1 Binary operations (09/20)

This course is about the theory of groups. Groups are sets equipped with extra structure, a binary operation, which satisfies certain conditions, namely associativity, the existence of an identity, and the existence of inverses.

Definition 1.1 (Products)**.** Let S be a set. The **product** of S with itself, written $S \times S$, is the set of ordered pairs (a, b) where a and b are in S. Elements of $S \times S$ are often called **ordered tuples**.

Definition 1.2 (Binary operations)**.** A binary operation on a set S is a function $m\colon S \times S \to S$. For $a, b \in S$ we will often write $a \cdot b$ or even ab for $m(a, b)$. This is multiplicative notation. We will also have occasion to use additive notation and write $a + b$ for $m(a, b)$.

Definition 1.3 (Properties of binary operations)**.** Let $m\colon S \times S \to S$ be a binary operation on a set S, written $m(a, b) = a \cdot b$.

(a) We say m is **commutative** if $a \cdot b = b \cdot a$ for all $a, b \in S$.

(b) We say m is **associative** if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in S$.

(c) We say m is **unitary** if there exists a (two-sided) **identity element**, which is an element $e \in S$ such that $e \cdot a = a = a \cdot e$ for all $a \in S$. If m is unitary, then the identity element e is unique; see Lemma 1.5.

(d) We say m has the **Latin square property** if for each $a, b \in S$ there exist unique $x, y \in S$ such that $a \cdot x = b$ and $y \cdot a = b$.

(e) We say that a *unitary* binary operation m has **inverses** if for each $a \in S$ there exists $b \in S$ such that $a \cdot b = b \cdot a = e$ for an identity element e (which is unique by Lemma 1.5). Such an element b is called a (two-sided) **inverse** of a and is written as a^{-1}. Inverses are unique if m is additionally associative by Exercise 1.3.

Example 1.4. Binary operations can be very simple, too simple to be of interest. For example, let $\mathbf{Z}$ be the **set of integers**. Define $m\colon \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ by setting $m(a, b) = 17$ for all integers a, b. In the notation above, we let $a \cdot b = 17$ for all $a, b \in \mathbf{Z}$. This is a binary operation, which is commutative and associative, but not terribly useful.

Lemma 1.5 (Identities are unique)**.** *Suppose that m is a unitary binary operation on a set S. If e and e' are identity elements, then $e = e'$.*

Proof. We have $e = e \cdot e' = e'$, where the first equality uses the identity property of e' and the second equality uses the identity property of e. □

Notation 1.6. We will sometimes write 1 for the identities with respect to binary operations when writing multiplicatively; and we will sometimes write 0 for the identities with respect to binary operation written additively. Similarly, we might write $-a$ for the inverse of a when writing additively.

Remark 1.7 (Commutative diagrams)**.** Associativity can be expressed as follows. Let $m \times \mathrm{id}_S\colon S \times S \times S \to S \times S$ be defined by $(m \times \mathrm{id}_S)(a, b, c) = (m(a, b), c)$ and let $\mathrm{id}_S \times m\colon S \times S \times S \to S \times S$ be defined by $(\mathrm{id} \times m)(a, b, c) = (a, m(b, c))$. The functions $m \circ (m \times \mathrm{id}_S)$ and $m \circ (\mathrm{id} \times m)$ define two functions on the set $S \times S \times S$ of ordered triples of elements of S. (These might be called ternary operations.) The binary

operation m is associative if these two functions are equal. In contemporary mathematics, it is common to express this via a **commutative diagram**. In this case, the diagram would be as follows:

$$\begin{array}{ccc} S \times S \times S & \xrightarrow{m \times \mathrm{id}_S} & S \times S \\ \Big\downarrow{\scriptstyle \mathrm{id}_S \times m} & & \Big\downarrow{\scriptstyle m} \\ S \times S & \xrightarrow[m]{} & S. \end{array}$$

Saying that the diagram is commutative amounts to asserting that the two ways of traversing the diagram from the upper left to the bottom right by composing functions result in the same function $S \times S \times S \to S$. Commutative diagrams need not be square. For example, let $t\colon S \times S \to S \times S$ be defined by $t(a, b) = (b, a)$. Commutativity is the statement that the following triangular diagram commutes:

$$\begin{array}{ccc} S \times S & \xrightarrow{t} & S \times S \\ & {\scriptstyle m} \searrow \quad \swarrow {\scriptstyle m} & \\ & S, & \end{array}$$

which means that $m \circ t = m$.

Remark 1.8. If m is a binary operation on S satisfying the Latin square property, then the multiplication table of m is a Latin square: each element of S appears exactly once in each row and column. In the context of binary operations, these are called Cayley tables. For example, the Latin square of Figure 1 can be viewed

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table 1: A Cayley table, which in this case represents a Latin square (the bottom right 3×3 part of the table).

as the "addition table" of a binary operation m on the set $S = \{0, 1, 2\}$.

Example 1.9. Let $\mathbf{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$ be the set of **natural numbers**, which we take to be the non-negative integers. On $\mathbf{N}$ we have the binary operation of addition, given by $m(a, b) = a + b$. This binary operation is commutative, associative, and unital; it has neither the Latin square property nor inverses.

Example 1.10. Let $\mathbf{Z}$ be the set of integers. On $\mathbf{Z}$ the binary operation of addition has all of the properties (a)-(e) of Definition 1.3. We can also multiply integers: the binary operation of multiplication satisfies properties (a)-(c) but not (d) or (e).

Example 1.11. We can construct Cayley tables for the outcomes of simple games. For example, consider the two-player game of rock, paper, scissors. The plays are denoted by r, p, and s. The outcomes of possible plays are listed in Figure 2. For example, if $p \cdot s = s = s \cdot p$ represents the fact that scissor beats paper, no matter who plays it. Now, consider

$$(r \cdot p) \cdot s = p \cdot s = s \quad \text{and} \quad r \cdot (p \cdot s) = r \cdot s = r,$$

which shows that this commutative binary operation is not associative.

$\cdot$	r	p	s
r	r	p	r
p	p	p	s
s	r	s	s

Table 2: A Cayley table for rock, paper, scissors. The associated binary operation is commutative, but not associative.

1.1 Exercises

Exercise 1.1. If S and I are sets, let S^I be the set of functions $f\colon I \to S$. Let $I = \{0, 1\}$. Prove that for any set S there is a bijection $p\colon S^I \to S \times S$.

Exercise 1.2. Let $S = \{1, \dots, n\}$ for some positive integer n. Compute the number of binary operations on S.

Exercise 1.3. Show that if m is a unital, associative binary operation on a set S, then inverses are unique when they exist: if $a \in S$ and $x, y \in S$ are inverses of a, then $x = y$.

Exercise 1.4 (The Eckmann–Hilton argument)**.** Let S be a set with two binary operations $\bullet$ and $\circ$ satisfying the following two axioms:

(i) $\bullet$ and $\circ$ each has a two-sided identity element, $\mathbf{1}_\bullet$ and $\mathbf{1}_\circ$, respectively;

(ii) for each $a, b, c, d \in S$, there is the identity $(a \circ b) \bullet (c \circ d) = (a \bullet c) \circ (b \bullet d)$.

Prove that (a) $\mathbf{1}_\bullet = \mathbf{1}_\circ$, (b) $\bullet = \circ$, (c) $\bullet$ is associative, and (d) $\bullet$ is commutative.

Exercise 1.5. Find a binary operation which is not commutative and not associative.

2 Groups (09/22)

Algebraic structures are sets equipped with additional structures, often binary operations, which satisfy certain properties and are viewed as being part of the data of the algebraic structure.

Definition 2.1 (Magmas)**.** A **magma** M is a pair $(S, \cdot)$ where S is a set and $\cdot$ is a binary operation on S. The binary operation could also be written as $+$ or $\bullet$ or $\star$, etc.

Notation 2.2. It is very convenient to write M for the magma *and* the underlying set. So, a magma M will be a set M equipped with a binary operation on M. This is an abuse of notation, but is harmless and will make everything a bit prettier.

Remark 2.3. While a set has varying binary operations, a magma has a single binary operation which is singled out and viewed as fixed.

Definition 2.4 (Types of magmas)**.** In general, one can say that a magma is commutative, associative, unital, and so forth if its binary operation has that property. In many cases, magmas possessing these properties have special names.

(a) A **semigroup** is an associative magma.

(b) A **monoid** is a unital semigroup (a unital associative magma).

(c) A **group** is a monoid which has inverses (a unital associative magma with inverses).

(d) An **abelian group** is a group whose underlying magma is commutative.[1]

(e) A **quasigroup** is a magma with the Latin square property.

(f) A **loop** is a unital quasigroup.

This course will focus on the theory of groups, although monoids are also sometimes useful.

Definition 2.5. A **finite group** is a group whose underlying set is finite.

Example 2.6. The set $\mathbf{N} = \{0, 1, 2, \cdots\}$ of natural numbers is a commutative monoid under addition. It is not a group.

Example 2.7. The set $\mathbf{Z} = \{0, \pm 1, \pm 2, \cdots\}$ of integers under addition is an abelian group. Unless otherwise specified, when we speak of $\mathbf{Z}$ we will always mean this particular group.

Warning 2.8. There is another natural binary operation on $\mathbf{Z}$: multiplication. Under this operation, $(\mathbf{Z}, \cdot)$ is a commutative monoid, but it is not a group. Taken together, the triple $(\mathbf{Z}, +, \cdot)$ forms a **ring**: a set with an abelian group structure under $+$, a monoid structure under $\cdot$, and where $+$ and $\cdot$ interact in a prescribed way via the **distributivity laws**: $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$. This particular ring is commutative because the multiplicative monoid is. These algebraic structures are the subject of the second quarter of this sequence.

Example 2.9. The sets $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, and $\mathbf{R}^n$ under (vector) addition are abelian groups.

Example 2.10. If k is a field and V is a k-vector space, then addition makes V into an abelian group.

Example 2.11. If $G = \{e\}$ is a set with a single element, e, then the unique binary operation on G (specified by $e \cdot e = e$) makes G into a group (with identity element e).

[1] One could call these commutative groups, but for historical reasons, abelian groups are used instead.

Example 2.12. The empty set $\emptyset$ also admits a unique binary operation $\emptyset \times \emptyset \to \emptyset$. It is commutative, associative, and has the Latin square property, but is not unital as unitality asserts the existence of an element. So, it is a semigroup and a quasigroup, but it is not a group.

Now, we introduce two of the most important examples of groups: addition modulo N and symmetric groups.

Lemma 2.13. *Fix a positive integer $N \geqslant 1$. Let $\mathbf{Z}/N$ be the set $\{0, 1, \ldots, N-1\}$. The binary operation on $\mathbf{Z}/N$ defined by letting $a +_N b = r$ where r is the unique integer in $\{0, \ldots, N-1\}$ such that $a + b \equiv r \mod N$ makes $\mathbf{Z}/N$ into an abelian group.*

Proof. The existence and uniqueness of c follows from the fact that for $c \in \mathbf{Z}$ there are unique integers q and $r \in \{0, \ldots, N-1\}$ such that $c = qN + r$ (this is often called **Euclidean division**). Applying this to $c = a + b$ (where the sum is computed in $\mathbf{Z}$) produces q and r such that $a + b = qN + r$. We define $a +_N b = r$. This operation is commutative since $a + b = b + a = qN + r$, so $a +_N b = b +_N a$ and unital since $a + 0 = 0 + a = 0 \cdot N + a = a$ for $a \in \{0, \ldots, N-1\}$, so $a +_N 0 = 0 +_N a = a$. The inverse of a is computed by finding $r \in \{0, \ldots, N-1\}$ such that $-a = qN + r$. Then, $0 = a + r = a + qN + r$ is divisible by N so that $a + r = N$ and hence $a + r = (q+1)N + 0$, so $a +_N r = 0$. Thus, $+_N$ has inverses. For associativity, suppose that $a + b = q_0 N + r_0$ and $b + c = q_1 N + r_1$, where $r_0, r_1 \in \{0, \ldots, N-1\}$. Then, assume that $r_0 + c = q_2 N + r_2$ and $a + r_1 = q_3 N + r_3$ for $r_2, r_3 \in \{0, \ldots, N-1\}$. Then, by associativity of addition on $\mathbf{Z}$,

$$(q_1 + q_3)N + r_3 = a + q_1 N + r_1 = a + b + c = q_0 N + r_0 + c = (q_0 + q_1)N + r_2.$$

By uniqueness of the remainder, we must have $r_3 = r_2$, so that $a +_N (b +_N c) = (a +_N b) +_N c$, which proves associativity and finally that $\mathbf{Z}/N$ is an abelian group. □

Notation 2.14. We will typically write $a + b \equiv c \mod N$ instead of $a +_N b = c$ when working in $\mathbf{Z}/N$.

Example 2.15. The Cayley table of $\mathbf{Z}/3$ was already introduced in Remark 1.8. We reproduce it here for convenience.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table 1: The Cayley table of $\mathbf{Z}/3$.

2.1 Exercises

Exercise 2.1. An associative loop is a group. Show that there exist non-associative loops.

Exercise 2.2. Let G be a group and fix $a \in G$. Prove that $(a^{-1})^{-1} = a$.

Exercise 2.3. Let G be a group and fix $a, b \in G$. Prove that $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Exercise 2.4. Let G be a group with identity element e and fix $a \in G$ and $n \in \mathbf{Z}$. Set $a^0 = e$. For $n > 0$, define a^n inductively by $a^n = a \cdot a^{n-1}$. For $n < 0$, define $a^n = (a^{-n})^{-1}$. One has $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ for $m, n \in \mathbf{Z}$. Prove that if G is abelian, then $(a \cdot b)^n = a^n \cdot b^n$ for all $a, b \in G$.

Exercise 2.5. Let G be a finite group with identity element e. Show that there exists an integer $n > 0$ such that $a^n = e$ for all $a \in G$.

3 Symmetric groups (09/25)

Lemma 3.1. *Let X be a set. Let S_X be the set of bijections $f\colon X \to X$. On S_X we define a binary operation via $f \circ g$, the composition of f and g. This makes S_X into a group.*

Proof. Let $\mathrm{id}_X\colon X \to X$ be the function $\mathrm{id}_X(x) = x$ for all $x \in X$. This is an identity element for S_X. Indeed, if $f\colon X \to X$ is another function, then $(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x) = \mathrm{id}_X(f(x)) = (\mathrm{id}_X \circ f)(x)$ for all $x \in X$, so $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$.[1] Associativity follows from the fact that $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x)$. Finally, the existence of inverses follows because each $f \in S_X$ is a bijection; the inverse of f is the inverse function f^{-1}. □

Definition 3.2. The group S_X is called the **group of permutations of** X. When $X = \{1, \dots, n\}$, we write S_n for S_X. This is called the **permutation group on** n **symbols** or the **symmetric group of degree** n. We write e for the identity element of S_n.

