\varphi : A \to G$ by $\prod x_i^{\alpha_i} \mapsto \prod g_i^{\alpha_i}$. Note φ is well defined since if $x = y$ for $x, y \in A$, then both x and y (as products of powers of the x_i) can be reduced, using commutativity and the relations $|x_i| = n_i$, to the same expression of the form $\prod_{i=1}^r x_i^{k_i}$ where $0 \le k_i < n_i$ for $1 \le i \le r$. Since the g_i also commute and satisfy the relations $g_i^{n_i} = 1$, the elements $\varphi(x)$ and $\varphi(y)$ can both be reduced to the product $\prod_{i=1}^r g_i^{k_i}$, hence $\varphi(x) = \varphi(y)$.

Clearly $\varphi : x_i \mapsto g_i$ for $1 \le i \le r$, and trivially φ is a homomorphism. Also φ is unique since any homomorphism sending $x_i \mapsto g_i$ for $1 \le i \le r$ must map according to φ. This completes the proof. □

Note this proof uses some of the same reasoning used in the proof that two groups with the same presentations are isomorphic. Also, this proof captures the essence of the proof of the Fundamental Theorem for Finitely Generated Abelian Groups.

EXERCISE 16. No finitely generated abelian group is divisible.

Proof. Let $G = \langle g_1, \dots, g_r \rangle$ be a finitely generated abelian group. If each g_i has finite order, then G is finite and we are done (by Exercise 2.4.19, or directly by noting that for $k = \prod |g_i|$, $g^k = 1$ for all $g \in G$, hence no nontrivial element in G has a k-th root).

If $|g_i| = \infty$, then g_i has no square root, hence G is not divisible. □

Section 4

In the following exercises, for a group G, G' denotes the commutator subgroup of G.

EXERCISE 4,5. $S_4' = A_4$ and $A_4' = V_4$. For all $n \geq 5$, $S_n' = A_n' = A_n$.

Proof. Since S_n is nonabelian but $S_n/A_n \cong Z_2$ which is abelian, $1 < S_n' \leq A_n$. It is easily seen (by looking at the group lattice) that no nontrivial proper subgroup of A_4 is normal in S_4, hence $S_4' = A_4$. For $n \geq 5$, A_n is simple, so $S_n' = A_n$. Note this shows in particular that A_n is characteristic in S_n for all $n \geq 4$.

Since A_4 is nonabelian but $A_4/V_4 \cong Z_3$ is abelian, $1 < A_4' \leq V_4$. Now A_4' char A_4 char S_4, hence A_4' char S_4. No nontrivial proper subgroup of V_4 is characteristic in S_4, hence $A_4' = V_4$. For $n \geq 5$, simplicity of A_n forces $A_n' = A_n$. □

Note for $1 \leq n \leq 3$, we also have $S_n' = A_n$. Also for $1 \leq n \leq 2$, $A_n' = A_n$, but $A_3' = 1$. Thus in particular we obtain: *for all $n \geq 1$, A_n is characteristic in S_n*.

EXERCISE 7. Let P a nonabelian group with $|P| = p^3$ (p prime). Then $P' = Z(P)$.

Proof. Since P is a nontrivial p-group, $Z(P) \neq 1$. Also p^2 does not divide $|Z(P)|$, lest $P/Z(P)$ be cyclic, contradicting that P is nonabelian. Hence $|Z(P)| = p$.

It follows that $|P/Z(P)| = p^2$, hence $P/Z(P)$ is abelian and $P' \leq Z(P)$. Since P is nonabelian, $P' \neq 1$, thus we must have $P' = Z(P)$. □

EXERCISE 10. A finite abelian group is the direct product of its Sylow subgroups.

Proof. Let A be a finite abelian group. Set $n = |A|$ and write $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (where the p_i are pairwise distinct primes). Let A_i be the Sylow subgroup of A with $|A_i| = p_i^{\alpha_i}$. Then $A_i \trianglelefteq A$, and by Lagrange's Theorem, $A_i \cap A_j = 1$ for $i \neq j$. Thus we have

$$A = A_1 \cdots A_k \cong \prod A_i$$

□

EXERCISE 11. Let G be a group and suppose $G = HK$ for characteristic subgroups H, K with $H \cap K = 1$. Then $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.

Proof. Note any automorphism of H or K may be extended to an automorphism of G in a natural way. In this way, identify $\mathrm{Aut}(H)$ and $\mathrm{Aut}(K)$ with their naturally corresponding subgroups of $\mathrm{Aut}(G)$.

Claim $\mathrm{Aut}(H) \trianglelefteq \mathrm{Aut}(G)$. Indeed, for $\sigma \in \mathrm{Aut}(G)$ and $\tau \in \mathrm{Aut}(H)$, $\sigma\tau\sigma^{-1} \in \mathrm{Aut}(G)$, and since H char G, $\sigma\tau\sigma^{-1}$ maps H to itself and is the identity on $G - H$, so $\sigma\tau\sigma^{-1} \in \mathrm{Aut}(H)$. By similar reasoning, $\mathrm{Aut}(K) \trianglelefteq \mathrm{Aut}(G)$. Also $\mathrm{Aut}(H) \cap \mathrm{Aut}(K) = 1$ because $G = HK$ and $H \cap K = 1$. Indeed, if $\sigma \in \mathrm{Aut}(H) \cap \mathrm{Aut}(K)$, then σ is the identity on H (since $\sigma \in \mathrm{Aut}(K)$) and σ is the identity on K (since $\sigma \in \mathrm{Aut}(H)$), hence $\sigma = 1$.

Finally $\mathrm{Aut}(G) = \mathrm{Aut}(H)\mathrm{Aut}(K)$ since for $\sigma \in \mathrm{Aut}(G)$, $\sigma = (\sigma|_H) \circ (\sigma|_K)$ (this also relies on $G = HK$ and $H \cap K = 1$). Hence we have

$$\mathrm{Aut}(G) = \mathrm{Aut}(H)\mathrm{Aut}(K) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$$

□

This result shows that if a group can be factored into disjoint subgroups, each of which is preserved under automorphisms of the group, then any automorphism of the group can be naturally factored into automorphisms of those subgroups.

EXERCISE 17. Let K be a cyclic normal subgroup of G. Then $G' \le C_G(K)$.

Proof. Since $K \trianglelefteq G$, $N_G(K) = G$. Thus $G/C_G(K)$ is isomorphic to a subgroup of $\mathrm{Aut}(K)$, which is abelian since K is cyclic. Thus $G' \le C_G(K)$. □

EXERCISE 18. Let $K_1, \ldots, K_n$ be nonabelian simple groups and set $G = \prod K_i$. If $N \trianglelefteq G$, then $N = G_I$ for some $I \subseteq \{1, \ldots, n\}$.

Proof. Let $N \trianglelefteq G$ and set $N_i = N \cap K_i$. Then $N_i \trianglelefteq K_i$, and so since K_i is simple, $N_i = 1$ or $N_i = K_i$. Note $Z(K_i) = 1$ since $Z(K_i) \trianglelefteq K_i$ but $Z(K_i) \neq K_i$.

Claim $N = \prod N_i$. Indeed, suppose $x = (a_1, \ldots, a_n) \in N$. If $a_i = 1$, trivially $a_i \in N_i$. If $a_i \neq 1$, then (because $a_i \notin Z(K_i)$) there exists $y \in K_i$ with $[a_i, y] \neq 1$. It follows that $1 \neq [x, y] \in N_i$, so $N_i = K_i$ and $K_i \le N$. Thus $x \in \prod N_i$. Since x was arbitrary, $N \le \prod N_i$. The reverse inclusion is trivial.

It follows that $G = G_I$ where $I = \{\, i \mid 1 \le i \le n \text{ and } N_i \neq 1\}$. □

Section 5

For the following exercises, unless otherwise noted, H and K denote arbitrary groups, $\varphi : K \to \mathrm{Aut}(H)$, and $G = H \rtimes_\varphi K$ (with H and K treated as subgroups of G).

EXERCISE 1. $C_K(H) = \ker\varphi$

Proof. From definitions and Theorem 10 we have

$$\begin{aligned}\ker\varphi &= \{\, k \in K \mid \varphi(k) = 1 \,\}\\ &= \{\, k \in K \mid (\forall h \in H)[\varphi(k)(h) = h] \,\}\\ &= \{\, k \in K \mid (\forall h \in H)(khk^{-1} = h) \,\}\\ &= \{\, k \in K \mid (\forall h \in H)(kh = hk) \,\}\\ &= \{\, k \in K \mid k \in C_G(H) \,\}\\ &= K \cap C_G(H) = C_K(H)\end{aligned}$$

□

EXERCISE 2. $C_H(K) = N_H(K)$

Proof. Trivially $C_H(K) \leq N_H(K)$. Conversely suppose $h \in N_H(K)$ and let $k \in K$ be arbitrary. Consider the commutator element $[h,k] = h^{-1}k^{-1}hk$. Since $h \in N_H(K)$, $(h^{-1}k^{-1}h)k \in K$, and since K acts on H by conjugation, $h^{-1}(k^{-1}hk) \in H$. Hence $[h,k] \in H \cap K = 1$, so $[h,k] = 1$ and h and k commute. Since k was arbitrary, $h \in C_H(K)$. Since h was arbitrary, $N_H(K) \leq C_H(K)$, completing the proof. □

EXERCISE 5. Let $G = \mathrm{Hol}(Z_2 \times Z_2)$.

(a) $G = H \rtimes K$ where $H = Z_2 \times Z_2$ and $K \cong S_3$. Thus $|G| = 24$.

Proof. Set $H = Z_2 \times Z_2$ and $K = \mathrm{Aut}(H)$. Then $G = H \rtimes K$ by definition, and so it suffices to prove that $K \cong S_3$. This follows from the observation that there are exactly three elements of order 2 in H (if $H = \langle x \rangle \times \langle x \rangle$, these elements are $(x,1)$, $(1,x)$, and (x,x)), K acts on these elements, and the induced representation is bijective. It follows that $|G| = 4 \cdot 3! = 24$. □

(b) $G \cong S_4$.

Proof. Note $|G : K| = 4$, so the action of G on the coset space G/K induces a representation $\varphi : G \to S_4$. We claim this representation is an isomorphism. Since $|G| = 24 = |S_4|$, it is sufficient to prove φ is faithful, i.e., $\ker\varphi = 1$.

Note $\ker\varphi \leq K$. If $k \in K$, $k \neq 1$, then by definition of the holomorph there exists some $h \in H$ such that $khk^{-1} = k \cdot h \neq h$, that is, h and k do not commute in G. But then we cannot have $k(hK) = hK$, lest in particular $h^{-1}kh \in K$, so (as in the proof of Exercise 2) $[h,k] \in H \cap K = 1$, a contradiction. Thus k acts nontrivially on G/K. Since k was arbitrary nontrivial, $\ker\varphi = 1$ as desired. □

EXERCISE 6 (ISOMORPHIC SEMIDIRECT PRODUCTS). Suppose H is arbitrary, K is cyclic, and φ_1 and φ_2 are homomorphisms from K to $\mathrm{Aut}(H)$ (assumed injective if K is infinite) such that $\varphi_1(K)$ is conjugate to $\varphi_2(K)$. Then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.

Proof. Suppose $\sigma\varphi_1(K)\sigma^{-1} = \varphi_2(K)$. Since K is cyclic, there exists some n such that $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^n$ for all $k \in K$.

Recall that for $h \in H$ and $k \in K$, k acts on h in $H \rtimes_{\varphi_1} K$ by conjugation with $khk^{-1} = \varphi_1(k)(h)$. From our intuitive understanding of conjugation, we know that $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^n = \varphi_2(k^n)$ acts 'in the same way' on $\sigma(h)$, that is, k^n acts 'in the same way' on $\sigma(h)$ in $H \rtimes_{\varphi_2} K$. This suggests the isomorphism

$$\psi : (h,k) \mapsto (\sigma(h), k^n)$$

Indeed, we claim ψ is an isomorphism. First note that ψ is a homomorphism since if (h_1,k_1) and (h_2,k_2) are in $H \rtimes_{\varphi_1} K$, then

$$\begin{aligned}
\psi\big[(h_1,k_1)(h_2,k_2)\big] &= \psi\big(\, h_1\,\varphi(k_1)(h_2)\;,\; k_1k_2\,\big)\\
&= \big(\,\sigma(h_1\,\varphi_1(k_1)(h_2))\;,\;(k_1k_2)^n\,\big)\\
&= \big(\,\sigma(h_1)\sigma\varphi_1(k_1)(h_2)\;,\;k_1^nk_2^n\,\big)\\
&= \big(\,\sigma(h_1)\sigma\varphi_1(k_1)\sigma^{-1}(\sigma(h_2))\;,\;k_1^nk_2^n\,\big)\\
&= \big(\,\sigma(h_1)\varphi_2(k_1^n)(\sigma(h_2))\;,k_1^nk_2^n\,\big)\\
&= (\sigma(h_1),k_1^n)(\sigma(h_2),k_2^n)\\
&= \psi(h_1,k_1)\psi(h_2,k_2)
\end{aligned}$$

We claim that ψ is bijective.

Indeed, if K is infinite, note that $\sigma^{-1}\varphi_2(K)\sigma = \varphi_1(K)$, hence there exists some m such that $\sigma^{-1}\varphi_2(k)\sigma = \varphi_1(k)^m = \varphi_1(k^m)$ for all $k \in K$. This suggests that a two-sided inverse for ψ is given by

$$\psi^* : (h,k) \mapsto (\sigma^{-1}(h), k^m)$$

To prove that it is indeed an inverse, it is sufficient to prove $k^{mn} = k$ for all $k \in K$. We obtain for all $k \in K$

$$\varphi_1(k^{mn}) = \varphi_1(k^n)^m = \sigma^{-1}\varphi_2(k^n)\sigma = \sigma^{-1}(\sigma\varphi_1(k)\sigma^{-1})\sigma = \varphi_1(k)$$

and similarly $\varphi_2(k^{mn}) = \varphi_2(k)$. Thus since φ_1 and φ_2 are injective by hypothesis, we must have $k^{mn} = k$ for all $k \in K$ as desired.

If K is finite,[2] note that since $|\varphi_1(K)| = |\varphi_2(K)|$ we have

$$|\ker\varphi_1| = \frac{|K|}{|\varphi_1(K)|} = \frac{|K|}{|\varphi_2(K)|} = |\ker\varphi_2|$$

Therefore $\ker\varphi_1 = \ker\varphi_2$ since K is cyclic (and hence has a unique subgroup of this order). Now set $N = \ker\varphi_i$, $\overline{K} = K/N$, and let $\overline{\varphi_i} : \overline{K} \to \varphi_i(K)$ be the naturally induced isomorphisms. Also let c_σ denote conjugation by σ. Then $\overline{\varphi} = \overline{\varphi_2}^{-1} c_\sigma \overline{\varphi_1} \in \mathrm{Aut}(\overline{K})$.

[2] For this case I required some assistance from Professor Google.

But there is a natural surjective homomorphism $\mathrm{Aut}(K) \to \mathrm{Aut}(\overline{K})$, hence there is a map $k \mapsto k^r \in \mathrm{Aut}(K)$ whose image is $\overline{\varphi}$. It follows from computation that $c_\sigma(\varphi_1(k)) = \varphi_2(k)^r$ for all $k \in K$, so $n = r$. Thus there exists m such that $(k^n)^m = k$ for all $k \in K$, and hence the map ψ^* above, with this m, is a two-sided inverse of ψ.

Thus in either case ψ is an isomorphism, completing the proof. □

Note in particular if $\varphi_1(K) = \varphi_2(K)$, then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$. It follows from this that, up to isomorphism, *when constructing a semidirect product $H \rtimes K$ with K cyclic, it does not matter which generator of K is chosen to define the action on H*, since in all cases the representation of K will produce the same set of automorphisms. This is a very useful observation when classifying groups.

EXERCISE 7 (GROUPS OF ORDER 56). We classify groups G with $|G| = 56$.

(a) If G is abelian, then G is isomorphic to one of

$$Z_8 \times Z_7 \; (\cong Z_{56}) \qquad Z_2 \times Z_4 \times Z_7 \qquad Z_2 \times Z_2 \times Z_2 \times Z_7$$

Proof. By the Fundamental Theorem. Note $56 = 2^3 \cdot 7$, hence the possible lists of elementary divisors of G are $\{8,7\}$, $\{2,4,7\}$, and $\{2,2,2,7\}$, which correspond to the direct products given above.

Since $(8,7) = 1$, $Z_8 \times Z_7 \cong Z_{56}$ gives the cyclic case. □

(b) G has a normal Sylow 2-subgroup or a normal Sylow 7-subgroup.

Proof. Recall $n_7 \equiv 1(7)$ and $n_7|8$, hence $n_7 = 1$ or $n_7 = 8$. If $n_7 = 1$, the Sylow 7-subgroup is normal. If $n_7 = 8$, then since distinct Sylow 7-subgroups have trivial intersection, there are $(7-1)\cdot 8 = 48$ elements of order 7 in G. This leaves $56 - 48 = 8$ elements remaining, namely the elements in the single, and hence normal, Sylow 2-subgroup. □

(c) We classify nonabelian G with a normal Sylow 7-subgroup.

Note that $G \cong H \rtimes_\varphi K$ where $H \cong Z_7$ (and hence $\mathrm{Aut}(H) \cong Z_6$), $|K| = 8$, and $\varphi : K \to \mathrm{Aut}(H)$. From the classification of groups of order 8 we know K is isomorphic to one of

$$Z_8 \quad Z_2 \times Z_4 \quad Z_2 \times Z_2 \times Z_2 \quad D_8 \quad Q_8$$

We consider these cases in turn and, for each such K, find all possible maps φ (up to a possible choice of generators in K, which does not change the isomorphism type by Exercise 6). In the first three cases we do not consider case $\varphi = 1$ explicitly, since the trivial map gives rise to abelian groups which we have already classified above. Note since $(8,6) = 2$, if $\varphi \neq 1$, then $\varphi(K)$ must be the unique subgroup of $\mathrm{Aut}(H)$ of order 2.