Lemma 3.3. *The symmetric group S_n on degree n has $n! = n(n-1)(n-2)\cdots 1$ elements for $n \geqslant 1$.*[2]

Proof. We prove the result by induction. Let s_n be the number of bijections from a set with n elements to another set with n elements. We want to show $s_n = n!$. When $n = 1$, this is true because there is exactly 1 function from a set with 1 element to another set with 1 element. Now, suppose the result is true for $1, \dots, n-1$. In particular, $s_{n-1} = (n-1)!$. To specify a bijection $f\colon \{1, \dots, n\} \to \{1, \dots, n\}$, we must choose $f(1)$. Let $Y = \{1, \dots, n\} - \{f(1)\}$. Then, the rest of the values of f are determined by a bijective function $f'\colon \{2, \dots, n\} \to Y$. There are n choices of $f(1)$ and for each such choice $s_{n-1} = (n-1)!$ for f'. Thus, there are $n \cdot (n-1)! = n!$ bijections f, so $s_n = n!$, as desired. □

Definition 3.4. Fix $n \geqslant 1$ and consider the symmetric group S_n of degree n. A **cycle** of order k is an ordered string $(a_1\, a_2 \cdots a_k)$ where $a_1, \dots, a_k \in \{1, \dots, n\}$ are distinct. We view a cycle as a bijection $\sigma = (a_1 \cdots a_k)\colon \{1, \dots, n\} \to \{1, \dots, n\}$, and hence as an element of S_n, by letting

$$\sigma(x) = \begin{cases} a_{k+1} & \text{if } x = a_1, \dots, a_{k-1}, \\ a_1 & \text{if } x = a_k, \text{ and} \\ x & \text{otherwise.} \end{cases}$$

In words, $\sigma = (a_1 \cdots a_k)$ is the function which takes a_1 to a_2, a_2 to a_3 and so on, all the way to a_k to a_1. It does not change other elements.

Example 3.5. If $i \in \{1, \dots, n\}$, then the cycle (i) of length 1 is equal to the identity element of S_n.

Example 3.6. Recall that if G is a group and $a \in G$, then **the order of** a, if it exists, is the least integer $k \geqslant 1$ such that $a^k = e$. Write $|a| = k$ for the order of a. (Written additively, this would be the least $n \geqslant 1$ such that $na = 0$.) If $f = (a_1 \cdots a_k)$ is a cycle, then its order is k.

Definition 3.7. A **transposition** is a cycle $(a\, b)$ of length 2. If $f = (a\, b)$, then $f^2 = e$, so $f^{-1} = f$.

Proposition 3.8. *If X is a set with at least 3 elements, then S_X is not abelian. In particular, if $n \geqslant 3$ be an integer, then S_n is not abelian.*

[1] We use throughout that two functions f and g from X to Y are equal if and only if $f(x) = g(x)$ for all $x \in X$.

[2] It also makes sense to write S_0 for $S_\emptyset$; this group has 1 element.

Proof. We can assume that X contains the set $\{1,2,3\}$. We compute the compositions

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

These cycles represent different functions on $\{1,\dots,n\}$, so $(1\,2)\circ(2\,3) \neq (2\,3)\circ(1\,2)$. (Here, as in Definition 3.4, the cycles given act as the identity away from $\{1,2,3\}$.) □

Remark 3.9. Note that as an element of S_n there is no difference between $(a_1\,a_2\,\cdots\,a_n)$ and $(a_2\,a_3\,\cdots\,a_n\,a_1)$. But, as in the previous proof, if two cycles $(a_1\,\cdots\,a_k)$ and $(b_1\,\cdots\,b_m)$ start with the same element $a_1 = b_1$, then they are the same if and only if $m = k$ and $b_i = a_i$ for $1 \leqslant i \leqslant k$.

Lemma 3.10 (Disjoint cycles commute)**.** *Suppose that $f = (a_1\,\cdots\,a_k)$ and $g = (b_1\,\cdots\,b_m)$ are disjoint cycles, meaning that $a_i \neq b_j$ for all $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant m$. Then, $f \circ g = g \circ f$.*

Proof. Fix $x \in \{1,\cdots,n\}$. If x is not in $\{a_1,\dots,a_k\}$, then $f(x) = x$ and $g(x)$ is also not in $\{a_1,\dots,a_k\}$ so that $(f\circ g)(x) = f(g(x)) = g(x) = g(f(x)) = (g\circ f)(x)$. The same holds if x is not in $\{b_1,\dots,b_m\}$. But, the union of the complements of $\{a_1,\dots,a_k\}$ and $\{b_1,\dots,b_m\}$ is all of $\{1,\dots,n\}$. So, $f\circ g$ and $g\circ f$ are equal on all of $\{1,\dots,n\}$ and hence are equal. □

Notation 3.11. Since disjoint cycles commute, if $(a_1\,\cdots\,a_k)$ and $(b_1\,\cdots\,b_m)$ are disjoint cycles, we write $(a_1\,\cdots\,a_k)(b_1\,\cdots\,b_m)$ for their composition, in any order. Thus, for example, $(1\,2)(3\,4) = (1\,2)\circ(3\,4) = (3\,4)\circ(1\,2)$. We also make this convention for compositions of multiple pairwise disjoint cycles.

3.1 Exercises

Exercise 3.1. Let $f = (a_1\,\cdots\,a_k)$ be a cycle of length k in S_n. Write the inverse of f as a cycle.

Exercise 3.2. Let $f = (a_1\,\cdots\,a_k)$ be a cycle of length k in S_n. Prove that f has order k.

Exercise 3.3. Let $f = (a_1\,\cdots\,a_k)$ be a cycle of length k in S_n. Fix $s \geqslant 1$. Find (and prove) necessary and sufficient conditions for f^s to be a cycle. Hint: first consider the case of $s = 2$.

Exercise 3.4. Let $\mathbf{Z}/N = \{0,\dots,N-1\}$. Equip $\mathbf{Z}/N$ with the binary operation given by multiplication modulo N, so that if $a, b \in \mathbf{Z}/N$, then $a \cdot_N b = r$ where $ab = qN + r$ where $r \in \{0,\cdots,N-1\}$. We write $ab \equiv r \mod N$.

(a) Show that this binary operation makes $\mathbf{Z}/N$ into a commutative monoid with identity element 1.

Let $(\mathbf{Z}/N)^\times \subseteq \mathbf{Z}/N$ be the subset of elements $a \in \mathbf{Z}/N$ such that there exists $b \in \mathbf{Z}/N$ with $ab \equiv ba \equiv 1 \mod N$.

(b) Show that $(\mathbf{Z}/N)^\times$ is an abelian group.

(c) Show that $(\mathbf{Z}/N)^\times$ consists of the elements of $\mathbf{Z}/N$ which are relatively prime to N.

4 Cycle decomposition in cyclic groups (09/27)

Theorem 4.1 (Cycle decomposition)**.** *Let $f \in S_n$ be an element of S_n. Then, for some $1 \leqslant r \leqslant n$ there are r pairwise disjoint cycles $(a_{11} \cdots a_{1,k_1}), (a_{21} \cdots a_{2,k_2}), \ldots, (a_{r1}, \ldots, a_{r,k_r})$ such that*

$$f = (a_{11} \cdots a_{1,k_1}) \cdots (a_{r1} \cdots a_{r,k_r}).$$

Proof. As $\{1, \ldots, n\}$ is finite, there is some smallest $k \geqslant 1$ for which $f^{(k)}(1) = 1$. Then, $(1\, f(1)\, f(f(1) \cdots f^{(k-1)}(1))$ is a cycle of length k. Let this be $(a_{11} \cdots a_{1,k_1})$. Let a_{21} be the first element in $\{1, \ldots, n\}$ not in the cycle $(a_{11} \cdots a_{1,k_1})$ and consider the cycle generated by a_{21}, say $(a_{21} \cdots a_{2,k_2})$. This is a disjoint cycle. Continue on in this way until every element of $\{1, \ldots, n\}$ appears in a cycle. □

Remark 4.2. As cycles of length 1 all correspond to the identity element of S_n it is standard to omit them from the final cycle decomposition of f. The cycle decomposition of f is unique up to cyclically rotating the terms in the cycles (Remark 3.9) and reordring the cycles themselves (Lemma 3.10).

Example 4.3. If $f = (a_{11} \cdots a_{1,k_1}) \cdots (a_{r1} \cdots a_{r,k_r})$ is a decomposition of f into disjoint cycles, then the order of f is the least common multiple of $k_1, \ldots, k_r$. For example, if $f = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)$, then $|f| = 30$.

Recall the following definition from last time.

Definition 4.4. A **transposition** is a cycle $(a\, b)$ of length 2. If $f = (a\, b)$, then $f^2 = e$, so $f^{-1} = f$.

Lemma 4.5. *Every element $f \in S_n$ can be written as a product of transpositions.*

Proof. Using cycle decomposition, it is enough to prove the result for cycles. Thus, assume that $f = (a_1 \cdots a_k)$. Then, $f = (a_1\, a_2) \circ (a_2\, a_3) \circ \cdots \circ (a_{k-1}\, a_k)$. Indeed, for a_i with $1 \leqslant i \leqslant k-1$, it us unchanged except by $(a_i\, a_{i+1})$, which sends it to a_{i+1}. For a_k, $(a_{k-1}\, a_k)$ sends it to a_{k-1}, then $(a_{k-2}\, a_{k-1})$ sends it to a_{k-2}. This continues until finally $(a_1\, a_2)$ sends the result to a_1. □

Example 4.6. Write down the cycle decomposition of each element of S_3 and compute the order of each element. See Table 1 for the solution.

e	1
$(1\,2)$	2
$(1\,3)$	2
$(2\,3)$	2
$(1\,2\,3)$	3
$(1\,3\,2)$	3

Table 1: The cycle decompositions and orders of the $6 = 3!$ elements of S_3.

Example 4.7. If $f = (a_{11} \cdots a_{1,k_1}) \cdots (a_{r1} \cdots a_{r,k_r})$ is a decomposition of f into disjoint cycles, then the order of f is the least common multiple of $k_1, \ldots, k_r$. For example, if $f = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)$, then $|f| = 30$.

Example 4.8 (Dummit–Foote, Exercise 1.3.1)**.** One way to write down permutations is using a kind of matrix notation: the permutation $f \in S_5$ given by

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$$

can be written efficiently as

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix},$$

which is just a lookup table. The cycle decomposition of f is $f = (1\,3\,5)(2\,4)$. If we consider

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix},$$

which has cycle decomposition $g = (1\,5)(2\,3)$, then we can compute the cycle decompositions

$$\begin{aligned} f^2 &= (1\,5\,3) \\ fg &= (2\,5\,3\,4) \\ gf &= (1\,2\,4\,3) \\ g^2 f = f &= (1\,3\,5)(2\,4). \end{aligned}$$

4.1 Exercises

Exercise 4.1. Justify Example 4.7. Fix pairwise commuting elements $f_1, \ldots, f_r$ of a group G, i.e., elements such that $f_i f_j = f_j f_i$ for all $1 \leqslant i, j \leqslant r$. Prove that if each f_i has finite order n_i, then $f = f_1 \cdots f_r$ has order dividing the least common multiple of $f_1, \ldots, f_r$. Show that if moreover $f_1, \ldots, f_r$ are pairwise disjoint cycles in a symmetric group S_n, then the order of $f = f_1 \cdots f_r$ is exactly the least common multiple of $f_1, \ldots, f_r$.

Exercise 4.2. By Lemma 4.5, every element $f \in S_n$ can be written as a product of transpositions. Suppose that $f = g_1 \circ \cdots \circ g_k$ where $g_1, \ldots, g_k$ are transpositions. We say that f is **even** if k is even and we say that f is **odd** if k is odd. Show that this is well-defined by proving that if $f = h_1 \circ \cdots \circ h_m$ is another way of writing f as a product of transpositions, then $k \equiv m \mod 2$.

Exercise 4.3. Let $f = (a_1 \cdots a_k)$ be a cycle. Show that f is even if k is odd and that f is odd if k is even.

Exercise 4.4. Write down the cycle decomposition of each element of S_4 and compute the order of each element.

Exercise 4.5 (Dummit–Foote, Exerice 1.3.2)**.** Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix}$$

and

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 9 & 10 & 2 & 12 & 6 & 5 & 11 & 15 & 3 & 8 & 7 & 4 & 1 & 13 \end{pmatrix}$$

be two elements of S_{15}. Find cycle decompositions for f, g, f^2, $f \circ g$, $g \circ f$, and $g^2 \circ f$.

5 Group homomorphisms (09/29)

Definition 5.1 (Magma homomorphisms)**.** Let M and N be two magmas. A function $f\colon M \to N$ is a **magma homomorphism** if $f(ab) = f(a)f(b)$ for all $a, b \in M$.

Remark 5.2. The magma homomorphisms are the functions between the underlying sets that *respect the algebraic structures* given by the binary operations on M and N.

Definition 5.3. If G and H are groups, a function $f\colon G \to H$ is a **group homomorphism** if it is a homomorphism of the underlying magmas, i.e., if $f(ab) = f(a)f(b)$ for all $a, b \in G$.

Remark 5.4. In the same way, one can define semigroup, monoid, quasigroup, and loop homomorphisms.

Lemma 5.5. *If $f\colon G \to H$ is a group homomorphism, then $f(e_G) = e_H$ where e_G is the identity element of G and e_H is the identity element of H.*

Proof. Since H is a group, $f(e_G)$ posseses an inverse, say a so that $af(e_G) = e_H$. We have $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$; multiplying both sides on the left by a we obtain $e_H = af(e_G) = af(e_G)f(e_G) = e_H f(e_G) = f(e_G)$, as desired. □

Lemma 5.6. *If $f\colon G \to H$ is a group homomorphism, then $f(a)^{-1} = f(a^{-1})$ for all $a \in G$.*

Proof. By uniqueness of inverses in groups, it is enough to show that $f(a^{-1})$ is an inverse for $f(a)$. But, $f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H$, by Lemma 5.5, and similarly $f(a)f(a^{-1}) = e_H$. □

Example 5.7. Consider the exponential function $\exp\colon \mathbf{R} \to \mathbf{R}$ given by $\exp(x) = e^x$. As $\exp(x + y) = \exp(x)\exp(y)$, the map exp is a commutative monoid homomorphism $(\mathbf{R}, +) \to (\mathbf{R}, \times)$. If we delete 0, the function exp can be viewed as a group homomorphism $\mathbf{R} \to \mathbf{R}^\times$, where $\mathbf{R}^\times = \mathbf{R} - \{0\}$ is the *group* of non-zero elements of $\mathbf{R}$ under multiplication.

Example 5.8. We can also consider the function $f\colon (\mathbf{R}, +) \to (\mathbf{R}, \times)$ given by $f(x) = 0$ for all x. This is also a commutative monoid homomorphism. However, we do not have $f(0) = 1$, so it does not preserve the identity element of $(\mathbf{R}, +)$. This shows that the hypothesis that G and H be groups in Lemma 5.5 is necessary.

Definition 5.9. We say that a group homomorphism $f\colon G \to H$ is injective (one-to-one), surjective (onto), or bijective if the underlying function of sets is injective, surjective, or bijective.