If $K \cong Z_8$, then we must have $\ker\varphi = Z_4$.

If $K \cong Z_2 \times Z_4$, then we must have either $\ker\varphi = Z_4$ or $\ker\varphi = Z_2 \times Z_2$.

If $K \cong Z_2 \times Z_2 \times Z_2$, then we must have $\ker\varphi \cong Z_2 \times Z_2$.

If $K \cong D_8$, then $\ker\varphi$ must be one of D_8, Z_4, or $Z_2 \times Z_2$.

If $K \cong Q_8$, then $\ker\varphi$ must be one of Q_8 or Z_4 (recall there are no subgroups of Q_8 isomorphic to $Z_2 \times Z_2$).

In addition, each one of these cases is realized, and gives rise to a distinct semidirect product type (since for each distinct type of K, the kernels listed are of different types).

Thus there are nine possible isomorphism types for nonabelian G with normal Sylow 7-subgroup.

(d),(e) We classify (nonabelian) G with a nonnormal Sylow 7-subgroup.

We know that G must have a normal Sylow 2-subgroup, so $G \cong H \rtimes_\varphi K$ where $|H| = 8$, $K \cong Z_7$, and $\varphi : K \to \mathrm{Aut}(H)$.

We claim $H \cong Z_2 \times Z_2 \times Z_2$. Indeed, if $k \in Z_7$, $k \neq 1$, then k acts nontrivially on H by conjugation. By the Orbit-Stabilizer Theorem then, the orbit of any element in H moved by k must have order 7. Hence the 7 nonidentity elements in H must all be in a single orbit, and so have the same order. The only possibility is the one stated by the claim.

We know $\mathrm{Aut}(H) \cong GL_3(\mathbb{F}_2)$, so $|\mathrm{Aut}(H)| = 168 = 2^3{\cdot}3{\cdot}7$. Thus in particular there exists an element in $\mathrm{Aut}(H)$ of order 7, so a semidirect product of the current form does exist. In addition, all subgroups of order 7 in $\mathrm{Aut}(H)$ are conjugate by Sylow's Theorem, so by Exercise 6, this gives only one isomorphism type.

It follows from this exercise that there are exactly thirteen distinct isomorphism types for groups of order 56.

EXERCISE 8 (GROUPS OF ORDER 75).

Suppose G is a group with $|G| = 75 = 3 \cdot 5^2$. Recall from Sylow's Theorem that $n_5 \equiv 1(5)$ and $n_5|3$, hence $n_5 = 1$ and the Sylow 5-subgroup of G is normal. It follows that $G \cong H \rtimes_\varphi K$ where $|H| = 5^2$, $K \cong Z_3$, and $\varphi : K \to \mathrm{Aut}(H)$.

Now H is abelian since it has order p^2 ($p = 5$), so H is isomorphic to one of Z_{25} or $Z_5 \times Z_5$. If $\varphi = 1$, G is isomorphic to one of the abelian groups

$$Z_3 \times Z_{25}\ (\cong Z_{75}) \qquad Z_3 \times Z_5 \times Z_5$$

Suppose $\varphi \neq 1$, so $\mathrm{Aut}(H)$ has a subgroup of order 3. Recall $|\mathrm{Aut}(Z_{25})| = 5(5-1) = 2^2 \cdot 5$, so we cannot have $H \cong Z_{25}$ in this case. If $H \cong Z_5 \times Z_5 = E_{5^2}$, then $\mathrm{Aut}(H) \cong GL_2(\mathbb{F}_5)$, so $|\mathrm{Aut}(H)| = (5^2-1)(5^2-5) = 2^5{\cdot}3{\cdot}5$. In particular, $\mathrm{Aut}(H)$ has a subgroup of order 3, and every subgroup of order 3 in $\mathrm{Aut}(H)$ is conjugate (since they are Sylow 3-subgroups). Thus this case is possible, and (by Exercise 6) gives rise to a single nonabelian isomorphism type for G.

EXERCISE 12 (GROUPS OF ORDER 20).

Suppose G is a group with $|G| = 20 = 2^2 \cdot 5$. By Sylow's Theorem, $n_5 \equiv 1(5)$ and $n_5|4$, hence $n_5 = 1$ and $G \cong H \rtimes_\varphi K$ where $H \cong Z_5$, $|K| = 4$ (so $K \cong Z_4$ or $K \cong Z_2 \times Z_2$), and $\varphi : K \to \mathrm{Aut}(H) \cong Z_4$.

If $\varphi = 1$, G is one of the abelian groups $Z_5 \times Z_4$ ($\cong Z_{20}$) or $Z_5 \times Z_2 \times Z_2$.

If $\varphi \neq 1$, then if $K \cong Z_4$, either $\ker\varphi = 1$ and $G \cong \mathrm{Hol}(Z_5)$ or else $\ker\varphi \cong Z_2$. If $K \cong Z_2 \times Z_2$, then we must have $\ker\varphi \cong Z_2$.

Since all of these cases are possible and nonisomorphic, there are exactly five isomorphism types for groups of order 20.

EXERCISE 15 (GROUPS OF ORDER $2p^2$).

Suppose G is a group with $|G| = 2p^2$, p prime. If $p = 2$, then $|G| = 2^3 = 8$, an order which we have already classified, so assume $p \neq 2$. From Sylow's Theorem, $n_p \equiv 1(p)$ and $n_p|2$, hence $n_p = 1$ and $G \cong H \rtimes_\varphi K$ where $|H| = p^2$, $K \cong Z_2$, and $\varphi : K \to \mathrm{Aut}(H)$.

Since H is abelian (order p^2), H is isomorphic to one of Z_{p^2} or $Z_p \times Z_p$. If $\varphi = 1$, G is isomorphic to one of $Z_{p^2} \times Z_2$ ($\cong Z_{2p^2}$) or $Z_p \times Z_p \times Z_2$.

Suppose $\varphi \neq 1$. If $H \cong Z_{p^2}$, then $\mathrm{Aut}(H) \cong Z_{p(p-1)}$, and 2 must divide $p - 1$. Since $Z_{p(p-1)}$ is cyclic, it has a unique subgroup of order 2, hence this case gives rise to a single isomorphism type. Note this case is possible (take $p = 3$).

If $H \cong Z_p \times Z_p = E_{p^2}$, then $\mathrm{Aut}(H) \cong GL_2(\mathbb{F}_p)$. We claim that in $GL_2(\mathbb{F}_p)$, every element of order 2 is conjugate (similar) to one of

$$\begin{bmatrix} 1 & \\ & -1 \end{bmatrix} \qquad \begin{bmatrix} -1 & \\ & -1 \end{bmatrix}$$

Note that this is equivalent to proving that for any $A \in GL_2(\mathbb{F}_p)$ with $|A| = 2$, there is a change of basis under which A becomes one of the above. (Note that since $p \neq 2$, and hence $2 \neq 0$, the two matrices above are not conjugate, since the one at right has no eigenvectors but the one at left does.)

Suppose $A \in GL_2(\mathbb{F}_p)$ with $|A| = 2$. Note[3] that for any $v \in Z_p^2$,

$$A(v + Av) = Av + A^2 v = Av + v = v + Av$$
$$A(v - Av) = Av - A^2 v = Av - v = -(v - Av)$$

Let (v, w) be a basis for the space. Note it cannot be true that both $v + Av$ and $v - Av$ are in the span of w, lest

$$v = \frac{1}{2}((v + Av) + (v - Av))$$

is also in the span of w, contradicting the linear independence of (v, w). (Note the above equation relies on the fact that $p \neq 2$, so $2 \neq 0$ and $1/2$ is defined.) Let v^* be whichever is not in the span of w. Then (v^*, w) is a basis and $Av^* = \pm v^*$. Similarly there is w^* with $Aw^* = \pm w^*$ such that (v^*, w^*) is a basis of the space. This proves the conjugacy claim above.

It follows that there are at most two (and at least one, taking say $p = 3$) possible isomorphism types for G in this case.

[3] For the following observations I required some assistance from Professor Google.

EXERCISE 18. Let H be any group. There exists a group G containing H as a normal subgroup such that any automorphism of H is witnessed as an inner automorphism in G (restricted to H).

Proof. Take $G = \mathrm{Hol}(H) = H \rtimes \mathrm{Aut}(H)$. □

EXERCISE 19 (HOLOMORPHS AS NORMALIZERS). Let H be a finite group with $|H| = n$, $K = \mathrm{Aut}(H)$, and $G = \mathrm{Hol}(H) = H \rtimes K$. Let G act on the coset space G/K by left multiplication with representation $\pi : G \to S_n$ (since $|G : K| = n$).

(a) The elements of H are coset representatives in G/K, and if we identify H and G/K, $\pi|_H$ is just the left regular representation of H.

Proof. Let $h_1, h_2 \in H$. If $h_1K = h_2K$, then $h_2^{-1}h_1K = K$, so $h_2^{-1}h_1 \in H \cap K = 1$, and hence $h_1 = h_2$. Thus we may identify H and G/K by the natural projection $h \mapsto hK$. Trivially then $\pi|_H$ is just the left regular representation of H. □

(b) $N_{S_n}(\pi(H)) = \pi(G)$. Therefore in general the normalizer of the (left) regular representation of a group H is isomorphic to $\mathrm{Hol}(H)$.

Proof. Note $\pi(H) \trianglelefteq \pi(G)$ since $H \trianglelefteq G$, hence $\pi(G) \leq N(\pi(H))$. Because H is finite, it is sufficient to prove that $|\pi(G)| = |N(\pi(H))|$.

We need $|N(\pi(H))| \leq |\pi(G)|$.

Recall $N(\pi(H))/C(\pi(H))$ is isomorphic to a subgroup of $\mathrm{Aut}(\pi(H))$. Since π is injective, $\mathrm{Aut}(\pi(H)) \cong \mathrm{Aut}(H) = K$. By Exercise 4.3.36, $C(\pi(H)) \cong H$. Hence

$$\frac{|N(\pi(H))|}{|H|} \quad \text{divides} \quad |K|$$

Thus $|N(\pi(H))|$ divides $|H||K| = |G|$, so $|N(\pi(H))| \leq |\pi(G)|$ as desired.

Thus $N(\pi(H)) = \pi(G) \cong G = \mathrm{Hol}(H)$. The general result follows from (a). □

(c) The normalizer of a group generated by an n-cycle in S_n is isomorphic to $\mathrm{Hol}(Z_n)$ and has order $n\varphi(n)$.

Proof. If σ is the n-cycle and $Z_n = \langle x \rangle$, the map $x \mapsto \sigma$ realizes $\langle \sigma \rangle$ as a (left) regular representation of Z_n under some numbering of Z_n. Thus by part (b), $N_{S_n}(\sigma) \cong \mathrm{Hol}(Z_n) = Z_n \rtimes \mathrm{Aut}(Z_n)$, and since $|\mathrm{Aut}(Z_n)| = \varphi(n)$, $|N_{S_n}(\sigma)| = n\varphi(n)$. □

Note this exercise shows how holomorphs arise naturally from permutation groups. Also, this and Exercise 4.3.36 together give us characterizations of the centralizers and normalizers of regular permutation representations.

EXERCISE 23 (WREATH PRODUCT). Let K and L be groups with $\rho : K \to S_n$ for some positive integer n.

Let $H = \prod^n L$ and $\varphi : K \to \mathrm{Aut}(H)$ be naturally induced from ρ by letting the elements of K permute the factors of H (see Exercise 1.8). Then the *wreath product* of L by K is defined by

$$L \wr K = H \rtimes_\varphi K$$

If ρ is not mentioned, it is assumed to be the left regular representation of (finite) K.

(a) Suppose K and L are finite. Then $|L \wr K| = |L|^{|K|}|K|$. *Proof:* Immediate.

(b) Let p be a prime. Then $Z_p \wr Z_p$ is a nonabelian group of order p^{p+1} isomorphic to a subgroup of S_{p^2}.

Proof. The group $Z_p \wr Z_p$ is nonabelian since the left regular representation of Z_p is nontrivial, and has order p^{p+1} by (a).

The p copies of Z_p in the direct product can be seen as producing a grid of p^2 elements, with the elements of each factor arranged in vertical columns. The wreath product $Z_p \wr Z_p$ acts naturally on this grid as follows: the element $(x_1^{\alpha_1}, \cdots, x_p^{\alpha_p}, x_{p+1}^{\alpha_{p+1}})$ cyclically permutes the elements in column i by α_i for $1 \le i \le p$, and then cyclically permutes the columns themselves by α_{p+1}. We thus obtain a faithful representation $Z_p \wr Z_p \to S_{p^2}$, so $Z_p \wr Z_p$ is isomorphic to a subgroup of S_{p^2}. □

Note examples like (b) might shed some light on the name 'wreath product'. In that example, each of the factors in the direct product can be seen as a little circle, and the factors themselves are cyclically permuted in a larger circle.

Chapter 6

Section 1

EXERCISE 1. Let G be a group. Then $Z_i(G)$ char G for all i.

Proof. We proceed by induction on i.

Case $i = 0$: $Z_0(G) = 1$ char G.

Case $i = 1$: $Z_1(G) = Z(G)$, and we claim $Z(G)$ char G. Indeed, fix $\sigma \in \mathrm{Aut}(G)$ and suppose $x \in Z(G)$ and $g \in G$. Let $\sigma(h) = g$. Then

$$g\sigma(x) = \sigma(h)\sigma(x) = \sigma(hx) = \sigma(xh) = \sigma(x)\sigma(h) = \sigma(x)g$$

Letting g vary we see $\sigma(x) \in Z(G)$, then letting x vary we see $\sigma[Z(G)] \subseteq Z(G)$. Now substituting σ^{-1} for σ, we have $\sigma^{-1}[Z(G)] \subseteq Z(G)$, so $Z(G) = \sigma[\sigma^{-1}[Z(G)]] \subseteq \sigma[Z(G)]$, so $\sigma[Z(G)] = Z(G)$. Since σ was arbitrary, $Z(G)$ char G as claimed.

Now if $Z_i(G)$ char G for some $i \ge 1$, set $\overline{G} = G/Z_i(G)$. If $\sigma \in \mathrm{Aut}(G)$, σ naturally induces a map

$$\begin{aligned} \overline{\sigma} : \overline{G} &\to \overline{G} \\ \overline{g} &\mapsto \overline{\sigma(g)} \end{aligned}$$

This map is well-defined since if $\overline{x} = \overline{y}$, that is, $xZ_i(G) = yZ_i(G)$, then

$$\overline{\sigma(x)} = \sigma(x)Z_i(G) = \sigma[xZ_i(G)] = \sigma[yZ_i(G)] = \sigma(y)Z_i(G) = \overline{\sigma(y)}$$

where the second and fourth equalities hold since $Z_i(G)$ char G. It is immediate that $\overline{\sigma}$ is a homomorphism, and $\overline{\sigma^{-1}}$ is a two-sided inverse of $\overline{\sigma}$, hence $\overline{\sigma} \in \mathrm{Aut}(\overline{G})$.

Now it follows from the reasoning above that $\overline{\sigma}[Z(\overline{G})] = Z(\overline{G})$. We claim that $\sigma[Z_{i+1}(G)] = Z_{i+1}(G)$. Indeed, recall by definition $\overline{Z_{i+1}(G)} = Z(\overline{G})$. Thus if $g \in Z_{i+1}$, then $\overline{g} \in Z(\overline{G})$, hence $\overline{\sigma(g)} = \overline{\sigma}(\overline{g}) \in Z(\overline{G})$, that is, $\sigma(g) \in Z_{i+1}$. Since g was arbitrary, $\sigma[Z_{i+1}(G)] \subseteq Z_{i+1}(G)$, and as above it follows that $\sigma[Z_{i+1}(G)] = Z_{i+1}(G)$ as claimed.

Thus Z_{i+1} char G. By induction, the result is true for all i. □

Exercise 2,4,5 (Nilpotent Groups are Like p-Groups). Let G be nilpotent.

(a) If $1 < H \trianglelefteq G$, then $H \cap Z(G) \neq 1$. In particular, if $G \neq 1$, then $Z(G) \neq 1$.[4]

Proof. If $H \leq Z(G)$, the result holds, so assume that $H \not\leq Z(G)$. Then we have $Z(G) < HZ(G) \trianglelefteq G$, so by the Lattice Theorem $\overline{1} < \overline{H} \trianglelefteq \overline{G}$ where $\overline{G} = G/Z(G)$. By induction on nilpotence class, we may assume $\overline{H} \cap Z(\overline{G}) \neq \overline{1}$. Now it follows from the Lattice Theorem again that $HZ(G) \cap Z_2(G) \not\leq Z(G)$, which implies $H \cap Z_2(G) \neq 1$. Since $H \trianglelefteq G$, $[G,H] \leq H$ (Proposition 5.7(2)), and by definition of $Z_2(G)$, $[G, Z_2(G)] \leq Z(G)$. Therefore we have $[G, H \cap Z_2(G)] \leq H \cap Z(G)$. If $[G, H \cap Z_2(G)] \neq 1$, the result holds, otherwise that means $H \cap Z_2(G) \leq Z(G)$, so again $H \cap Z(G) \neq 1$ and the result holds. □

(b) If $H < G$, then $H < N_G(H)$.

Proof. Suppose $H < G$. If $Z(G) \not\leq H$, then $H < \langle H, Z(G)\rangle \leq N_G(H)$. If $Z(G) \leq H$, set $\overline{G} = G/Z(G)$. By the Lattice Theorem, $\overline{H} < \overline{G}$. Since $Z(G) \neq 1$, by induction on nilpotence class we may assume $\overline{H} < N_{\overline{G}}(\overline{H})$. Then since $\overline{N_G(H)} = N_{\overline{G}}(\overline{H})$, $H < N_G(H)$ by the Lattice Theorem. □

(c) If G is finite and $M \leq G$ is maximal, then $|G : M| = p$ for some prime p.