Lemma 5.10. *A group homomorphism $f\colon G \to H$ is injective if and only if $f(x) = e$ implies $x = e$.*

Proof. Suppose that $f(x) = f(y)$ for some $x, y \in G$. Then, $e = f(e) = f(x^{-1})f(x) = f(x^{-1})f(y) = f(x^{-1}y)$, so $x^{-1}y = e$, or $y = x$. □

Lemma 5.11. *Suppose that $f\colon G \to H$ is a bijective group homomorphism. Let $f^{-1}\colon H \to G$ be the inverse function. Then, f^{-1} is a group homomorphism (which is again bijective).*

Proof. Let $x, y \in H$. We have to prove that $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. Write $x = f(a)$ and $y = f(b)$, for unique $a, b \in G$, using that f is a bijection. Then, $f(ab) = f(a)f(b) = xy$, so that $f^{-a}(xy) = ab = f^{-1}(x)f^{-1}(y)$. □

Definition 5.12. A bijective group homomorphism is called a **isomorphism**. Two groups G and H are called **isomorphic** if there exists a group isomorphism $f\colon G \to H$.

Example 5.13. Let $\mathbf{R}_+^\times$ be the group of positive real numbers under multiplication. The exponential map $\exp\colon \mathbf{R} \to \mathbf{R}_+^\times$ is an isomorphism, so $\mathbf{R} \cong \mathbf{R}_+^\times$.

Remark 5.14. If G is a group, then the identity function id_G is a group isomorphism. If $f\colon G \to H$ and $h\colon H \to K$ are group isomorphisms, then so is $h \circ f\colon G \to K$. Using these facts and Lemma 5.11, it follows that the relation $G \cong H$ if G and H are isomorphic is an equivalence relation on the class of groups.

Example 5.15. Let G and H be groups with 1 element. Then, $G \cong H$. In particular, $S_0 = S_\emptyset$ and S_1 are isomorphic.

Example 5.16. There is an isomorphism $\mathbf{Z}/2 \to S_2$, so $\mathbf{Z}/2 \cong S_2$.

Example 5.17. If G is a group of order 2 (i.e., the underlying set has exactly 2 elements), then $G \cong \mathbf{Z}/2$.

Example 5.18. If G is a group of order 3, then $G \cong \mathbf{Z}/3$.

Definition 5.19 (Cyclic groups)**.** A group G is **cyclic** if $G \cong \mathbf{Z}$ or $G \cong \mathbf{Z}/N$ for some $N \geqslant 1$.

Example 5.20. Let $K = \mathbf{Z}/2 \times \mathbf{Z}/2$ be the product of two copies of $\mathbf{Z}/2$, with addition defined componentwise, so that $(a, b) + (c, d) = (a + c, b + d)$ where $a + c$ and $b + d$ are computed in $\mathbf{Z}/2$. This is a group with 4 elements, but K is not isomorphic to $\mathbf{Z}/4$. Indeed, $\mathbf{Z}/4$ has an two elements of order 4, but K has no element of order 4.

5.1 Exercises

Exercise 5.1. Prove that if $n \geqslant 3$, then S_n is not cyclic.

Exercise 5.2. Recall the group $(\mathbf{Z}/N)^\times$ from Exercise 3.4. Let $\phi(N)$ be the number of elements of $(\mathbf{Z}/N)^\times$. The function ϕ is called the **Euler totient function**.[1]

(a) Show that if $M, N \geqslant 1$ are relatively prime, then $\phi(MN) = \phi(M)\phi(N)$.

(b) Show that if $n \geqslant 1$, then for every prime number p we have $\phi(p^n) = p^{n-1}\phi(p)$.

(c) Show that $\phi(p) = p - 1$ if p is prime.

(d) What is $\phi(3072)$?

Exercise 5.3. Let $f\colon X \to Y$ be a bijection. Consider the permutation groups S_X and S_Y and the function $g\colon S_X \to S_Y$ defined by $g(h) = f \circ h \circ f^{-1}$ for $h \in S_X$. Prove that g is a group isomorphism.

[1] This is just a name. As far as I know, "totient" does not mean anything else.

6 Subgroups (10/02)

Definition 6.1 (Subgroups)**.** Let G be a group and let X be a subset of G we say that X is a **subgroup** if the following conditions hold:

(i) X is nonempty,

(ii) if $a \in X$, then $a^{-1} \in X$, and

(iii) if $a, b \in X$, then $ab \in X$.

These conditions imply

(iv) $e \in X$,

Example 6.2. The group $\mathbf{Z}$ is a subgroup of $\mathbf{R}$, while $\mathbf{N}$ is not a subgroup of $\mathbf{Z}$ because (ii) fails.

Example 6.3. If V is a vector space and $W \subseteq V$ is a subspace, then W is a subgroup of V.

Example 6.4. The set of positive real numbers $\mathbf{R}^{\times}_{+}$ is a subgroup of the group $\mathbf{R}^{\times}$ of non-zero real numbers under multiplication.

Remark 6.5. If G is a group and $X \subseteq G$ is a subgroup, then X is a group. Here, we use condition (iii) to view the restriction of the binary operation from G to X as a binary operation on X. Specifically, write $a \cdot_G b$ for the binary operation in G and if $a, b \in X$, define $X \times X \to X$ by $a \cdot_X b = a \cdot_G b$, viewed as an element of X. Then, X together with this binary operation is a group.

Lemma 6.6. *If $f\colon G \to H$ is a group homomorphism, then the image of f, written $\mathrm{im}(f)$ or $f(G)$, is a subgroup of H and f induces a group homomorphism $G \to f(G)$.*

Proof. Since G has an identity element e, there is an element $f(e) \in f(G)$, so $f(G)$ is nonempty. Similarly, if $x, y \in f(G)$, we can write $x = f(g)$ and $y = f(h)$ for some $g, h \in G$ and hence $xy = f(g)f(h) = f(gh)$, so $xy \in f(G)$ as well. Finally, $x^{-1} = f(g^{-1})$. That the induced function $G \to f(G)$ is a group homomorphism follows from the fact that $f\colon G \to H$ is. □

Lemma 6.7. *If $f\colon G \to H$ is an injective group homomorphism, then the induced function $G \to f(G)$ is a group isomorphism.*

Proof. It is surjective by definition and injective by hypothesis. □

Example 6.8 (Subgroup lattice of S_3)**.** Figure 1 shows the subgroups of S_3 arranged into what is called a subgroup lattice. The lines represent containment. The group on the middle left is isomorphic to $\mathbf{Z}/3$ while the three groups on the middle right are isomorphic to $\mathbf{Z}/2$. These are all of the subgroups because one checks that if a subgroup of S_3 has an element of order 2 and an element of order 3, then it is all of S_3. Note that two distinct elements of order 2 multiply to an element of order 3.

Example 6.9 (Subgroup lattice of $\mathbf{Z}/6$)**.** Figure 2 shows the subgroup lattice of $\mathbf{Z}/6$. The middle left subgroup is isomorphic to $\mathbf{Z}/3$ and the middle right to $\mathbf{Z}/2$.

Theorem 6.10 (Cayley's theorem)**.** *If G is a group, then there is an injective group homomorphism $\ell\colon G \to S_G$, where S_G denotes the group of bijections from the set of elements of G to itself.*

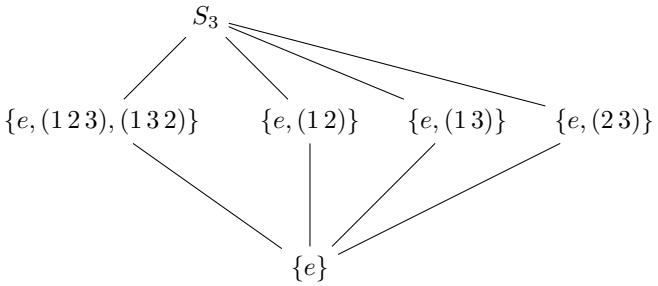

Figure 1: Subgroups of S_3.

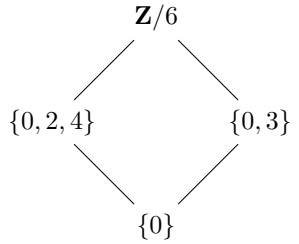

Figure 2: Subgroups of $\mathbf{Z}/6$.

Proof. Given $g \in G$, let $\ell_g \colon G \to G$ be defined by $\ell_g(h) = gh$. This is a bijection by the Latin square property, which holds for all groups. Alternatively, $\ell_g(g^{-1}h) = g(g^{-1}h) = h$, and this is a unique solution to $\ell_g(x) = h$. Thus, the assignment $g \mapsto \ell_g$ gives a function $\ell \colon G \to S_G$ where $\ell(g) = f_g$. The claim is that this is an injective group homomorphism. If $\ell_g = \ell_{g'}$ for $g, g' \in G$, then $g = \ell_g(e) = \ell_{g'}(e) = g'$, which proves injectivity. Now, $(\ell_g \circ \ell_{g'})(h) = \ell_g(\ell_{g'}(h)) = \ell_g(g'h) = g(g'h) = (gg')h = \ell_{gg'}(h)$, so $\ell_g \circ \ell_{g'} = \ell_{gg'}$ and the function ℓ is a group homomorphism. □

Remark 6.11. Cayley's theorem implies every group is a subgroup of a permutation group. However, this can be rather inefficient. For example, the injective group homomorphism $\ell \colon \mathbf{Z}/N \to S_{\mathbf{Z}/N} \cong S_N$ embeds the group $\mathbf{Z}/N$ of order N into a group of order $N!$. What does this embedding look like? It sends $1 \in \mathbf{Z}/N$ to a cycle $c = (0\,1\,\cdots\,N-1)$ (where we use $\{0, \ldots, N-1\}$ instead of $\{1, \ldots, N\}$ since these are the elements of $\mathbf{Z}/N$) and $a \in \mathbf{Z}/N$ to c^a.

Example 6.12. What about S_3? This is a group with 6 elements, so the homomorphism from Cayley's theorem is a group homomorphism $\ell \colon S_3 \to S_6$. Let's label the elements of S_3 as:

$$\begin{pmatrix} e & (1\,2) & (1\,3) & (2\,3) & (1\,2\,3) & (1\,3\,2) \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Then, e of S_3 gets mapped to the identity element e of S_6. A cycle decomposition for $\ell(1\,2)$ is $(1\,2)(3\,6)(4\,5)$.

Remark 6.13 (Orders and group homomorphisms)**.** If $f \colon G \to H$ is a group homomorphism and $a \in G$ has order n, then $f(a)$ has order dividing n. Indeed, $f(a)^n = f(a^n) = f(e) = e$. Thus, in the example above $\ell(1\,2)$ has order dividing 2. But, it's clearly not of order 1, so its order must be exactly 2, which means the only cycles appearing in its cycle decomposition are of length 1 or 2.

6.1 Exercises

Exercise 6.1. Show that if G is a group and $a \in G$ is an element satisfying $a^n = e$ for some integer $n \geqslant 1$, then the order of a divides n.

Exercise 6.2. Draw the lattice of subgroups for the group $K = \mathbf{Z}/2 \times \mathbf{Z}/2$. (Sample LaTeX code is in Discord.)

Exercise 6.3. Draw the lattice of subgroups for the group $\mathbf{Z}/12$.

Exercise 6.4. Using Example 6.12, find a cycle decomposition for $\ell(1\,2\,3)$.

7 Group actions (10/04)

Definition 7.1. Let G be a group and X a set. An **action** of G on X is a function $k\colon G \times X \to X$, written $a \cdot x = k(a, x)$ for $a \in G$ and $x \in X$, satisfying the following axioms:

(a) $e \cdot x = x$ for all $x \in X$ where e is the identity element of G;

(b) $a \cdot (b \cdot x) = (ab) \cdot x$ for all $a, b \in G$ and $x \in X$.

Example 7.2. The group $\mathbf{Z}$ acts on $\mathbf{R}$ by $n \cdot x = n + x$ for $n \in \mathbf{Z}$ and $x \in \mathbf{R}$.

Example 7.3. The group S_X acts on X by $f \cdot x = f(x)$ for $f \in S_X$ and $x \in X$. In particular, S_n acts on the set $\{1, \dots, n\}$.

Example 7.4. If V is a real vector space, then the group $\mathbf{R}^\times$ of non-zero real numbers acts on V by scalar multiplication: if $v \in V$ and $\alpha \in \mathbf{R}^\times$, then $\alpha \cdot v = \alpha v$.

Example 7.5. If G is a group, it acts on itself by left multiplication: for $g, h \in G$, we let $g \cdot h = gh$. Here, we view the G which acts as the *left* G in $m\colon G \times G \to G$. This is called the *left regular action* of G on itself. The formula $g \cdot h = hg$ would not generally be a group action of G on itself. Why not?

Example 7.6 (Return to Exercise 4.2)**.** We can learn about a group G via its actions. For example, consider a symmetric group S_n. The symmetric group acts on the set F of functions $\mathbf{R}^n \to \mathbf{R}$ as follows. Given $a \ni S_n$ and $f\colon \mathbf{R}^n \to \mathbf{R}$, we let $(a \cdot f)(x_1, \dots, x_n) = f(x_{a(1)}, x_{a(2)}, \dots, x_{a(n)})$, i.e., by reordering the inputs. Let $g(x) = \prod_{1 \leqslant i < j \leqslant n}(x_i - x_j)$. This polynomial is called the Vandermonde polynomial. Note that for any $a \in S_n$, either $a \cdot g = g$ or $a \cdot g = -g$. For example, if $n = 4$, this polynomial is

$$g(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

The element $a = (1\,2\,3\,4)$ of S_4 then acts as

$$(a \cdot g)(x_1, x_2, x_3, x_4) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1) = -g(x_1, x_2, x_3, x_4).$$

Let S_n act on $\{1, -1\}$ by letting $a \cdot \epsilon = \gamma$ if $a \cdot (\epsilon g) = \gamma g$. In the example above, the 4-cycle a has $a \cdot 1 = -1$ and $a \cdot (-1) = 1$. If $a \in S_n$ is a transposition, then $a \cdot 1 = -1$. To see this, suppose that $a = (c\,d)$ where $1 \leqslant c < d \leqslant n$. If $i < c$, then $a \cdot (x_i - c) = (x_i - d)$ and if $d < j$, then $a \cdot (c - x_j) = (d - x_j)$. We also have $a \cdot (x_i - x_j) = (x_j - x_i) = -(x_i - x_j)$. Finally, if $c < i < d$,

$$a \cdot (x_c - x_i)(x_i - x_d) = (x_d - x_i)(x_i - x_c) = (-(x_i - x_d))(-(x_c - x_i)) = (x_c - x_i)(x_i - x_d).$$

Collating these calculations, it follows that $a \cdot v = -v$ for $a = (c\,d)$. Thus, by axiom (b) of a group action, if a is a product of k transpositions, then $a \cdot 1 = (-1)^k$. This proves the claim from Exercise 4.2 as if $(-1)^k = (-1)^m$, then $k \equiv m \mod 2$.

The next theorem says that group actions of G on X are "the same" as group homomorphisms $G \to S_X$.

Theorem 7.7. *Let G be a group and X as set. There is a bijection*

$$\{\textit{actions } k \textit{ of } G \textit{ on } X\} \xrightarrow{k \mapsto f_k} \mathrm{Hom}(G, S_X).$$

Proof. Next time. □

Example 7.8. The action of S_n on the Vandermonde polynomial induces, via the theorem, a surjective group homomorphism $S_n \to S_{\{1,-1\}}$, which we view as a group homomorphism $\epsilon\colon S_n \to S_2 \cong \mathbf{Z}/2 \cong \{1, -1\}$, where $\{1, -1\}$ is a group under multiplication. The **sign** of an element $a \in S_n$ is $\epsilon(a) \in \{1, -1\}$.

7.1 Exercises

Exercise 7.1. Suppose that G is a finite group of even order. Show that there exists $x \neq e$ in G with $x^2 = e$.

Exercise 7.2. Show that every finite group G of order 4 is isomorphic to either $\mathbf{Z}/4$ or to $K = \mathbf{Z}/2 \times \mathbf{Z}/2$.

Exercise 7.3. Show that a finite group G of order 5 is isomorphic to $\mathbf{Z}/5$.

8 The adjoint homomorphism (10/06)

Our next theorem says that group actions of G on X are "the same" as group homomorphisms $G \to S_X$.

Theorem 8.1. *Let G be a group and X as set. There is a bijection*

$$\{\text{actions } k \text{ of } G \text{ on } X\} \xrightarrow{k \mapsto f_k} \mathrm{Hom}(G, S_X),$$

where $\mathrm{Hom}(G, S_X)$ denotes the set of group homomorphisms from G to S_X.

Proof. Let $k\colon G \times X \to X$ be a group action; we will write $g \cdot_k x$ for $k(g, x)$ in this proof. For $g \in G$, let $f_k(g)$ be the function $X \to X$ defined by $f_k(g)(x) = k(g, x) = g \cdot_k x$. This is a bijection as one sees by observing that $f_k(g^{-1})$ is an inverse using (a) and (b) from the definition of a group action. Therefore, f_k is a function $G \to S_X$. In fact, this is a group homomorphism. Indeed, $f_k(gh)(x) = gh \cdot_k x = g \cdot_k (h \cdot_k x) = f_k(g)(f_k(h)(x))$ for all $g, h \in G$ and $x \in X$. Therefore, $f_k(gh) = f_k(g) \circ f_k(h)$, as desired.

To show that the assignment $k \mapsto f_k$ is bijective, assume first that k and n are distinct group actions. Then, there exists a pair $(g, x) \in G \times X$ such that $g \cdot_k x \neq g \cdot_n x$. It follows that $f_k(g) \neq f_n(g)$. This shows injectivity.

Given a group homomorphism $f\colon G \to S_X$, we define a new group action k_f of G on X by letting $g \cdot_{k_f} x = f(g)(x)$. By definition, $f_{k_f}(g)(x) = g \cdot_{k_f} x = f(g)(x)$, so $f_{k_f}(g) = f(g)$ for all $g \in G$ and hence $f_{k_f} = f$, which proves surjectivity. □

Definition 8.2. If k is an action of G on X, then $f_k\colon G \to S_X$ is called the **adjoint homomorphism**. If $f\colon G \to S_X$ is a homomorphism, then k_f is called the **action associated to** f.

Example 8.3. Let G be a group and consider its left regular action on itself $m\colon G \times G \to G$. The adjoint homomorphism $\ell = f_m\colon G \to S_G$ is the homomorphism used in the proof of Cayley's Theorem 6.10.

Example 8.4. Recall the group $K = \mathbf{Z}/2 \times \mathbf{Z}/2$, sometimes known as the **Klein four-group**. It has four elements, which we label as follows:

$$\begin{pmatrix} (0,0) & (1,0) & (0,1) & (1,1) \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

The adjoint homomorphism $\ell\colon K \to S_K$ we view, using the labeling above, as a homomorphism $\ell\colon K \to S_4$. A cycle decomposition of $\ell(1,0)$ is $((0,0)\,(1,0))((0,1)\,(1,1)) = (1\,2)(3\,4)$.

8.1 Exercises

Exercise 8.1. Say that an action of a group G on a set X is **trivial** if $g \cdot x = x$ for all $g \in G$ and x on X. Suppose that p is a prime and that X is a set with fewer than p elements. Show that all actions of $\mathbf{Z}/p$ on X are trivial.

Exercise 8.2. Compute the set $\mathrm{Hom}(\mathbf{Z}/2, S_4)$ of group homomorphisms into S_4. Use your computation to describe all group actions of $\mathbf{Z}/2$ on $\{1, 2, 3, 4\}$.

9 Dihedral groups (10/09)

Example 9.1 (Dihedral groups)**.** Fix $n \geqslant 3$. Let X be a regular n-gon with vertices labeled as $\{1, \ldots, n\}$ sitting in $\mathbf{R}^2$ centered at the origin. Let $D_{2n} \subseteq S_n$ be the set of permutations of the vertex set $\{1, \ldots, n\}$ consisting of those which can be achieved by a rigid motion of X in $\mathbf{R}^3$ returning X bijectively to itself. Among these, we single out two. Let r denote the permutation obtained by counterclockwise rotation about the origin by $\frac{2\pi i}{n}$. Let s denote the reflection across the line between 1 and the origin. Geometrically, we see that $rs = sr^{-1}$. This implies that the elements $\{e, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ form a subgroup of S_n. Indeed,

$$(s^a r^b)(s^c r^d) = s^a s^c r^{(-1)^c b} r^d = s^{a+c} r^{(-1)^c b + d} = s^e r^f,$$

where $e \equiv a + c \mod 2$ is in $\{0, 1\}$ and $f \equiv (-1)^c b + d \mod 2$ is in $\{0, \ldots, n\}$. We claim that this is all of D_{2n} and hence that D_{2n} is a subgroup of S_n, known as the **dihedral group of order** $2n$. To see this, suppose that $x \in D_{2n}$. We want to show that x is in the list of $2n$ elements above. We can compose with a rotation and assume that x sends the vertex 1 to itself. Then, since it arises from a rigid motion of $\mathbf{R}^3$, we must have that x sends either 2 to itself and $n-1$ to itself, or it sends 2 to $n-1$ and $n-1$ to 2. In the first case, it must be the identity. In the second case, it must be the reflection s.

Remark 9.2. Let $n = 4$ and consider the dihedral group D_8 of order 8. Let s denote the reflection across the diagonal through 1 and 3 and let s' denote the reflection across the diagonal through 2 and 4. Then, ss' has cycle decomposition $(1\,3)(2\,4)$. But, so does r^2. So, $ss' = r^2$.

9.1 Exercises

Exercise 9.1. Make a list of all elements of D_8, their orders, and a cycle decomposition for each (with respect to the action above of D_8 on $\{1, 2, 3, 4\}$).

Exercise 9.2. Find the lattice of subgroups of D_8.

Exercise 9.3. Find the lattice of subgroups of D_{10}.

10 Some properties of group actions (10/11)

Recall the following definition from Section 8.

Definition 10.1 (Trivial actions)**.** Say that an action of G on X is **trivial** if $g \cdot x = x$ for all $x \in X$ and all $g \in G$. This is the case if and only if the adjoint homomorphism $f\colon G \to S_X$ satisfies $f(g) = e$ for all $g \in G$.

At the opposite extreme, we have the faithful actions.

Definition 10.2. The action of a group G on a set X is **faithful** if the adjoint homomorphism $G \to S_X$ is injective.

Remark 10.3. In other words, an action of G on X is faithful if different elements of G produce different permutations on X. Unwinding, this means that for each pair of distinct elements $f, g \in G$ there exists $x \in X$ such that $f \cdot x \neq g \cdot x$.

Remark 10.4. If X is a set and S_X is the permutation group of X, then any subgroup $G \subseteq S_X$ comes with an action on X which is faithful.

Example 10.5. As D_{2n} is a subgroup of S_n, its action on $\{1, \ldots, n\}$ is faithful.

Definition 10.6 (Orbits and stabilizers)**.** Let G be a group acting on a set X.

(i) If $x \in X$, the **orbit** of G containing x is the set $G \cdot x = \{g \cdot x | g \in G\}$. Alternatively, if $k\colon G \times X \to X$ denotes the action map, it is the image of $G \times \{x\}$ under k.

(ii) If $x \in X$, the **stabilizer** of x in G is the set $G_x = \{g \in G | g \cdot x = x\}$.

Lemma 10.7. *If G acts on a set X and if $x \in X$, then the stabilizer $G_x \subseteq G$ is a subgroup.*

Proof. Of course, $e \in G_x$. We also have that if $g \in G_x$, then $g^{-1} \in G_x$ as $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$. Similarly, if $g, h \in G_x$, then $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, so $gh \in G_x$. □

Example 10.8. Consider D_{2n} acting on the n-gon X_n with vertex set $\{1, \ldots, n\}$ as in Definition 9.1. The orbit of any vertex is $\{1, \ldots, n\}$. What about the orbit of a point on X that is not a vertex? The stabilizer of 1 in G is $G_1 = \{e, s\}$. Indeed, any rotation must "move" 1. Any element f which fixes 1 must either send 2 to itself, in which case $f = 1$ or it sends 2 to n and n to 2, in which case $sf = e$, or $f = s$. The stabilizer of a point which is not a vertex is trivial if n is even and usually trivial if n is odd, the exception being the points opposite to vertices which are fixed by appropriate reflections.

Philosophy 10.9. The approach to defining the dihedral group is very helpful in finding new groups. For example, let T in $\mathbf{R}^3$ be a regular tetrahedron with vertex set $\{1, 2, 3, 4\}$. Among all rigid motions of $\mathbf{R}^3$, there are those which act bijectively on T, and must send vertices to vertices, edges to edges, and faces to faces. How many are there? I can send 1 to any vertex $i \in \{1, 2, 3, 4\}$, which amounts to four choices of where 1 goes. Once that is fixed, 2 must go to one an element of $\{1, 2, 3, 4\} - \{i\}$, so there are three more choices. But, then it is fixed. For example, if 1 maps to 3 and 2 maps to 1, then one sees by rigidity that 3 maps to 2 and 4 maps to 3.

Example 10.10 (The conjugation action)**.** Let G be a group. We define a new action of G on itself, given by conjugation. Namely, let $c\colon G \times G \to G$ be defined by $c(g, h) = ghg^{-1}$. This is the result of *conjugating h by g*. We have $c(e, h) = ehe^{-1} = h$ for all $h \in G$ and we have $c(f, c(g, h)) = f(ghg^{-1})f^{-1} = (fg)h(fg)^{-1} = c(fg, h)$. So, conjugation defines a group action of G on itself. The conjugation action is always different from the left regular action if G is not the trivial group $\{e\}$.

Question 10.11. When is the conjugation action trivial?

Definition 10.12 (Orbit set)**.** Let a group G act on a set X. For $x, y \in X$, write $x \sim y$ if there exists $g \in G$ such that $g \cdot x = y$. This defines an equivalence relation on X. Indeed, $e \cdot x = x$ so $x \sim x$ (reflexivity), if $g \cdot x = y$, then $g^{-1} \cdot y = x$ (reflexivity), and if $g \cdot x = y$ and $h \cdot y = z$, then $(hg) \cdot x = z$ (transitivity). The equivalence classes are precisely the orbits. We write X/G for the set of orbits. The quotient function $f \colon X \to X/G$ sends $x \in X$ to $G \cdot x \in X/G$.

Question 10.13. What does the orbit set of D_{2n} acting on X_n look like? It is bijective to the closed line segment L from vertex 1 (inclusive) to midpoint (inclusive) between vertices 1 and 2. Indeed, for each $x \in X_n$ there is a unique y on L such that $g \cdot x = y$ for some $g \in D_{2n}$ (note that you have to use rotations *and* reflections to see this).

Definition 10.14 (Transitive actions)**.** The action of a group G on a set X is **transitive** if X/G is a point or, equivalently, if there is only one orbit or, equivalently, if for all pairs $x, y \in X$ there exists $g \in G$ such that $g \cdot x = y$.

10.1 Exercises

Exercise 10.1. Let $G = S_n$ act on $X = \{1, \ldots, n\}$ via permutations.

(a) What is the orbit $G \cdot 1$?

(b) What is the stabilizer G_1 of 1 in G? (It is isomorphic to a group we have a name for.)

(c) What is the set of orbits X/G?

(d) Is the action faithful?

(e) Is the action transitive?

Exercise 10.2. Repeat Exercise 10.1(a)-(e) for the left regular action of a group G on itself (where 1 is replaced by e in parts (a) and (b)).

Exercise 10.3. Repeat Exercise 10.1(a)-(e) for the conjugation action of $G = D_8$ on itself (where 1 is replaced by e in parts (a) and (b)).

Exercise 10.4. Arguing as in Philosophy 10.9, compute the order of the group of rigid motions of an icosahedron in $\mathbf{R}^3$.

11 Lagrange's theorem and consequences (10/13)

Definition 11.1 (Cosets)**.** Let G be a group and $H \subseteq G$ a subgroup. Given $g \in G$, define

$$gH = \{gh : h \in H\} \quad \text{and} \quad Hg = \{hg : h \in H\},$$

the left and right **cosets** of H containing g. (Note that $g \in gH$ and $g \in Hg$.) These are subsets of G.

Remark 11.2. When G is written additively, the cosets are often written $g + H$.

Example 11.3. Suppose we consider the subgroup $H = \{0, 2, 4\}$ of $\mathbf{Z}/6 = \{0, 1, 2, 3, 4, 5\}$. The right cosets are

$$\begin{aligned} H + 0 &= \{0, 2, 4\}, \\ H + 1 &= \{1, 3, 5\}, \\ H + 2 &= \{0, 2, 4\}, \\ H + 3 &= \{1, 3, 5\}, \\ H + 4 &= \{0, 2, 4\}, \\ H + 5 &= \{1, 3, 5\}. \end{aligned}$$

This scintillating pattern is explained in Lemma 11.5.

Example 11.4. Suppose we consider the subgroup $H = \{e, (1\,2)\}$ of S_3. The right cosets are

$$\begin{aligned} He &= \{e, (1\,2)\}, \\ H(1\,2) &= \{e, (1\,2)\}, \\ H(1\,3) &= \{(1\,3), (1\,3\,2)\}, \\ H(2\,3) &= \{(2\,3), (1\,2\,3)\}, \\ H(1\,2\,3) &= \{(1\,2\,3), (2\,3)\}, \\ H(1\,3\,2) &= \{(1\,3\,2), (1\,3)\}. \end{aligned}$$

Lemma 11.5. *Let G be a group and $H \subseteq G$ a subgroup. If $g_0, g_1 \in G$, then the following are equivalent:*

(i) $g_0H \cap g_1H \neq \emptyset$,

(ii) $g_0^{-1}g_1 \in H$,

(iii) $g_0H = g_1H$.

Proof. Suppose that $g_0H \cap g_1H \neq \emptyset$. Then, there exist $h_0, h_1 \in H$ such that $g_0h_0 = g_1h_1$, which implies $h_0h_1^{-1} = g_0^{-1}g_1$ (multiplying on the left by g_0^{-1} and on the right by h_1^{-1}). So, (i) implies (ii) since $h_0h_1^{-1}$ is in H as H is a subgroup of G. Assume $g_0^{-1}g_1 \in H$, in which case the inverse $g_1^{-1}g_0$ is also in H. Then, for $h \in H$, we have $g_1h \in g_1H$. But, $g_1g_1^{-1}g_0h = g_0h$ is also in g_1H, so $g_0H \subseteq g_1H$. Similarly, $g_1H \subseteq g_0H$, so (ii) implies (iii). Finally, (iii) implies (i) using that cosets are always nonempty. □

Remark 11.6. Lemma 11.5 holds with right cosets instead of left cosets where condition (ii) is replaced by

(ii) $g_1g_0^{-1} \in H$.