Proof. Suppose G is finite and M is a maximal subgroup of G. Then $M \trianglelefteq G$ by Proposition 7, hence $\overline{G} = G/M$ is defined and $|G : M| = |\overline{G}|$. Note $|\overline{G}| > 1$ since $M < G$. If $|\overline{G}|$ is composite, then (by Cauchy's Theorem, say) there exists a subgroup $\overline{1} < \overline{H} < \overline{G}$, so $M < H < G$ by the Lattice Theorem, contradicting the maximality of M. Therefore $|\overline{G}|$ is prime, as desired. □

Together with the fact that all p-groups are nilpotent (Proposition 2), these results exhibit strong connections between p-groups and nilpotent groups in general. For this reason it is often convenient to think about (simpler) p-groups when working with nilpotent groups.

[4] For this problem, I required some assistance from Professor Google.

EXERCISE 3. Let G be a finite group. Then G is nilpotent iff G has a normal subgroup of every order dividing $|G|$, and G is cyclic iff G has a unique subgroup of every order dividing $|G|$.

Proof. If G has a normal subgroup of every order dividing $|G|$, then in particular G has a normal (and hence unique) Sylow p-subgroup for all primes p dividing $|G|$. Thus all Sylow p-subgroups of G are normal, so G is nilpotent by Theorem 3.

Conversely, if G is nilpotent, write $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (p_i prime), so by Theorem 3 $G = P_1 \times \cdots \times P_k$ where $P_i \in \mathrm{Syl}_{p_i}(G)$. If n divides $|G|$, write $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$. Then by Theorem 1(3), we know each P_i has a normal subgroup N_i with $|N_i| = p_i^{\beta_i}$. Now set $N = N_1 \times \cdots \times N_k$. Then $N \trianglelefteq G$ and $|N| = n$, as desired.

If G is cyclic, we know G has a unique subgroup of each order dividing $|G|$ by Theorem 2.7(3). To prove the converse, we exhibit for any noncyclic G two distinct subgroups having the same order. So consider an arbitrary noncyclic group G. If G is abelian, then by the fundamental theorem and Proposition 5.6(2), we must be able to write G as a direct product of cyclic groups where, for some prime p, at least two of the factors are nontrivial p-groups. From these p-groups we can select elements of order p which generate distinct subgroups of order p.

If G is nilpotent but not abelian, proceed by induction. Note $G/Z(G)$ is also nilpotent but not cyclic, lest G be abelian. Hence we may assume $G/Z(G)$ contains distinct subgroups of the same order. The complete preimages of these subgroups in G are distinct subgroups of G of the same order.

Finally if G is not nilpotent, then by Theorem 3 at least one of its Sylow subgroups is nonnormal and hence not unique. Therefore in all cases, G has distinct subgroups of the same order. □

EXERCISE 6. G is nilpotent iff $G/Z(G)$ is nilpotent.

Proof. Set $\overline{G} = G/Z(G)$. We first establish a natural relationship between the upper central series in G and the upper central series in $\overline{G}$:

$$\overline{Z_{i+1}(G)} = Z_i(\overline{G}) \qquad (i \geq 0)$$

To prove this, we proceed by induction on i. The result is immediate for cases $i = 0, 1$. If the result holds for some $i \geq 1$, we claim that the result also holds for $i+1$, that is, $\overline{Z_{i+2}(G)} = Z_{i+1}(\overline{G})$. Note both $\overline{Z_{i+2}(G)}$ and $Z_{i+1}(\overline{G})$ are subgroups of $\overline{G}$. Our idea is to choose $N \trianglelefteq \overline{G}$ with $N \leq \overline{Z_{i+2}(G)} \cap Z_{i+1}(\overline{G})$ such that $\overline{Z_{i+2}(G)}/N = Z_{i+1}(\overline{G})/N$, so that our claim then follows from the Lattice Theorem.

Choose $N = Z_i(\overline{G})$. Then $N \trianglelefteq \overline{G}$ and $N \leq Z_{i+1}(\overline{G})$. By hypothesis, $N = \overline{Z_{i+1}(G)}$, and since $Z_{i+1}(G) \leq Z_{i+2}(G)$, we have $N \leq \overline{Z_{i+2}(G)}$ by the Lattice Theorem. Now

$$\begin{aligned} Z_{i+1}(\overline{G})/N &= Z_{i+1}(\overline{G})/Z_i(\overline{G}) \\ &= Z(\overline{G}/Z_i(\overline{G})) && \text{by definition of } Z_{i+1}(\overline{G}) \\ &= Z(\overline{G}/\overline{Z_{i+1}(G)}) \end{aligned}$$

On the other hand, $\overline{Z_{i+2}(G)}/N = \overline{Z_{i+2}(G)}/\overline{Z_{i+1}(G)}$. Therefore we must prove that $\overline{Z_{i+2}(G)}/\overline{Z_{i+1}(G)} = Z(\overline{G}/\overline{Z_{i+1}(G)})$.

We know that $Z_{i+2}(G)/Z_{i+1}(G) = Z(G/Z_{i+1}(G))$ by definition of $Z_{i+2}(G)$. And by the Third Isomorphism Theorem, $\overline{G}/\overline{Z_{i+1}(G)} \cong G/Z_{i+1}(G)$. Using this isomorphism, and the fact that centers are preserved under isomorphism, it can be seen that the required equality holds.

Therefore our claim holds for $i+1$. By induction, our result holds for all $i \geq 0$.

Returning to the problem, note for $i \geq 0$ that $Z_{i+1}(G) = G$ iff $Z_i(\overline{G}) = \overline{G}$ by our result and the Lattice Theorem. Hence G is nilpotent iff $\overline{G}$ is nilpotent, as desired. □

Note the proof gives us more information: for $n > 0$, G is of nilpotence class $n+1$ iff $G/Z(G)$ is of nilpotence class n.

EXERCISE 7. Let G be nilpotent. If $H \leq G$, then H is nilpotent. If $H \trianglelefteq G$, then G/H is also nilpotent.

Proof. We use the lower central series characterization of nilpotence.

Suppose $H \leq G$. We claim $H^i \leq G^i$ for $i \geq 0$. Indeed, $H^0 = H \leq G = G^0$. If $i \geq 0$ and $H^i \leq G^i$, then by definitions it follows that

$$H^{i+1} = [H, H^i] \leq [G, G^i] = G^{i+1}$$

Thus the claim holds for all $i \geq 0$ by induction. Since G is nilpotent, $G^n = 1$ for some n, so $H^n = 1$ and H is nilpotent.

Suppose now $\varphi : G \to K$ is a surjective homomorphism. We claim $\varphi[G^i] = K^i$ for $i \geq 0$. Note $\varphi[G^0] = \varphi[G] = H = H^0$ since φ is surjective. If $i \geq 0$ and $\varphi[G^i] = H^i$, then

$$\varphi[G^{i+1}] = \varphi[[G, G^i]] = [\varphi[G], \varphi[G^i]] = [H, H^i] = H^{i+1}$$

The second equality follows since if $x \in G$ and $y \in G^i$, then $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ by the definition of the commutator. Hence the claim holds for all $i \geq 0$ by induction. Since G is nilpotent, $G^n = 1$ for some n, hence $K^n = 1$ and K is nilpotent. Thus we see that the homomorphic image of a nilpotent group is nilpotent.

If $H \trianglelefteq G$, then G/H is the homomorphic image of G under a natural projection, so G/H is nilpotent. □

It is not true in general that if $H \trianglelefteq G$ is nilpotent and G/H is nilpotent, then G is nilpotent. Indeed, S_3 is not nilpotent, but $\langle(123)\rangle \trianglelefteq S_3$ is cyclic, hence abelian and nilpotent, and $S_3/\langle(123)\rangle$ is cyclic of order 2, hence also nilpotent. This differentiates nilpotent groups from solvable groups (Proposition 10(3)).

EXERCISE 8. Let p be prime and P a nonabelian group of order p^3. Then $|Z(P)| = p$ and $P/Z(P) \cong Z_p \times Z_p$.

Proof. We know that $|Z(P)| = p^\alpha$ for $0 \leq \alpha \leq 3$ by Lagrange's Theorem, and $\alpha > 0$ by Theorem 1(1). If $\alpha > 1$, then $P/Z(P)$ is cyclic, contradicting that P is nonabelian. Therefore $|Z(P)| = p$, and $|P/Z(P)| = p^2$. Since every group of order p^2 is abelian, $P/Z(P)$ is abelian, and either $P/Z(P) \cong Z_{p^2}$ or $P/Z(P) \cong Z_p \times Z_p$ (Corollary 4.9). The first case is impossible since P is nonabelian, hence $P/Z(P) \cong Z_p \times Z_p$ as desired. □

Exercise 9. Let G be finite. Then G is nilpotent iff for all $x, y \in G$ if $(|x|, |y|) = 1$ then $xy = yx$.

Proof. Suppose G is nilpotent. By Theorem 3(4), we may assume $G = P_1 \times \cdots \times P_k$ where $P_i \in \mathrm{Syl}_{p_i}(G)$ for $1 \le i \le k$. If $x, y \in G$ with $(|x|, |y|) = 1$, write $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$, so $|x| = \mathrm{lcm}(|x_1|, \ldots, |x_k|)$ and $|y| = \mathrm{lcm}(|y_1|, \ldots, |y_k|)$. If $x_i \neq 1$, then $y_i = 1$, lest p_i is a common divisor of $|x_i|$ and $|y_i|$, hence also of $|x|$ and $|y|$. Thus $x_i y_i = y_i x_i$ for all $1 \le i \le k$, so $xy = yx$ as desired.

Conversely, suppose $xy = yx$ for all $x, y \in G$ with $(|x|, |y|) = 1$. Let $H < G$. Since G is finite, $|H| < |G|$, and thus by Cauchy's Theorem we may choose $x \in G$ with $|x| = p$ for some prime p not dividing $|H|$. If $y \in H$, then y divides $|H|$, so $(|x|, |y|) = 1$, and hence by assumption $xy = yx$. Since y was arbitrary, this shows $x \in C_G(H) \le N_G(H)$, and hence $H < N_G(H)$. Since H was arbitrary, G is nilpotent by Theorem 3(2). □

Exercise 10. D_{2n} is nilpotent iff n is a power of 2.

Proof. Suppose n is a power of 2 and write $n = 2^k$. Since D_{2n} is trivially nilpotent for $k \le 1$, we may assume $k > 1$. By Exercise 2.2.7, $Z(D_{2n}) = \{1, r^{2^{(k-1)}}\}$, hence by Exercise 3.1.34, $D_{2n}/Z(D_{2n}) \cong D_{2\cdot 2^{k-1}}$. Now by induction we may assume $D_{2\cdot 2^{k-1}}$ is nilpotent, hence D_{2n} is nilpotent by Exercise 6.

Conversely, suppose n is not a power of 2. Then $p|n$ for some prime $p \neq 2$, and $x = r^{(n/p)}$ is an element in D_{2n} of order p. Now x is not in $Z(D_{2n})$, hence x cannot commute with s (since x commutes with r), but $(|x|, |s|) = (p, 2) = 1$. Therefore D_{2n} is not nilpotent by Exercise 9. □

Exercise 12. We find the upper and lower central series for A_4 and S_4.

Proof. By definition $Z_0(A_4) = 1$, and by examining the lattice of A_4 (Exercise 3.5.8) and checking conjugates (Proposition 4.10), we see $Z_1(A_4) = 1$. Hence $Z_n(A_4) = 1$ for all $n \ge 0$. Similarly, $Z_0(S_4) = 1$, and by constructing conjugates we see $Z_1(S_4) = 1$, hence $Z_n(S_4) = 1$ for all $n \ge 0$ as well. This establishes the two upper central series.

To find the lower central series of A_4, note by definition $A_4^0 = A_4$. Recall from the lattice and Exercise 3.5.9 that $V_4 \trianglelefteq A_4$. Now $A_4/V_4 \cong Z_3$ is abelian, hence by definition and Proposition 5.7(4), $A_4^1 = [A_4, A_4] \le V_4$. Since A_4^1 is characteristic in A_4 (Exercise 14), $A_4^1 = V_4$ or $A_4^1 = 1$, but since A_4 is not abelian, we must have $A_4^1 = V_4$. Now $A_4^2 = [A_4, V_4]$, so again the only possibilities are $A_4^2 = V_4$ or $A_4^2 = 1$. But it is easy to check that not everything in V_4 commutes with everything in A_4 (that is, $V_4 \nleq Z(A_4) = 1$), hence $A_4^2 = V_4$. It follows that $A_4^n = V_4$ for all $n \ge 1$.

Similarly $S_4^0 = S_4$, and since $A_4 \trianglelefteq S_4$ and $S_4/A_4 \cong Z_2$ is abelian, we must have $S_4^1 = [S_4, S_4] \le A_4$. Now $V_4 = [A_4, A_4] \le [S_4, S_4]$, but it is easy to check that $V_4 \ntrianglelefteq S_4$, hence $S_4^1 = A_4$. We then have $S_4^2 = [S_4, A_4]$, so again $V_4 \le S_4^2 \le A_4$, so again we must have $S_4^2 = A_4$. It follows that $S_4^n = A_4$ for all $n \ge 1$.

In particular, these results show that neither A_4 nor S_4 is nilpotent. □

Note by this exercise and Exercise 3.5.10, A_4 is solvable but not nilpotent.

EXERCISE 13. We find the upper and lower central series for A_n and S_n, for $n \geq 5$.

Proof. Fix $n \geq 5$. Recall A_n is simple (Theorem 4.24), that is, A_n has no nontrivial proper normal subgroups. We know that $Z_0(A_n) = 1$. By Exercise 14, we must have $Z_1(A_n) = 1$ or $Z_1(A_n) = A_n$. But A_n is not abelian, hence $Z_1(A_n) = 1$ and it follows that $Z_k(A_n) = 1$ for all $k \geq 0$. It is trivial that $Z_k(S_n) = 1$ for all $k \geq 0$.

We know $A_n^0 = A_n$, and since A_n is simple, $A_n^1 = A_n$ or $A_n^1 = 1$. Again since A_n is not abelian, we must have $A_n^1 = A_n$, and it follows that $A_n^k = A_n$ for all $k \geq 0$. Now $S_n^0 = S_n$, but $A_n \trianglelefteq S_n$ and $S_n/A_n \cong Z_2$ is abelian, hence $S_n^1 \leq A_n$. Since S_n is not abelian, the simplicity of A_n forces $S_n^1 = A_n$. Now $S_n^2 = [S_n, A_n] \leq A_n$. Again by the simplicity of A_n, and the fact that $A_n \not\leq Z(S_n) = 1$, we must have $S_n^2 = A_n$. It follows that $S_n^k = A_n$ for all $n \geq 1$.

In particular, these results show that neither A_n nor S_n is nilpotent. □

EXERCISE 14,17. Let G be a group. For all $i \geq 0$, G^i char G and $G^{(i)}$ char G.

Proof. By induction. Trivially $G^0 = G^{(0)} = G$ char G. If G^i char G and $G^{(i)}$ char G, let $\sigma \in \mathrm{Aut}(G)$. Then

$$\begin{aligned}
\sigma[G^{i+1}] &= \sigma[[G, G^i]] && \text{by definition of } G^{i+1}\\
&= [\sigma[G], \sigma[G^i]] && \text{by definition of commutators}\\
&= [G, G^i] && \text{by induction}\\
&= G^{i+1} && \text{by definition of } G^{i+1}
\end{aligned}$$

Similarly $\sigma[G^{(i+1)}] = G^{(i+1)}$. Since σ was arbitrary, this shows that G^{i+1} char G and $G^{(i+1)}$ char G. By induction, the result holds for all $i \geq 0$. □

EXERCISE 16. $\mathbb{Q}$ has no maximal subgroups.

Proof. Suppose towards a contradiction that $H < \mathbb{Q}$ is maximal. Fix $q \in \mathbb{Q} - H$. Then by maximality of H, we have $H < \langle H, q\rangle = \mathbb{Q}$. If $r \in \mathbb{Q}$ is arbitrary, then $r = \alpha q + h$ for some $\alpha \in \mathbb{Z}$ and $h \in H$.

Write $q/2 = \alpha q + h$ for $\alpha \in \mathbb{Z}$ and $h \in H$. Then $(1 - 2\alpha)q = 2h \in H$, and hence $|1 - 2\alpha| q \in H$ (since H is a subgroup). Note $1 - 2\alpha \neq 0$ since $\alpha \in \mathbb{Z}$, so $|1 - 2\alpha| > 0$ and there exists a positive integral multiple of q in H. Let $\mu \in \mathbb{Z}$ be least positive with $\mu q \in H$. By choice of q, $\mu > 1$. We claim that the cosets

$$H,\ q + H,\ \ldots,\ (\mu - 1)q + H$$

partition $\mathbb{Q}$. Indeed, if $r \in \mathbb{Q}$, write $r = \beta q + h'$. By division with remainder, $\beta = \rho + \delta\mu$ for some $\delta, \rho \in \mathbb{Z}$ with $0 \leq \rho < \mu$. Hence

$$r = \beta q + h' = (\rho + \delta\mu)q + h' = \rho q + (\delta\mu q + h') = \rho q + h''$$

where $h'' = \delta\mu q + h' \in H$. Thus $r + H = \rho q + (h'' + H) = \rho q + H$, so since $0 \leq \rho \leq \mu - 1$, $r + H$ is one of the cosets above. Since r was arbitrary, this establishes the claim.

But we know $\mathbb{Q}$ has no proper subgroups of finite index (Exercise 3.2.21), so this is a contradiction. Thus $\mathbb{Q}$ has no maximal subgroups. □

EXERCISE 20. Let G be finite, $P \in \mathrm{Syl}_p(G)$, and $N \trianglelefteq G$ with $(|N|, p) = 1$.