Remark 11.7. Say that $g_0 \sim g_1$ if the equivalent conditions of Remark 11.6 hold. This defines an equivalence relation on G with equivalence classes given by the varying Hg. The set of equivalence classes (right cosets) is written as G/H. (Note that left and right cosets do not generally agree. There is an example in S_3.)

Remark 11.8. If H is a subgroup of G we can view it as acting on G via $h \cdot g = hg$. The orbit of H containing g, written $H \cdot g$ in Lecture 10, is the right coset Hg.

Lemma 11.9. *Let G be a group, $H \subseteq G$ a subgroup, and $g_0, g_1 \in G$. Multiplication on the right by $g_0^{-1}g_1$ gives a bijection $Hg_0 \to Hg_1$.*

Proof. Given hg_0, we have $(hg_0)(g_0^{-1}g_1) = hg_1$, so this operation defines a function $Hg_0 \to Hg_1$. It has an inverse given by right multiplication by $g_1^{-1}g_0$, so it is a bijection. □

Corollary 11.10. *If G is a group and $H \subseteq G$ is a finite group, then any two right cosets Hg_0 and Hg_1 have the same number of elements (equal to the number of elements of H).*

Proof. Bijective finite sets have the same number of elements and $He = H$, so the corollary follows from Lemma 11.9. □

Theorem 11.11 (Lagrange)**.** *Suppose that G is a finite group and $H \subseteq G$ is a subgroup, then the order of H divides the order of G.*

Proof. Since the relation $\sim$ introduced in Remark 11.7 is an equivalence relation, G is the disjoint union of some equivalence classes $Hg_1, Hg_2, \ldots, Hg_k$. Thus,

$$|G| = \sum_{i=1}^{k} |Hg_i|.$$

As each $|Hg_i| = |H|$ by Corollary 11.10, it follows that the sum is equal to $k|H|$. So, $|G| = k|H|$, as desired. □

Motto 11.12 ($|G| = |H||G/H|$)**.** If $H \subseteq G$ is a subgroup of a finite group, then the number of (right) cosets times the order of H is equal to the order of G. Indeed, in the proof of Theorem 11.11 the number of right cosets is k.

Corollary 11.13 (Lagrange's theorem for elements)**.** *Let G be a finite group and $g \in G$ an element, then $|g|$ divides $|G|$.*

Proof. Let $N = |g|$. Then, the set $\{1, g, g^2, \ldots, g^{N-1}\}$ forms a subgroup of G of order N. By Theorem 11.11, $N = |g|$ divides $|G|$. □

Remark 11.14. The converse does not hold: if G is a finite group and if $N > 1$ divides $|G|$, there need not be an element of G of order N. See Exercise 11.1.

Corollary 11.15. *If G is a finite group and $g \in G$, then $g^{|G|} = e$.*

Proof. Write $|G| = |g|k$. Then, $g^{|G|} = (g^{|g|})^k = e^k = e$. □

11.1 Exercises

Exercise 11.1. The largest order of an element of S_3 is 3. The largest order of an element of S_4 is 4. The largest order of an element of S_5 is **6**! The largest order of an element of S_6 is 6. The largest order of an element of S_7 is **12**! What are the largest orders of elements in S_8, S_9, and S_{10}? (Recall our previous work on the order of elements of symmetric groups in terms of their cycle decompositions.)

Exercise 11.2. Prove that if G is a finite group of order p, where p is a prime, then $G \cong \mathbf{Z}/p$.

Exercise 11.3. Prove that if $N \geqslant 1$ and $a \in (\mathbf{Z}/N)^\times$, then $a^{\phi(N)} \equiv 1 \mod N$, where ϕ is Euler's totient function.

Exercise 11.4 (Fermat's little theorem)**.** Prove that if p is a prime, then $a^p \equiv a \mod p$ for any $a \in \mathbf{Z}$.

12 Kernels and normal subgroups (10/16)

Definition 12.1 (Kernels)**.** Let $f\colon G \to H$ be a group homomorphism. The kernel of f is the subset $\ker(f) \subseteq G$ consisting of elements $g \in G$ such that $f(g) = e$.

Lemma 12.2 (The kernel is a group)**.** *If $f\colon G \to H$ is a group homomorphism, then $\ker(f) \subseteq G$ is a subgroup.*

Proof. If $a, b \in \ker(f)$, then $f(ab) = f(a)f(b) = ee = e$, so $ab \in \ker(f)$. If $a \in \ker(f)$, then $e = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) = ef(a^{-1}) = f(a^{-1})$, so $a^{-1} \in \ker(f)$. Finally, the kernel is non-empty as $e \in \ker(f)$. □

Example 12.3. Recall the sign homomorphism $\operatorname{sgn}\colon S_n \to \{\pm 1\}$. The kernel, consisting of the subset of *even* elements, is called the alternating group and denoted by A_n.

Definition 12.4 (Normal subgroups)**.** Let G be a group and $N \subseteq G$ be a subgroup. We say that N is a **normal** subgroup of G if for every $g \in G$ and $n \in N$ the conjugate of n by g, namely gng^{-1}, is in N.

Lemma 12.5 (Kernels are normal)**.** *If $f\colon G \to H$ is a group homomorphism, then $\ker(f)$ is a normal subgroup of G.*

Proof. Fix $n \in \ker(f)$, so that $f(n) = e$. Fix $g \in G$. Then, $f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)ef(g)^{-1} = e$, so $gng^{-1} \in \ker(f)$. □

Lemma 12.6 (Subgroups of abelian groups are normal)**.** *If G is an abelian group and $K \subseteq G$ is a subgroup, then K is normal.*

Proof. Indeed, if $n \in K$ and $g \in G$, then $gng^{-1} = gg^{-1}n = n$, which is certainly in K. □

Example 12.7 (Not all subgroups are normal)**.** We must look in a non-abelian group. Our first example is S_3. Consider the subgroup $K = \{e, (1\,2)\}$ in S_3. Then, $(1\,3)(1\,2)(1\,3) = (1\,3)(1\,3\,2) = (2\,3)$, which is not in K. So, letting $n = (1\,2)$ and $g = (1\,3)$ (so that $g^{-1} = (1\,3)$ as well), we see that K is not normal. In particular, this means that K is not the kernel of any group homomorphism $S_3 \to H$, by Lemma 12.5.

Lemma 12.8 (Right is left for cosets of normal subgroups)**.** *Let G be a group. If $N \subseteq G$ is a subgroup, then N is normal in G if and only if every left coset of N in G is a right coset of N in G.*

Proof. Using Exercise 12.2, we see that N is normal if and only if $gNg^{-1} = N$ for all $g \in G$, which is the case if and only if $gN = Ng$ for all $g \in G$. This shows that normality implies that the left and right cosets are the same. Now, suppose that every left coset gN is a right coset, say Nh for some h (depending on G). But, $g \in gN$, so $g \in Nh$, so $Nh = Ng$ by the right coset version of Lemma 11.5. In other words, for every g, we have $gN = Ng$, which yields $gNg^{-1} = N$ by multiplying on the right by g^{-1}. This proves normality of N in G. □

Lemma 12.9 (Products of (right) cosets are cosets)**.** *Fix a normal subgroup N in a group G. Then, the product of two right cosets is again a right coset.*

Proof. Let $g, h \in G$. Then, $(Ng)(Nh) = NN(gh) = N(gh)$, so the product of two right cosets is a right coset. Second, assume that products of right cosets are right cosets. □

Theorem 12.10 (Normal subgroups are kernels)**.** *Let $N \subseteq G$ be a normal subgroup. Then, the set of right cosets G/N is equipped with a group structure via $(Ng)(Nh) = N(gh)$, the map $f\colon G \to G/N$ given by $f(g) = Ng$ is a group homomorphism, and $N = \ker(f)$.*

Proof. The formula $(Ng)(Nh) = N(gh)$ is a well-defined binary operation on right cosets. It has an identity element given by $N = Ne$. The inverse of Ng is $N(g^{-1})$. And, associativity is inherited from the multiplication on G. Thus, G/N is a group under this multiplication of right cosets. Letting $f\colon G \to G/N$ be given by $f(g) = Ng$, we see $f(gh) = N(gh) = (Ng)(Nh) = f(g)f(h)$, so that f is a group homomorphism. Finally, the kernel of f consists of those $g \in G$ such that $f(g) = Ng = Ne = N$. But, this is precisely N. □

Definition 12.11 (Quotient groups)**.** If N is a normal subgroup of G, then the set of right cosets G/N with the product defined above is called the **quotient of G by N**. Quotient group constructions are ubiquitous and important ways of creating new groups and understanding given ones.

Definition 12.12 (Simple groups)**.** A group G is **simple** if its only normal subgroups are $\{e\}$ and G. Equivalently, G is simple if every group homomorphism $G \to H$ is either injective or sends all of G to $e \in H$. A major achievement of 20th century group theory is the classification of *finite* simple groups.

Example 12.13. Fix an integer $N \geqslant 1$ and let $N\mathbf{Z} \subseteq \mathbf{Z}$ be the subgroup of integers divisible by N. This is a normal subgroup. The quotient group $\mathbf{Z}/N\mathbf{Z}$ is what we have been writing as $\mathbf{Z}/N$. Put another way, there is a group homomorphism $f\colon \mathbf{Z} \to \mathbf{Z}/N$ given by $f(k) \equiv k \mod N$ whose kernel is $N\mathbf{Z}$.

Proposition 12.14 (Lagrange's theorem for normal subgroups)**.** *If N is a normal subgroup of a finite group G, then $|G/N||N| = |G|$.*

Proof. In fact, we already proved this last time under the weaker hypothesis that N is simply a subgroup. That was called Lagrange's theorem. □

Remark 12.15. Phrased differently, if $f\colon G \to H$ is a *surjective* group homomorphism where G is a finite group, then $|\ker(f)||H| = |G|$.

Example 12.16. The order of A_n is $\frac{n!}{2}$.

12.1 Exercises

Exercise 12.1. Fix $n \geqslant 3$ and let s denote the composition of the inclusion $D_{2n} \to S_n$ and the sign homomorphism $\operatorname{sgn}\colon S_n \to \{\pm 1\}$. Determine $\ker(s) \subseteq D_{2n}$.

Exercise 12.2. Prove that a subgroup $N \subseteq G$ is normal if and only if for every $g \in G$, the subset $gNg^{-1} = \{gng^{-1} : n \in N\}$ is equal to N.

Exercise 12.3. Prove that if $f\colon G \to H$ is a surjective group homomorphism with kernel $N = \ker(f)$, then $H \cong G/N$.

Exercise 12.4. Prove that if $N \geqslant 2$, then $\mathbf{Z}/N$ is simple if and only if N is prime.

Exercise 12.5. Prove that if A is a non-trivial abelian group (meaning that it is not isomorphic to the group $\{e\}$), then A is simple if and only if $A \cong \mathbf{Z}/p$ for some prime number p.

13 Normal subgroups and orbit decomposition (10/23)

13.1 Normal subgroups

Remark 13.1. Recall that last time we defined normal subgroups $N \subseteq G$ to be those subgroups such that for every $n \in N$ and every $g \in G$, the conjugate gng^{-1} is in N. We observed that every kernel is normal and that conversely if N is a normal subgroup of G, then the equality holds $(Ng)(Nh) = N(gh)$ and makes the set G/N of right cosets into a group. Also, in this case, the set of left cosets is equal to the set of right cosets and we could have defined G/N via left cosets as well.

Lemma 13.2. *Let G be a group and let $N \subseteq G$ be a normal subgroup. There is a bijection between the set of normal subgroups of G/N and the set of normal subgroups of G containing N.*

Proof. Let $f\colon G \to G/N$ be the quotient homomorphism defined by $f(g) = Ng$. If $K \subseteq G/N$ is normal, then we can construct a further group homomorphism $g_K\colon G/N \to (G/N)/K$. The kernel of the composition $g_K \circ f$ is a normal subgroup of G and contains N. It is $f^{-1}(K)$. This gives a function from normal subgroups of G/N to normal subgroups of G containing N. Now, if $N \subseteq M \subseteq G$ and N, M are normal in G, then I claim that $f(M) \subseteq G/N$ is normal. Indeed, if $m \in M$ and $g \in G$, we have to show that $(Ng)(Nm)(Ng)^{-1} = Nm_0$ for some $m_0 \in M$. We have $(Ng)^{-1} = N(g^{-1})$ by normality and $(Ng)(Nm)(N(g^{-1})) = N(gmg^{-1})$. But, $gmg^{-1} \in M$. Thus, $M \mapsto f(M)$ and $K \mapsto f^{-1}(K)$ give mutually inverse bijections. □

13.2 Orbit decomposition

Remark 13.3. On the practice midterm, we saw that if G is a finite group acting on a set X, then for every element $x \in X$,

$$|G| = |G_x||G \cdot x|.$$

In other words, the number of elements of G is equal to the size of the stabilizer of x in G times the size of the orbit of G containing x.

Lemma 13.4. *Suppose that a finite group G acts on a finite set X. Then,*

$$|X| = \sum_{\mathcal{O} \in X/G} \frac{|G|}{|G_x|},$$

where $\mathcal{O}$ ranges over the orbits of G acting on X and where x is a choice of a representative of $\mathcal{O}$.

Proof. We know that the action of G on X leads to an equivalence relation on X where $x \sim y$ if there exists $g \in G$ such that $g \cdot x = y$. It follows that X is partitioned into equivalence classes, which we have called the orbits of G acting on X and written as X/G. Thus, we have the equality

$$|X| = \sum_{\mathcal{O} \in X/G} |\mathcal{O}|.$$

It suffices to compute $|\mathcal{O}|$. If $x \in \mathcal{O}$, then Remark 13.3 implies that $|G| = |G_x||G \cdot x| = |G_x||\mathcal{O}|$ or $|\mathcal{O}| = \frac{|G|}{|G_x|}$. Substituting into the displayed equation above, the lemma follows. □

Example 13.5. Recall that a group G acts transitively on X if there is only one orbit $\mathcal{O}$ (which must then be equal to X). In this case, it follows that for any $x \in X$ there is an equality $|X| = |\mathcal{O}| = \frac{|G|}{|G_x|}$. Suppose

then that D_{2n} is the dihedral group acting on the set $\{1, \ldots, n\}$. This is a transitive action (as one sees by using rotations). The equality

$$n = |\{1, \ldots, n\}| = \frac{|D_{2n}|}{|(D_{2n})_x|} = \frac{2n}{|(D_{2n})_x|}$$

holds for every $x \in \{1, \ldots, n\}$. In particular, we see that the stabilizer of x is a subgroup of order 2 for each $x \in D_{2n}$. These are precisely the reflections. For example, $\{e, sr^k\}$ is the stabilizer of some vertex (which one?) and every stabilizer is of this form.

13.3 Exercises

Exercise 13.1. If G is a group, and $N \subseteq M \subseteq G$ are subgroups where N is normal in G and M is normal in G, then $(G/N)/(M/N) \cong G/M$. Hint: construct a surjective homomorphism $G/N \to G/M$ and compute its kernel.