(a) $\overline{N_G(P)} = N_{\overline{G}}(\overline{P})$

Proof. Note $N < NP$ and $\overline{NP} = \overline{P}$, so by the Lattice Theorem

$$\overline{N_G(NP)} = N_{\overline{G}}(\overline{NP}) = N_{\overline{G}}(\overline{P})$$

We claim $NN_G(P) = N_G(NP)$, so that $\overline{N_G(P)} = \overline{NN_G(P)} = \overline{N_G(NP)} = N_{\overline{G}}(\overline{P})$, establishing the desired result.

Indeed, note that $NP \trianglelefteq N(NP)$ and $P \in \mathrm{Syl}_p(NP)$ since p does not divide $|N|$. Therefore by Frattini's Argument, $NN_G(P) = (NP)N_G(P) = N_G(NP)$, which is precisely the claim. □

Note the lattice of G naturally suggests $NN_G(P) = N_G(NP)$: this just means the chain $N \le NP \le N_G(NP)$ is the lifting by N of the chain $1 \le P \le N_G(P)$. Also, this proof shows the utility of Frattini's Argument: knowing $P \le NP \trianglelefteq N_G(NP)$ with P a Sylow subgroup of NP, we use the fact that P is "somewhat normal" in $N_G(NP)$ to lift $N_G(P)$ up to $N_G(NP)$.

For a group G, the *Frattini subgroup* $\Phi(G)$ of G is defined to be the intersection of all maximal subgroups of G (if G has no maximal subgroups, $\Phi(G) = G$). The following exercises establish some basic properties of the Frattini subgroup.

EXERCISE 21. Let G be a group. Then $\Phi(G)$ char G.

Proof. If $\sigma \in \mathrm{Aut}(G)$ and M is maximal in G, then $\sigma[M]$ is maximal in G. Therefore

$$\sigma[\Phi(G)] = \sigma[\bigcap_M M] = \bigcap_M \sigma[M] = \Phi(G)$$

where M varies over maximal subgroups of G. Since σ was arbitrary, $\Phi(G)$ char G. □

EXERCISE 24. Let G be a group. Call an element $x \in G$ a *nongenerator* if for all $H < G$, $\langle H, x\rangle < G$. Then $\Phi(G) = \{x \in G \mid x \text{ is a nongenerator}\}$.

Proof. If $x \notin \Phi(G)$, then there exists some maximal $M < G$ such that $x \notin M$. But then $M < \langle M, x\rangle = G$ by maximality of M, hence x is not a nongenerator.

Conversely, if x is not a nongenerator, there exists $H < G$ with $\langle H, x\rangle = G$. Now if $H \le M < G$ with M maximal, then $x \notin M$ lest $G = \langle H, x\rangle \le M < G$, a contradiction. Therefore we assume H is not contained in a maximal subgroup, so for all K with $H \le K < G$, we may choose $C(K)$ with $K < C(K) < G$. Set $C(G) = G$. Now define recursively on the ordinals

$$\begin{aligned} H_0 &= H \\ H_{\alpha^+} &= C(H_\alpha) \\ H_\lambda &= \bigcup_{\alpha<\lambda} H_\alpha \quad (\lambda \text{ a limit ordinal}) \end{aligned}$$

By induction, this forms an ascending chain of subgroups in G, and there must exist a limit ordinal μ with $G = \bigcup_{\alpha<\mu} H_\alpha$ and $H \le H_\alpha < G$ for all $\alpha < \mu$. Now $x \in \bigcup_{\alpha<\mu} H_\alpha$, hence $x \in H_\alpha$ for some $\alpha < \mu$. But then $G = \langle H, x\rangle \le H_\alpha < G$, a contradiction. Hence this case is impossible, so $x \notin \Phi(G)$ by the previous case. □

EXERCISE 25. Let G be a finite group. Then $\Phi(G)$ is nilpotent.

Proof. Let $P \in \mathrm{Syl}_p(\Phi(G))$. We claim that $P \trianglelefteq \Phi(G)$. Indeed, by Frattini's argument (Proposition 6), $G = \Phi(G)N_G(P)$. Now if $N_G(P) < G$, then $N_G(P) \le M < G$ for some maximal subgroup M. But then since $\Phi(G) \le M$, we have $G = \Phi(G)N_G(P) \le M < G$—a contradiction. Therefore $P \trianglelefteq G$, so in particular $P \trianglelefteq \Phi(G)$ as claimed. Since P was arbitrary, $\Phi(G)$ is nilpotent by Theorem 3(3). □

EXERCISE 26 (BURNSIDE'S BASIS THEOREM). Let p be prime, P be a finite p-group, and $\overline{P} = P/\Phi(P)$.[5]

(a) $\overline{P}$ is elementary abelian.

Proof. If M is maximal in P, then $M \trianglelefteq P$ and $|P : M| = p$ by Theorem 1(5), hence P/M is cyclic of order p. It follows that $P' \le M$ (by Proposition 5.7(4)) and $x^p \in M$ (that is, $\overline{x}^p = \overline{1}$) for all $x \in P$. Since M was arbitrary, $P' \le \Phi(P)$ and $x^p \in \Phi(P)$ for all $x \in P$, hence $P/\Phi(P)$ is elementary abelian. □

(b) If $N \trianglelefteq P$ and P/N is elementary abelian, then $\Phi(P) \le N$.

Proof. Write $\widetilde{P} = P/N$. Note $\Phi(\widetilde{P}) = 1$ since $\widetilde{P}$ is elementary abelian (indeed, write $\widetilde{P} = \prod Z_p$, and obtain maximal subgroups by dropping a Z_p factor from each position). Now

$$\widetilde{\Phi(P)} = \widetilde{\bigcap_M M} \le \bigcap_M \widetilde{M} = \Phi(\widetilde{P}) = \widetilde{1}$$

where M varies over maximal subgroups of P. Hence $\Phi(P) \le N$. □

(c) *Burnside's Basis Theorem*: The set $\{y_1, \dots, y_k\}$ is a minimal generating set for P iff $\{\overline{y_1}, \dots, \overline{y_k}\}$ is a basis of $\overline{P}$ (as a vector space over $\mathbb{F}_p$).

Proof. First we claim $\{y_1, \dots, y_k\}$ generates P iff $\{\overline{y_1}, \dots, \overline{y_k}\}$ spans $\overline{P}$. Indeed, the forward direction is immediate. Conversely, if $\{\overline{y_1}, \dots, \overline{y_k}\}$ spans $\overline{P}$, then by the Lattice Theorem, $P = \langle y_1, \dots, y_k\rangle\Phi(P)$. But since $\Phi(P)$ consists of non-generators (Exercise 24), this implies $P = \langle y_1, \dots, y_k\rangle$ as claimed.

It follows that the size of a minimal generating set is the same for both P and $\overline{P}$. Since a minimal generating set in $\overline{P}$ is just a basis of $\overline{P}$ (with size equal to the dimension of $\overline{P}$), the desired result follows. □

(d) If $\overline{P}$ is cyclic, P is cyclic. Moreover, if P/P' is cyclic, P is cyclic.

[5] For this exercise, I required some assistance from Professor Google.

Proof. If $\overline{P}$ is cyclic, then $\overline{P}$ is spanned by a single element, so by Burnside's Basis Theorem, P is generated by a single element, that is, P is cyclic.

If P/P' is cyclic, then $P' = \Phi(P)$ by parts (a) and (b), hence $\overline{P}$ is cyclic, and P is cyclic by the previous case. □

For a group G, a *minimal normal subgroup* of G is a subgroup M with $1 < M \trianglelefteq G$ such that there do not exist any subgroups N with $1 < N < M$ and $N \trianglelefteq G$.

EXERCISE 31. Let G be a finite solvable group and suppose M is a minimal normal subgroup of G. Then M is an elementary abelian p-group for some prime p.

Proof. By Proposition 10(1), M is solvable, hence $M' < M$. But M' char $M \trianglelefteq G$, hence $M' \trianglelefteq G$. By minimality of M, this means $M' = 1$, so M is abelian.

Let p divide $|M|$ and set $M_p = \{x \in M \mid x^p = 1\}$. Then M_p is a subgroup of M since M is abelian (Exercise 5.2.8), and it is immediate that M_p char M, hence $M_p \trianglelefteq G$. Since $M_p \neq 1$ (by Cauchy's Theorem, say), $M_p = M$, hence M is elementary abelian. □

EXERCISE 32. Let G be a finite solvable group and M be a maximal subgroup of G. Then M has prime power index.

Proof. Let N be a minimal normal subgroup of G and set $\overline{G} = G/N$.

If $N \leq M$, then by the Lattice Theorem, $\overline{M}$ is maximal in $\overline{G}$ and $|G : M| = |\overline{G} : \overline{M}|$ is a prime power by induction. If $N \not\leq M$, then $M < MN = G$ by maximality of M, so by the Diamond Isomorphism Theorem, $|G : M| = |N : M \cap N|$, which is a prime power since N is elementary abelian (Exercise 31). □

The previous two exercises show that the 'top' and 'bottom' of a finite solvable group have a relatively simple structure.

Section 2

In the following exercises, for a group G, $\mu(G)$ denotes the minimal possible index of a proper subgroup in G (cf. p. 203).

EXERCISE 1. Let G be a group, $P \in \mathrm{Syl}_p(G)$, and suppose for all $Q \in \mathrm{Syl}_p(G)$ with $P \neq Q$, $P \cap Q = 1$. Then for all $P_1, P_2 \in \mathrm{Syl}_p(G)$ with $P_1 \neq P_2$, $P_1 \cap P_2 = 1$. Therefore the number of nonidentity elements of p-power order in G is $(|P| - 1)|G : N_G(P)|$.

Proof. Let $P_1, P_2 \in \mathrm{Syl}_p(G)$ with $P_1 \neq P_2$. By Sylow's Theorem, write $P_1 = gPg^{-1}$ and $P_2 = hPh^{-1}$ with $g, h \in G$ and $h^{-1}g \notin P$. Now suppose towards a contradiction that $P_1 \cap P_2 \neq 1$, so there exist $x, y \in P$ with $gxg^{-1} = hyh^{-1} \neq 1$. But then

$$1 \neq (h^{-1}g)x(h^{-1}g)^{-1} = y \in P \cap (h^{-1}g)P(h^{-1}g)^{-1}$$

This contradicts that P has trivial intersection with distinct Sylow p-subgroups. Thus $P_1 \cap P_2 = 1$ as desired. The computational result follows trivially. □

EXERCISE 4. There are no simple groups of order 80.

Proof. Suppose $|G| = 80 = 2^4 \cdot 5$. By Sylow's Theorem, $n_5 \equiv 1(5)$ and $n_5 | 2^4$. If $n_5 = 1$, G has a nontrivial proper normal Sylow 5-subgroup, so G is not simple. If $n_5 \neq 1$, then $n_5 = 16$, so the number of elements of order 5 is $(5-1) \cdot 16 = 64$. This leaves $80 - 64 = 16$ elements in G, hence we must have $n_2 = 1$, so again G is not simple. □

EXERCISE 5. Let G be a solvable group with $|G| = pm$, p prime and $(p, m) = 1$. If $P \in \mathrm{Syl}_p(G)$ and $N_G(P) = P$, then G has a normal subgroup of order m.

Proof. Note $n_p = |G : N_G(P)| = m$, hence the number of elements of order p in G is $(p-1) \cdot m = pm - m$. This leaves m remaining elements in G. Since G is solvable, there exists $M \leq G$ with $|M| = m$ (Hall). By Lagrange's Theorem, M has no elements of order p. Therefore M consists of precisely the remaining elements, and hence $M \trianglelefteq G$ as desired. □

EXERCISE 6. There are no simple groups of order 4125.

Proof. Suppose G is simple with $|G| = 4125 = 3 \cdot 5^3 \cdot 11$. Note $\mu(G) \geq 15$. Now $n_5 \equiv 1(5)$, $n_5 | 3 \cdot 11$, and $n_5 > 1$. But then $n_5 = 11 < 15$, a contradiction. □

EXERCISE 8. There are no simple groups of order 792.

Proof. Suppose G is simple with $|G| = 792 = 2^3 \cdot 3^2 \cdot 11$. Then $n_{11} \equiv 1(11)$, $n_{11} | 2^3 \cdot 3^2$, and $n_{11} > 1$, hence $n_{11} = 12$. By simplicity then we may assume $G \leq S_{12}$. Now let $P \in \mathrm{Syl}_{11}(G)$. Note (p. 204) $|N_{S_{12}}(P)| = 11 \cdot (11-1) = 2 \cdot 5 \cdot 11$. But $|N_G(P)| = 2 \cdot 3 \cdot 11$, contradicting that $N_G(P) \leq N_{S_{12}}(P)$ by Lagrange's Theorem. □

EXERCISE 10. There are no simple groups of order 4095.

Proof. Suppose G is simple with $|G| = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$. Then by computation, $n_{13} = 3 \cdot 5 \cdot 7$ and $n_7 = 3 \cdot 5$. Let $P \in \mathrm{Syl}_7(G)$. Then $|N_G(P)| = 3 \cdot 7 \cdot 13$. Note $n_{13}(N_G(P)) = 1$, hence if $Q \in \mathrm{Syl}_{13}(N_G(P))$, then $Q \trianglelefteq N_G(P)$, so $3 \cdot 7 \cdot 13$ divides $|N_G(Q)|$. But also $Q \in \mathrm{Syl}_{13}(G)$, hence $|N_G(Q)| = 3 \cdot 13$—a contradiction. □

EXERCISE 14. There are no simple groups of order 144.

Proof. Suppose G is simple with $|G| = 144 = 2^4 \cdot 3^2$. Note $\mu(G) \geq 6$. By computation then, we must have $n_3 = 16$. If Sylow 3-subgroups have pairwise trivial intersection, then the number of nontrivial elements of 3-power order in G is $(9-1) \cdot 16$, leaving only 16 remaining elements in G and forcing $n_2 = 1$—a contradiction.

Therefore we may choose $P, Q \in \mathrm{Syl}_3(G)$ with $|P \cap Q| = 3$. Set $R = P \cap Q$. Then $R \trianglelefteq P$ and $R \trianglelefteq Q$, hence $P, Q \leq N_G(R)$. This implies that 3^2 divides $|N_G(R)|$ and $n_3(N_G(R)) > 1$. Since $n_3(N_G(R)) \equiv 1(3)$ and $n_3(N_G(R))$ divides 2^4, $n_3(N_G(R)) = 2^2$ and hence 2^2 must also divide $|N_G(R)|$. But then $|G : N_G(R)|$ divides 4, contradicting the value of $\mu(G)$. □

Section 3

EXERCISE 1. Let $F(R)$ and $F(S)$ be free groups. Then $F(R) \cong F(S)$ iff $|S| = |R|$.

Proof. First suppose $\varphi : S \to R$ is a bijection. We may naturally regard this as an injection $\varphi : S \to F(R)$, so by the universal property there exists $\Phi : F(S) \to F(R)$ with $\Phi|_S = \varphi$. Note that Φ is a bijection, so Φ witnesses as isomorphism $F(S) \cong F(R)$.

Now suppose conversely $\Phi : F(S) \cong F(R)$. We merely sketch an idea: by methods analogous to those in elementary vector space theory, we might be able to argue that any minimal generating set of $F(R)$ has the same cardinality as R, hence since S is mapped bijectively to such a set under Φ, $|S| = |R|$. □

EXERCISE 2. $F(S)$ is abelian iff $|S| = 1$.

Proof. If $|S| = 1$, then $F(S)$ is cyclic and hence abelian. If $|S| > 1$, choose $a, b \in S$ with $a \neq b$. Then by definition of products in $F(S)$, $[a, b] = a^{-1}b^{-1}ab \neq 1$, hence a and b do not commute, so $F(S)$ is nonabelian. □

EXERCISE 4. Every nonidentity element in $F(S)$ has infinite order.

Proof. Again trivial by definition of products in $F(S)$. □

EXERCISE 5. We give a presentation for A_4 using two generators. Set $\sigma = (123)$ and $\tau = (124)$. We know from the lattice that $A_4 = \langle \sigma, \tau \rangle$. Note $\sigma^3 = \tau^3 = (\sigma\tau)^2 = 1$. The latter relation implies that $\tau\sigma = \sigma^{-1}\tau^{-1}$, so (as in the dihedral group) these relations allow us to reduce any element of A_4 to a specific form $\sigma^i \tau^j$ where $0 \leq i, j < 3$. Thus any relations in A_4 may be derived from these three relations. It follows that

$$A_4 = \langle \sigma, \tau \mid \sigma^3 = \tau^3 = (\sigma\tau)^2 = 1 \rangle$$

EXERCISE 11. Let S be a set and $R = \langle [s, t] \mid s, t \in S \rangle$. Then $A(S) = \langle S \mid R \rangle$ is called the *free abelian group* on S. If G is abelian and $\varphi : S \to G$ is any set map, then there exists a unique homomorphism $\Phi : A(S) \to G$ such that $\Phi|_S = \varphi$.

In particular, if $|S| = n$, then $A(S) \cong \prod^n \mathbb{Z}$.

Proof. Note we could simply define the homomorphism directly as in Theorem 17. Alternately, note by the universal property of free groups that there exists a unique $\Phi : F(S) \to G$ with $\Phi|_S = \varphi$. Since G is abelian, $R \leq \ker\Phi$, hence if N is the normal closure of R, $N \leq \ker\Phi$. Therefore we obtain a natural sequence

$$A(S) = F(S)/N \longrightarrow F(S)/\ker\Phi \longrightarrow G$$

The composite homomorphism $A(S) \to G$ is φ on S, and is unique with this property.

If $|S| = n$, we can map the elements of S bijectively to the 1's in the factors of $\prod^n \mathbb{Z}$. The resulting homomorphism $A(S) \to \prod^n \mathbb{Z}$ is easily seen to be an isomorphism. □