Exercise 13.2. Find an example of a group G with subgroups $N \subseteq M \subseteq G$ where N is normal in M and M is normal in G but N is not normal in G.

Exercise 13.3. Let H be the stabilizer of n in S_n acting on $\{1, \ldots, n\}$. What is the order of H? Which group that we've studied is H isomorphic to?

14 The class equation (10/25)

Definition 14.1. Recall the conjugation action of G on itself defined by $g \cdot h = ghg^{-1}$. We write $G//G$ for the of orbits for the conjugation action. The set $G//G$ is also called the set of **conjugacy classes** of G as two elements h and k satisfy $h \sim k$ if and only if they are conjugate: there exists a $g \in G$ such that $ghg^{-1} = k$.

Definition 14.2. Let G be a group and let $x \in G$. The **normalizer** of x in G, written $N_G(x)$, is the subgroup of elements $g \in G$ such that $gxg^{-1} = x$. Note that the normalizer $N_g(x)$ is just the stabilizer of x with respect to the conjugation action.

Theorem 14.3 (The class equation)**.** *If G is a finite group, then*

$$|G| = \sum_{\mathcal{O} \in G//G} \frac{|G|}{|N_G(x_{\mathcal{O}})|},$$

where $\mathcal{O}$ ranges over the conjugacy classes in G and $x_{\mathcal{O}}$ is the choice of an element in $\mathcal{O}$.

Proof. This is an example of the class equation for group actions, Lemma 13.4. □

Remark 14.4. Here is another way the class equation is often stated. The **center** of a group G is the subgroup $Z(G)$ consisting of elements $h \in G$ such that $ghg^{-1} = h$ for all $g \in G$. In other words, it is the set up elements that commute with all elements in G. Note that $h \in Z(G)$ if and only if $N_g(h) = G$. In particular, the orbit of the conjugation action containing $h \in Z(G)$ is just $\{h\}$. It follows that we can write the class equation as

$$|H| = \sum_{h \in Z(G)} 1 + \sum_{\mathcal{O} \in G//G \text{ non-central}} \frac{|G|}{|N_G(x_{\mathcal{O}})|} = |Z(G)| + \sum_{\mathcal{O} \in G//G \text{ non-central}} \frac{|G|}{|N_G(x_{\mathcal{O}})|},$$

where the sum on the right ranges over the *non-central* conjugacy classes $\mathcal{O}$ and $x_{\mathcal{O}}$ is a representative of $\mathcal{O}$.

Notation 14.5. If G is a finite group and $H \subseteq G$ is a subgroup, then the **index** of H in G, written $|G : H|$ is the number of right cosets G/H. In other words, $|G : H| = \frac{|G|}{|H|}$, which is an integer by Lagrange's theorem.

Remark 14.6 (Class equation, final form)**.** Using the notation above and the simplification of Remark 14.4, we have

$$|G| = |Z(G)| + \sum_{\mathcal{O} \in G//G \text{ non-central}} |G : N_G(x_{\mathcal{O}})|,$$

where $x_{\mathcal{O}} \in \mathcal{O}$.

Definition 14.7. A p-group is a finite group G whose order is a prime power p^n for some prime p and natural number $n \geqslant 0$.

Theorem 14.8. *If G is a p-group of order p^n for some $n \geqslant 1$, then $Z(G)$ is non-trivial.*

Proof. Use the class equation. If $\mathcal{O} \in G//G$ is non-central, then $N_G(x_{\mathcal{O}})$ is a proper subgroup of G (so it has order $p^{m_{\mathcal{O}}}$ for some $m_{\mathcal{O}} < n$ by Lagrange's theorem). Thus, using the class equation, we have

$$p^n = |G| = |Z(G)| + \sum_{\mathcal{O} \in G//G \text{ non-central}} p^{n - m_{\mathcal{O}}}.$$

Working modulo p and using that $n - m_{\mathcal{O}} \geqslant 1$ for all non-central conjugacy classes $\mathcal{O}$, we find that $|Z(G)| \equiv 0 \mod p$. So, either $|Z(G)| = 0$ or it is non-trivial. But, $e \in Z(G)$, so $|Z(G)| > 0$ so $Z(G)$ has at least p elements, so it is non-trivial. □

14.1 Exercises

Exercise 14.1. Use Theorem 14.8 to show that if G is a group of order p^2 where p is a prime number, then either $G \cong \mathbf{Z}/p^2$ or $G \cong \mathbf{Z}/p \times \mathbf{Z}/p$. In particular, G is abelian.

Exercise 14.2. Let G be a finite *abelian* group such that $p \mid |G|$ where p is a prime number. Prove that G has an element of order p.

Exercise 14.3. Suppose that $n \geqslant 1$ and let $1 \leqslant n_1 \leqslant n_2 \leqslant \cdots \leqslant n_r \leqslant$ be integers such that $\sum_{i=1}^{r} n_i = n$. (Such a sequence is called a **partition** of n.) Say that an element $g \in S_n$ has cycle type $(n_1, \ldots, n_r)$ if it can be written as a product of *disjoint* cycles of lengths $n_1, \ldots, n_r$. Prove the following statements.

(a) If $f, g \in S_n$ are conjugate, then they have the same cycle types.

(b) If $f, g \in S_n$ have the same cycle types, then they are conjugate.

This proves that the set of conjugacy classes $S_n//S_n$ is in bijection to the set of partitions of n.

15 Cauchy's theorem and Sylow's theorem part 1 (10/27)

Theorem 15.1 (Cauchy's theorem)**.** *Let G be a finite group and p a prime number dividing $|G|$. Then, G has an element of order p.*

Proof. We will use induction and the abelian case of the theorem established in Exercise 14.2. Assume the result is true for all groups of order less than $|G|$. Note that it is true for groups of order 1, trivially. Recall the class equation

$$|G| = |Z(G)| + \sum_{\mathcal{O} \in G//G \text{ non-central}} |G : N_G(x_{\mathcal{O}})|,$$

where $x_{\mathcal{O}} \in \mathcal{O}$. If some normalizer $N_G(x_{\mathcal{O}})$ has order divisible by p, then it has an element of order p by our inductive hypothesis. Thus, assume that $N_G(x_{\mathcal{O}})$ has no element of order p for any of the non-central conjugacy classes $\mathcal{O}$. It follows from the inductive hypothesis that p does not divide $|N_G(x_{\mathcal{O}})|$ so that p *does* divide the index $|G : N_G(x_{\mathcal{O}})|$. Thus, since p also divides $|G|$, p must divide $|Z(G)|$. But, $|Z(G)| > 1$, so that $Z(G)$ is an abelian group whose order is divisible by p. By the special case of Cauchy's theorem for abelian groups, $Z(G)$ has an element of order p, which is also of order p in G. □

Question 15.2. Having established that there are elements of order p in groups whose order is divisible by p, it is natural to ask about subgroups of other types. Specifically, if $|G| = p^r n$ where $(n, p) = 1$, is there a subgroup of G of order p^r?

Definition 15.3 (p-Sylow subgroups)**.** If G has order $p^r n$ where p is a prime, $r \geqslant 0$, and $(p, n) = 1$, then any subgroup of G of order p^r is called a p**-Sylow** subgroup. The previous question asks if p-Sylow subgroups exist.

Remark 15.4. The next result is the first part of the Sylow theorems. It establishes the existence of p-Sylow subgroups. Later, we will prove that all p-Sylow subgroups are conjugate (and hence isomorphic) and give a way to count them.

Theorem 15.5 (Sylow 1)**.** *Suppose that G is a finite group of order $p^r n$ where p is a prime, $r \geqslant 0$, and $(p, n) = 1$. Then, G contains a p-Sylow subgroup.*

Proof. The theorem trivially holds when G is the trivial group, of order 1. Assume that it holds for all groups of order less than $|G| = p^r n$. If p divides the order of $Z(G)$, then there is a central element of G of order p. This element generates a cyclic subgroup $N \subseteq Z(G)$ isomorphic to $\mathbf{Z}/p$. Since it is a subgroup of $Z(G)$, it is normal. The quotient G/N has order $p^{r-1}n$, which is less than $p^r n$. By the inductive hypothesis, G/N has a p-Sylow subgroup Q of order p^{r-1}. Writing $f\colon G \to G/N$ for the quotient map, $f^{-1}(Q)$ is a p-Sylow subgroup of G.

Now, suppose that p does not divide the order of $Z(G)$. Then, since p divides $|G|$, the class equation implies that for some non-central orbit $\mathcal{O}$, p does not divide $|G : N_G(x_{\mathcal{O}})|$. But, this means that $|N_G(x_{\mathcal{O}})| = p^r m$ for some m prime-to-p. By induction, $N_G(x_{\mathcal{O}})$ contains a p-Sylow subgroup of order p^r, which is then a p-Sylow subgroup in G as well. □

Example 15.6. Let $G = S_3$. There are three 2-Sylow subgroups isomorphic to $\mathbf{Z}/2$, each generated by a transposition, and one 3-Sylow subgroup.

Example 15.7. Let p be a prime. In the dihedral group D_{2p}, there is a unique p-Sylow subgroup, which is normal, generated by the rotation r of angle $\frac{2\pi}{p}$. How many 2-Sylow subgroups are there? Each sr^a has order 2 as $(sr^a)(sr^a) = s^2 r^{-a} r^a = e$. There are thus 2-Sylow subgroups for each $s, sr, \ldots, sr^{p-1}$, so there are p of them.

15.1 Exercises

Exercise 15.1. Let p be a prime number and let $p \leqslant n \leqslant 2p-1$. Describe the p-Sylow subgroups of S_n, including how many there are.

Exercise 15.2. Describe the Sylow subgroups of D_{12}.

Exercise 15.3 (From Herstein)**.** Prove that a group of order 108 contains a normal subgroup of order 9 or 27.

Exercise 15.4. Let G be a finite *abelian* group of order $p_1^{r_1} \cdots p_k^{r_k}$. Let $P_1, \ldots, P_k$ be p_i-Sylow subgroups of G for $1 \leqslant i \leqslant k$. Show that G is isomorphic to the product $P_1 \times P_2 \times \cdots \times P_k$, consisting of k-tuples $(a_1, \ldots, a_k)$ where $a_i \in P_i$ for $1 \leqslant i \leqslant k$.

16 Statement of Sylow's theorem parts 2 and 3 (10/30)

Definition 16.1 (Normalizers)**.** If G is a group and $S \subseteq G$ is a subset, let $N_G(S) = \{g \in G : gSg^{-1} = S\}$. This is called the **normalizer** of S in G. If $x \in G$, then $N_G(x) = N_G(\{x\})$, where it is often also called the *centralizer* of x in G. We will be interested below in normalizers of subgroups of G. Note that if P is a subgroup of G, then P is a subgroup of $N_G(P)$. In fact, P is a normal subgroup of $N_G(P)$.

Remark 16.2. Given a group G, a subgroup $H \subseteq G$, and an element $g \in G$, the conjugate gHg^{-1} is another subgroup of G. (In fact, it is isomorphic abstractly as a group to H.) If P is a p-Sylow subgroup, then gPg^{-1} is another p-Sylow subgroup. Thus, G acts by conjugation on the set $\mathrm{Syl}_p(G)$ of p-Sylow subgroups of G.

Theorem 16.3 (Sylow parts 2 and 3)**.** *Let G be a finite group and fix a prime p. Fix a p-Sylow subgroup P of G.*

(2) *If Q is any p-subgroup of G, then $Q \subseteq gPg^{-1}$ for some $g \in G$. Thus, any two p-Sylow subgroups of G are conjugate.*

(3) *Let n_p be the number of p-Sylow subgroups of G. Then,*

$$n_p = [G : N_G(P)] \equiv 1 \mod p.$$

Of crucial import in studying a group G is the question of whether it has a normal p-Sylow subgroup P. If $|G| = p^r n$ where $(p, n) = 1$ and if $P \subseteq G$ is a *normal* p-Sylow subgroup, then G/P is a group of order n and we have excised the "p-part" from G and simplified our lives.

Example 16.4. Suppose that G is a group of order $56 = 2^3 \cdot 7$. Then, $n_7 \equiv 1 \mod 7$, while $[G : N_G(P_7)]$ is $1, 2, 4, 8$, where P_7 is a 7-Sylow. Since $n_7 \equiv 1 \mod 7$, it follows that n_7 is either 1 or 8. Note that any 7-Sylow subgroup is isomorphic to $\mathbf{Z}/7$. If there are 8 distinct 7-Sylow subgroups, then this gives $8 \cdot 6 = 48$ elements of order 7 in G. Now, let P_2 be a 2-Sylow subgroup. There are 8 elements in P_2 and as $48 + 8 = 56$, it follows that every element of G is either in a 7-Sylow or in P_2. In particular, there is only one 2-Sylow subgroup, which must be normal. In summary, a group of order 56 either has a normal 7-Sylow subgroup or it has a normal 2-Sylow subgroup. (It could have both, as in the case of $\mathbf{Z}/7 \times \mathbf{Z}/8$.)

The following lemma will be used in the proofs of the remaining parts of the Sylow theorems.

Lemma 16.5. *Let G be a finite group, p a prime number, $P \subseteq G$ a p-Sylow subgroup, and $Q \subseteq G$ a sub-p-group. Then, $P \cap Q = N_G(P) \cap Q$.*

Proof. Set $H = N_G(P) \cap Q$. I claim that $PH = HP$, which follows from the fact that every element of H normalizes P. It follows that PH is a subgroup of G. But,

$$|PH| = \frac{|P||H|}{P \cap H}.$$

As H and P are p-groups, it follows that PH is a p-group containing P. But, it must then be isomorphic to P since P has the largest possible p-power order of subgroups of G by Lagrange's theorem. So, $PH = P$, which implies that $H \subseteq P$. Since $H \subseteq Q$ as well, it follows that $N_G(P) \cap Q \subseteq P \cap Q$. The other inclusion follows from the fact that $P \subseteq N_G(P)$. □

16.1 Exercises

Exercise 16.1. Let p be a prime and let n be any integer satisfying $p \leqslant n \leqslant p^2 - 1$. Compute the isomorphism type of the p-Sylow subgroup of S_n.

Exercise 16.2. Using Exercises 16.1 and Exercise 14.3, find the number of p-Sylow subgroups of S_n when n is a prime and $n = p(p-1)$.

Exercise 16.3 (Herstein)**.** Prove, using all the Sylow theorems, that if G has order 42, then its 7-Sylow subgroup is normal.

Exercise 16.4. Show that if H and K are subgroups of G such that HK is a subgroup, then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

17 Proofs of Sylow's theorem parts 2 and 3 (11/01)

Lemma 17.1. *Let G be a finite group, p a prime number, $P \subseteq G$ a p-Sylow subgroup, and $Q \subseteq G$ a sub-p-group. Then, $P \cap Q = N_G(P) \cap Q$.*

Theorem 17.2 (Sylow parts 2 and 3)**.** *Let G be a finite group and fix a prime p. Fix a p-Sylow subgroup P of G.*

(2) *If Q is any p-subgroup of G, then $Q \subseteq gPg^{-1}$ for some $g \in G$. Thus, any two p-Sylow subgroups of G are conjugate.*

(3) *Let n_p be the number of p-Sylow subgroups of G. Then,*

$$n_p = [G : N_G(P)] \equiv 1 \mod p.$$

Proof. Let $X = \{P = P_1, \dots, P_k\}$ be the set of conjugates of P in G. This set is non-empty by because it contains P and it is finite because G has only finitely many subgroups. Let $\mathrm{Syl}_p(G)$ be the set of p-Sylow subgroups of G. We want, among other things, to show that $X = \mathrm{Syl}_p(G)$ and to show that G acts transitively on $\mathrm{Syl}_p(G)$ under conjugation. Let $Q \subseteq G$ be a p-subgroup of G. Then, Q acts on X by conjugation. While G acts transitively on X (by definition), we do not know that about Q. So, let $X = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \cdots \sqcup \mathcal{O}_r$ be the partition of X into disjoint orbits for the conjugation action of Q. Let $P_{\mathcal{O}_i} \in \mathcal{O}_i$ be a representative. This means that $P_{\mathcal{O}_i} \in X$ (so that is conjugate to P via an element of G) and its orbit under the conjugation action of Q is $\mathcal{O}_i$. Of course,

$$|\mathcal{O}_i| = [Q : N_Q(P_{\mathcal{O}_i})] = [Q : P_{\mathcal{O}_i} \cap Q],$$

where $N_Q(P_{\mathcal{O}_i})$ is defined to be $N_G(P_{\mathcal{O}_i}) \cap Q$ and where we use Lemma 17.1 for the second equality.

The paragraph above works for any p-group Q. Then, the orbit of X containing P_1 under conjugation by P_1 is just $\{P_1\}$. Call this orbit $\mathcal{O}_1$. If $\mathcal{O}_i$ is another orbit, so $2 \leqslant i \leqslant r$, then $P_{\mathcal{O}_i} \cap P_1$ is a proper subset of P_1, since otherwise they would be equal subgroups. Thus, $|\mathcal{O}_i| = [P_1 : P_{\mathcal{O}_i} \cap P_1]$ is a power of p. So,

$$|X| = \sum_{i=1}^{r} |\mathcal{O}_1| = 1 + pN$$

for some N. Therefore,

$$k \equiv 1 \mod p.$$

Now, let Q be an arbitrary non-trivial sub-p-group of G. Assume that Q is not contained in any p-Sylow subgroup of G and in particular in no member of X. Then, $P_i \cap Q$ is a proper subgroup of Q for all $i = 1, \dots, k$. Therefore, in the orbit decomposition, $p \mid |Q : N_Q(P_{\mathcal{O}_i})|$ for all $1 \leqslant i \leqslant r$. But, by the class formula for actions, this implies that $p \mid |X| \equiv 1 \mod p$, which is a contradiction. This proves that Q is contained in a member of X. As this applies also to other p-Sylow subgroups of G, we see that in fact X is a complete list of the p-Sylow subgroups and that every p-Sylow subgroup of G is conjugate to P. This proves (2).

It also proves that $n_p = k \equiv 1 \mod p$. Now, using orbit decomposition again, since the action of G on $\mathrm{Syl}_p(G)$ is transitive, we find that $n_p = \frac{|G|}{|N_G(P)|} = [G : N_G(P)]$. This completes the proof. □

Corollary 17.3. *Any two p-Sylow subgroups of a finite group are isomorphic as groups.*

Proof. By Theorem 17.2, it is enough to show that conjugate subgroups are isomorphic. Let G be a group, let $P, Q \subseteq G$ be subgroups, and let $g \in G$. If $gPg^{-1} = Q$, then $P \cong Q$. Let $c\colon P \to Q$ be defined by $c(h) = ghg^{-1}$. This is a group homomorphism because $c(hk) = ghkg^{-1} = ghg^{-1}ghg^{-1} = c(h)c(k)$. It is injective because if $c(h) = e$, it follows that $ghg^{-1} = e$ or $h = g^{-1}g = e$. It is surjective because given $k \in Q$ the element $g^{-1}kg$ is in P and $c(g^{-1}kg) = k$. □

Warning 17.4. We are *not* saying that any two p-Sylow subgroups are equal as subgroups, i.e. that they have the same elements. We are saying that they are isomorphic as abstract groups.

Corollary 17.5. *If G is a finite group and p is a prime and G has a normal p-Sylow subgroup P, then P is the only p-Sylow subgroup. Conversely, if P is the only p-Sylow subgroup in G, then it is normal.*

Proof. If P is normal, then $N_G(P) = P$ so $n_p = 1$. Conversely, if $n_p = 1$, then $[G : N_G(P)] = 1$, so $N_G(P) = G$ and P is normal in G. □

Example 17.6 (Groups of order pq)**.** Let $p < q$ be distinct prime numbers. Let G be a group of order pq. I claim that G has a normal subgroup of order q. Note that this is precisely what happens for S_3 which has a normal subgroup of order 3. Suppose that $p < q$. If Q is not normal, then $N_G(Q) = Q$ and $1 \neq n_q = p \equiv 1 \mod q$, which is impossible and gives a contradiction.

Example 17.7 (From Dummit–Foote)**.** Prove that a group G of order 200 has a normal 5-Sylow subgroup. (Note there are 52 such groups!) We have that $200 = 8 * 25 = 2^3 * 5^2$. We have $n_5 \equiv 1 \mod 5$ and is equal to one of $1, 2, 4, 8$. It must be 1, so there is one 5-Sylow subgroup, which is necessarily normal.

17.1 Exercises

Exercise 17.1. Prove that a group of order $2 \leqslant |G| \leqslant 20$ is either of prime order or has a nontrivial normal subgroup.

n

Exercise 17.2. Prove that a group of order 99 has a normal 11-Sylow subgroup.

18 Matrix groups (11/03)

Definition 18.1. Let k be a field (such as $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, or $\mathbf{F}_p = \mathbf{Z}/p$ for some prime number p) or even a commutative ring (such as $\mathbf{Z}$). Let $n \geqslant 0$ and let $\mathrm{M}_n(k)$ be the set of all $n \times n$-matrices with coefficients in k. We make $\mathrm{M}_n(k)$ into a magma via the binary operation of matrix multiplication. If M and N are $n \times n$-matrices, then the ijth entry of MN is

$$\sum_{k=1}^{n} M_{ik} N_{kj}.$$

It easy to see that this is a unital magma with identity element I_n, the diagonal matrix with 1s on the diagonal. It is less pleasant to see directly from the definition that matrix multiplication is associative.

Lemma 18.2. *Matrix multiplication makes* $\mathrm{M}_n(k)$ *into a monoid.*

Proof. We have already observed that there is a two-sided identity element I_n. To prove associativity we argue as follows. We can identify $\mathrm{M}_n(k)$ as the set of linear transformations $F\colon k^n \to k^n$, where k^n is the n-dimensional vector space over k equipped with the standard basis $e_1, \ldots, e_n$. Then, recall that M corresponds to the linear transformation $F(e_j) = \sum_{i=1}^{n} m_{ij} e_j$. Linear transformations are certain functions from k^n to itself. Thus, we have an inclusion of sets $\mathrm{M}_n(k) \to \mathrm{Fun}(k^n, k^n)$, where the right-hand side is the set of *all* functions $k^n \to k^n$. The right-hand side has a natural magma structure given by composition of functions. This magma is in fact a monoid. The identity element is the identity function; associativity follows from the fact that function composition is associative. Now, the inclusion $\mathrm{M}_n(k) \to \mathrm{Fun}(k^n, k^n)$ is a magma homomorphism that sends I_n to the identity element. As this homomorphism of magmas is injective and as $\mathrm{Fun}(k^n, k^n)$ is associative, it follows that $\mathrm{M}_n(k)$ is associative too. □

Remark 18.3. For commutative rings k a similar argument works, but one replaces the phrase "vector space" with k-module. Alternatively, for a ring like $\mathbf{Z}$, one can use the inclusion $\mathrm{M}_n(\mathbf{Z}) \subseteq \mathrm{M}_n(\mathbf{Q})$.

Lemma 18.4. *If M is a monoid and $U \subseteq M$ is the subset of elements of M with a two-sided inverse, then U is a group, called the maximal subgroup of M.*

Proof. As U contains the identity element and every element of U has an inverse, it is enough to show that U is closed under multiplication in M (as then associativity follows from that of M). But, if $u, v \in U$ with two-sided inverses u^{-1} and v^{-1}, then uv has two sided inverse $v^{-1}u^{-1}$ by associativity. □

Definition 18.5. If k is a field (or a ring), then $\mathbf{GL}_n(k) \subseteq \mathrm{M}_n(k)$ is the maximal subgroup of $\mathrm{M}_n(k)$. I.e., $\mathbf{GL}_n(k)$ consists of those matrices with a two-sided inverse.

Remark 18.6. Recall the determinant function $\det\colon \mathrm{M}_n(k) \to k$. It satisfies $\det(MN) = \det(M)\det(N)$ and is thus a monoid homomorphism (where k is equipped with the multiplicative monoid structure). The invertible matrices are precisely those M such that $\det(M)$ is a unit in k. The restriction of det to $\mathbf{GL}_n(k)$ induces a surjective group homomorphism $\det\colon \mathbf{GL}_n(k) \to k^\times$.

Definition 18.7. We let $\mathbf{SL}_n(k) = \ker(\det)$. It is the subgroup of invertible matrices whose determinant is 1.

Lemma 18.8. *The center of* $\mathbf{GL}_n(k)$ *consists of the matrices uI_n where $u \in k^\times$.*

Example 18.9 (Order of $\mathbf{GL}_2(\mathbf{F}_p)$)**.** Consider a prime p and the finite group $\mathbf{GL}_2(\mathbf{F}_p)$. First, what is its order? Well, $\mathbf{GL}_2(\mathbf{F}_p)$ is also the set of group homomorphisms $\mathbf{Z}/p \times \mathbf{Z}/p \to \mathbf{Z}/p \times \mathbf{Z}/p$ and so it acts on the non-zero elements of $\mathbf{Z}/p \times \mathbf{Z}/p$ of which there are $p^2 - 1$. What is the stabilizer of $(1, 0)$? Solving

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

we see that the stabilizer consists of those invertible matrices such that $a = 1$ and $c = 0$. Thus, since such a matrix has $\det(M) = d$, we have that $d \in k^\times$ and b can be anything. Thus, there are $p(p-1)$ elements in the stabilizer. It follows that

$$|\mathbf{GL}_2(\mathbf{F}_p)| = p(p-1)^2(p+1).$$

Note that $\mathbf{GL}_n(\mathbf{F}_p)$ is non-abelian for $n \geqslant 2$. In particular, we have $|\mathbf{GL}_2(\mathbf{F}_2)| = 6$ and thus it must be isomorphic to S_3. This corresponds to the permutations of the 3 non-zero elements of $\mathbf{Z}/2 \times \mathbf{Z}/2$.

Example 18.10 (p-Sylow subgroups of $\mathbf{GL}_2(\mathbf{F}_p)$)**.** Fix a prime p and let P be a p-Sylow subgroup of $\mathbf{GL}_2(\mathbf{F}_p)$. We see from the computation of the order that $P \cong \mathbf{Z}/p$. How many p-Sylows are there? We can write down one as

$$P = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\},$$

where $*$ can be any element of $\mathbf{F}_p$. This is *not* normal. What's the easiest way to see this? Well,

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

is another order p element not in P! So, $n_p > 1$. Let's see the stabilizer of $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ under conjugation. We solve

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

subject to the constraint that $ad - bc \neq 0$. We get

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

which implies $c = 0$, $a = d$, and $a^2 \neq 0$, or $a \neq 0$. So, these are the matrices of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a \neq 0$. There are $(p-1)p$ of these. Thus, it follows that there are $(p-1)(p+1) = \frac{|\mathbf{GL}_2(\mathbf{F}_p)|}{(p-1)p}$ conjugates of u. What happens if instead we solve for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

for $1 \leqslant k \leqslant p-1$? We get

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+kc & b+kd \\ c & d \end{pmatrix},$$

which implies $kc = 0$, which implies $c = 0$ and $a = kd$, with $d \neq 0$. These are the matrices of the form

$$\begin{pmatrix} kd & b \\ 0 & d \end{pmatrix}.$$

In particular, the powers u^k of u are indeed conjugate to u. It follows finally that there are $p+1$ subgroups obtained by conjugating P and hence $n_p = p+1$. (This matches up out with our knowledge that $S_3 \cong \mathbf{GL}_2(\mathbf{F}_2)$ has 3 2-Sylow subgroups.)

18.1 Exercises

Exercise 18.1. Let k be a field. Show that the center of $\mathbf{GL}_n(k)$ consists of the matrices uI_n where $u \in k^\times$.

Exercise 18.2. Let p be a prime. Determine the center of $\mathbf{SL}_2(\mathbf{F}_p)$.

Exercise 18.3. Fix a prime number p. Let $\mathbf{PGL}_n(\mathbf{F}_p)$ be the quotient of $\mathbf{SL}_n(\mathbf{F}_p)$ by its center. Compute the order of $\mathbf{PGL}_2(\mathbf{F}_p)$.[1]

Exercise 18.4. Find the number of p-Sylow subgroups in $\mathbf{SL}_2(\mathbf{F}_p)$.

Exercise 18.5. Find the number of p-Sylow subgroups in $\mathbf{PGL}_2(\mathbf{F}_p)$.

[1] Arguably a better definition of $\mathbf{PGL}_n(\mathbf{F}_p)$ is as the quotient of $\mathbf{GL}_n(\mathbf{F}_p)$ by *its* center, but this is the standard definition in the field of group theory. Are these two groups isomorphic?

19 Automorphisms (11/06)

19.1 ϵ more on matrix groups

There are many other types of matrix groups one can cook up.

Example 19.1 (Upper-triangular matrices)**.** Let $\mathbf{B}_n(k) \subseteq \mathbf{GL}_n(k)$ be the subgroup of invertible upper-triangular matrices. The order of $\mathbf{B}_2(\mathbf{F}_p)$ is $p(p-1)^2$. There is also the group of special upper-triangular matrices, i.e., the subgroup of $\mathbf{SB}_n(k)$ of elements with determinant 1. The order of $\mathbf{SB}_2(\mathbf{F}_p)$ is $p(p-1)$.

Example 19.2 (Unipotent matrices)**.** Let $\mathbf{U}_n(k) \subseteq \mathbf{GL}_n(k)$ be the subgroup of upper-triangular matrices with 1s on the diagonal. The order of $\mathbf{U}_2(\mathbf{F}_p)$ is p. The order of $\mathbf{U}_3(\mathbf{F}_p)$ is p^3.

19.2 The dream of finite groups

We now have at our disposal the powerful Sylow theorems to help us understand finite groups. With them, we can prove the existence of large p-groups inside a given group, if p divides the order, and in some situations these large p-groups are normal. In addition, the structure of p-groups seems to be somewhat tractable as the center of a non-trivial p-group is always non-trivial.

Understanding finite groups and their classification now boils down to two main problems,

(a) to understand the finite simple groups, i.e., those with no non-trivial normal subgroups, and

(b) to understand how to build every group out of simple groups;

together with these I will add the problem

(c) of understanding the p-groups and hence all possible p-Sylow subgroups.

We will not complete this task in this course and in fact the task is as of yet incomplete for humanity as a whole. However, in the 1980s, mathematicians did complete task (a), the classification of all finite simple groups. There are infinitely many (such as the $\mathbf{Z}/p$ for primes p), but they sit inside certain specific families except for finitely many exceptions.

19.3 Automorphisms

In general, it is difficult to say how a group is "built up out of" its subgroups. But, there is one important exception that we will discuss this week, namely the semidirect products. To understand these, we first have to say a little bit about automorphisms of groups.

Definition 19.3 (Automorphisms)**.** Given a group G, and **automorphism** of G is bijective group homomorphism (or, group isomorphism) $f\colon G \to G$.

Definition 19.4. Give a group G, we write $\mathrm{Aut}(G)$ for the group of automorphisms of G. That is,

$$\mathrm{Aut}(G) = \{f\colon G \to G \mid f \text{ is a group isomorphism}\}.$$

This is a group under composition.

Remark 19.5. We can view $\mathrm{Aut}(G)$ as sitting inside S_G. Whereas S_G consists of all permutations of G, or all functions $f\colon G \to G$, the group $\mathrm{Aut}(G)$ consists of only those permutations that behave well with respect to the group structure on G.

Example 19.6. The group $\mathrm{Aut}(\mathbf{Z})$ is isomorphic to $\{\pm 1\} \cong \mathbf{Z}/2$. Indeed, a group homomorphism $f\colon \mathbf{Z} \to \mathbf{Z}$ is determined by where it sends 1. It is a group isomorphism if and only if it sends 1 to 1 or -1 in $\mathbf{Z}$.

Example 19.7. The only automorphism of $\mathbf{Z}/2$ is the identity. Thus, $\mathrm{Aut}(\mathbf{Z}/2) = \{\mathrm{id}_{\mathbf{Z}/2}\}$ is the trivial group.

Example 19.8. An automorphism of $\mathbf{Z}/3$ can send 1 to 1 or to 2. Thus, $\mathrm{Aut}(\mathbf{Z}/3) \cong \mathbf{Z}/2$.

Example 19.9. An automorphism of $\mathbf{Z}/4$ can send 1 to either 1 or 3. Again, $\mathrm{Aut}(\mathbf{Z}/4) \cong \mathbf{Z}/2$.

19.4 Exercises

Exercise 19.1. Determine the number of p-Sylow subgroups in $\mathbf{B}_2(\mathbf{F}_p)$.

Exercise 19.2. Compute the order of $\mathbf{GL}_n(\mathbf{F}_p)$ following the idea of Example 18.9.

Exercise 19.3. Justify the claim in Example 19.6. Specifically, show that if $f\colon \mathbf{Z} \to \mathbf{Z}$ is an automorphism, then $f(1) = 1$ or -1.

Exercise 19.4. Compute the order of $\mathrm{Aut}(\mathbf{Z}/n)$ for all $n \geqslant 2$.

20 Inner and outer automorphisms (11/08)

20.1 More on automorphisms

Lemma 20.1. *There is a homomorphism $c\colon G \to \mathrm{Aut}(G)$ given by sending $g \in G$ to conjugation by g, denoted by c_g. The kernel is $Z(G)$, the center of G.*

Proof. Given $g \in G$, the function $c_g\colon G \to G$ is a bijective group homomorphism. It follows that $g \mapsto c_g$ defines a *function* $G \to \mathrm{Aut}(G)$. To see that this is a group homomorphism, it is enough to check that

$$(c_g \circ c_h)(x) = c_g(c_h(x)) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = c_{gh}(x),$$

for all $g, h, x \in G$. If $g \in Z(G)$, then $c_g(x) = gxg^{-1} = xgg^{-1} = x$, so c_g is the identity automorphism. Conversely, if $c_g = \mathrm{id}_G$, then $gxg^{-1} = x$ for every $x \in G$; in other words, g is in the center. □

Definition 20.2. The image of $c\colon G \to \mathrm{Aut}(G)$ is called $\mathrm{Inn}(G)$. It is a subgroup of $\mathrm{Aut}(G)$. Automorphisms in $\mathrm{Inn}(G)$ are called **inner automorphisms**.

Example 20.3. If G is abelian, then $Z(G) = G$ and $\mathrm{Inn}(G) = G/Z(G)$ is trivial.

Lemma 20.4. *The subgroup $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$ is normal. Specifically, if $g \in G$ and $\sigma \in \mathrm{Aut}(G)$, then $\sigma \circ c_g \circ \sigma^{-1} = c_{\sigma(g)}$.*

Proof. Given $x \in G$ we have

$$(\sigma \circ c_g \circ \sigma^{-1})(c) = \sigma(c_g(\sigma^{-1}(x))) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g^{-1}) = \sigma(g)x\sigma(g)^{-1} = c_{\sigma(g)}(x).$$

Thus, $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$ as claimed. □

Definition 20.5 (Outer automorphisms)**.** The quotient of $\mathrm{Aut}(G)$ by $\mathrm{Inn}(G)$ is the group of **outer automorphisms**. Note that, despite the name, the elements of $\mathrm{Out}(G)$ are not, in fact, automorphisms of G but are $\mathrm{Inn}(G)$-cosets of automorphisms.

Definition 20.6 (Characteristic subgroups)**.** A subgroup $H \subseteq G$ is **characteristic** if for every automorphism $\sigma \in \mathrm{Aut}(G)$ one has $\sigma(H) = H$.

Remark 20.7. A characteristic subgroup $H \subseteq G$ is necessarily normal. A normal subgroup is characteristic if every outer automorphism preserves H.

Example 20.8. The center $Z(G)$ of a group G is characteristic.

Example 20.9. A *normal* p-Sylow subgroup of a finite group is characteristic.

Example 20.10. Let $G = \mathbf{Z}/p \times \mathbf{Z}/p$. Every subgroup of G is normal since G is abelian. However, the only characteristic subgroups of G are trivial. To see this, note that $\mathrm{Aut}(G) = \mathbf{GL}_2(\mathbf{F}_p)$. This group acts transitively on the group of non-zero vectors in G. So, no subgroup of order p is fixed by $\mathrm{Aut}(G)$. For concreteness, assume that $H \subseteq G$ is the group of order p generated by the element $(1, 0)$. The element

$$\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

implements the "switch" automorphism $\sigma(a, b) = (b, a)$, And, $H \subseteq G$ is not fixed by σ.

Remark 20.11. In the situation of Example 20.10, $\mathrm{Inn}(G)$ is trivial, so $\mathrm{Aut}(G) \cong \mathrm{Out}(G)$.

20.2 Extensions

Definition 20.12 (Extensions)**.** An extension of a group H by a group N is a sequence

$$1 \to N \to G \to H \to 1$$

of group homomorphisms called an exact sequence (or a short exact sequence). Each arrow is a homomorphism of groups and at each point in the diagram we have ker = im. This is a short-hand way of expressing the following:

(a) $N \to G$ is injective,

(b) $G \to H$ is surjective,

(c) the kernel of $G \to H$ is N, and hence

(d) $G/N \cong H$.

Remark 20.13. In the notation for an exact sequence "1" denotes the trivial group $\{e\}$.

Example 20.14. If N is a normal subgroup of G there is an exact sequence

$$1 \to N \to G \to G/N \to 1,$$

and G is an extension of G/N by N.

Example 20.15. We can write S_3 as an extension of $\mathbf{Z}/2$ by $\mathbf{Z}/3$, resulting in $1 \to \mathbf{Z}/3 \to S_3 \to \mathbf{Z}/2 \to 1$. We *cannot* express S_3 as an extension of $\mathbf{Z}/3$ by $\mathbf{Z}/2$ because S_3 has no normal 2-Sylow subgroups.

Example 20.16. There is an exact sequence

$$1 \to \mathbf{Z}/3 \to \mathbf{Z}/6 \to \mathbf{Z}/2 \to 1.$$

Unlike for S_3, there is *also* an exact sequence

$$1 \to \mathbf{Z}/2 \to \mathbf{Z}/6 \to \mathbf{Z}/3 \to 1.$$

Remark 20.17. In the ideal case when attempting to understand a group G one expresses G as the middle term of an exact sequence, and hence as an extension of G/N by a normal subgroup N. Understanding N and G/N and how they are "glued together" in the exact sequence leads to an understanding of G. The puzzle of finite group theory is that there *are* simple groups, even simple non-abelian groups as we will see, which by definition foil this approach.

20.3 Exercises

Exercise 20.1. Compute $\mathrm{Inn}(\mathbf{Z}/n)$, $\mathrm{Aut}(\mathbf{Z}/n)$, and $\mathrm{Out}(\mathbf{Z}/n)$ for any $n \geqslant 2$.

Exercise 20.2. Compute $\mathrm{Inn}(D_{2n})$, $\mathrm{Aut}(D_{2n})$, and $\mathrm{Out}(D_{2n})$, where D_{2n} is the dihedral group of order $2n$ for $n \geqslant 3$.

21 Semidirect products (11/10)

Construction 21.1 (The normal action)**.** Let G be a group and let N be a normal subgroup, with automorphism group $\mathrm{Aut}(N)$. Then, conjugation induces a group homomorphism

$$G \to \mathrm{Aut}(N),$$

which we will also denote by $g \mapsto c_g$. The kernel of $c_g \colon G \to \mathrm{Aut}(N)$ is

$$C_G(N) = \{g \in G \mid gng^{-1} = n \text{ for all } n \in N\},$$

which is a subgroup of $N_G(N)$. The group $C_G(N)$ is called the centralizer of N in G.

Example 21.2 (Normal abelian subgroups)**.** A very important example of the previous construction is when the normal subgroup $N \subseteq G$ is abelian. In this case, N is in the kernel of $G \to \mathrm{Aut}(N)$ and so there is an induced homomorphism $G/N \to \mathrm{Aut}(N)$.

Example 21.3 (The center)**.** The center $Z(G) \subseteq G$ is always normal, but the homomorphism $G \to \mathrm{Aut}(Z(G))$ is trivial, so one does not learn much from this construction in this case.

Example 21.4 (The dihedral reflection)**.** Consider the dihedral group D_{2n} as an extension

$$1 \to \mathbf{Z}/n \to D_{2n} \to \mathbf{Z}/2 \to 1$$

of $\mathbf{Z}/2$ by $\mathbf{Z}/n$. As the normal subgroup $\mathbf{Z}/n$ is abelian, there is an induced group homomorphism $D_{2n}/(\mathbf{Z}/n) \cong \mathbf{Z}/2 \to \mathrm{Aut}(\mathbf{Z}/n)$. This homomorphism corresponds to multiplication by -1.

Notation 21.5. If σ is an automorphism of G and $g \in G$ we write g^σ for $\sigma(g)$.

Construction 21.6. Let $\varphi \colon H \to \mathrm{Aut}(N)$ be a group homomorphism. We define a group structure, denoted by $N \rtimes_\varphi H$ or $N \rtimes H$, on the set $N \times H$ by decreeing that

$$(n_0, h_0) \cdot (n_1, h_1) = (n_0 n_1^{\varphi(h_0)}, h_0 h_1).$$

Lemma 21.7. *Given $\varphi \colon H \to \mathrm{Aut}(N)$, the binary operation on $N \rtimes_\varphi H$ makes it into a group.*

Proof. The operation has an identity element (e_N, e_H). The inverse of (n, h) is $((n^{-1})^{\varphi(h)^{-1}}, h^{-1})$ as

$$(n,h)((n^{-1})^{\varphi(h)^{-1}}, h^{-1}) = (n((n^{-1})^{\varphi(h)^{-1}})^{\varphi(h)}, hh^{-1}) = (nn^{-1}, hh^{-1}) = (e_N, e_H),$$

and the other order is the same. We leave associativity for the reader as Exercise 21.1. □

Lemma 21.8. *Given a group homomorphism $\varphi \colon H \to \mathrm{Aut}(N)$, the semidirect product $N \rtimes_\varphi H$ fits into an exact sequence*

$$1 \to N \xrightarrow{i} N \rtimes_\varphi H \xrightarrow{q} H \to 1.$$

In particular, $N \subseteq N \rtimes_\varphi H$ is normal.

Proof. We define i by $i(n) = (n, e_H)$. This defines a group homomorphism as

$$i(n_0)i(n_1) = (n_0, e_H)(n_1, e_H) = (n_0(n_1)^{\varphi(e_H)}, e_H^2) = (n_0 n_1, e_H) = i(n_0 n_1).$$

as $\varphi(e_H)$ is the identity automorphism. The group homomorphism i is injective, by definition of $N \rtimes_\varphi H$. We identify N with its image under i. This subgroup is normal. Rather than check this directly, we check that $i(N)$ is the kernel of a homomorphism q, which is defined by $q(n, h) = h$. That q is a homomorphism follows from the definition of multiplication on $N \rtimes_\varphi H$. The kernel of q consists of those elements (n, h) of $N \rtimes_\varphi H$ where $h = e_H$. But, this is precisely N. In particular, N is normal. Since q is also surjective, the lemma is complete. □

Definition 21.9 (Split extensions)**.** An exact sequence

$$1 \to N \xrightarrow{i} G \xrightarrow{q} H \to 1$$

of groups is **split** if there is a group homomorphism $f\colon H \to G$ such that $q \circ f = \mathrm{id}_H$. We illustrate this as

$$1 \longrightarrow N \xrightarrow[i]{} G \underset{q}{\overset{f}{\rightleftarrows}} H \longrightarrow 1\,.$$

Semidirect products are very special extensions: they are split.

Lemma 21.10. *If $\varphi\colon H \to \mathrm{Aut}(N)$, then the exact sequence*

$$1 \to N \to N \rtimes_\varphi H \to H \to 1$$

is split.

Proof. We define $f\colon H \to N \rtimes_\varphi H$ by $f(h) = (e_N, h)$. Evidently, $q \circ f = \mathrm{id}_H$ and f is a group homomorphism. □

Example 21.11 (Not every extension is split)**.** Consider

$$1 \to \mathbf{Z}/2 \xrightarrow{i} \mathbf{Z}/8 \xrightarrow{q} \mathbf{Z}/4 \to 1.$$

This is extension is not split. Indeed, a group homomorphism $f\colon \mathbf{Z}/4 \to \mathbf{Z}/8$ must send $1 \in \mathbf{Z}/4$ to an element of order dividing 4 in $\mathbf{Z}/8$, i.e., one of $\{0, 2, 4, 6\} \subseteq \mathbf{Z}/8$. As $q(1) = 1$, it follows that $q(f(4))$ is in $\{0, 2\}$, so $q \circ f$ is not the identity. In particular, we see that $\mathbf{Z}/8$ is **not** the semidirect product of $\mathbf{Z}/2$ and $\mathbf{Z}/4$.

Proposition 21.12. (i) *An extension G of H by N is isomorphic to $N \rtimes_\varphi H$ for some $\varphi\colon H \to \mathrm{Aut}(N)$ if and only if the extension*

$$1 \to N \xrightarrow{i} G \xrightarrow{q} H \to 1$$

is split.

(ii) *A group G is isomorphic to a semidirect product $N \rtimes_\varphi H$ if and only if it contains N and H as subgroups with N normal, $N \cap H = \{e\}$, and $NH = G$.*

Proof. We have already seen that if $G \cong N \rtimes_\varphi H$, then the corresponding exact sequence is split. Thus, assume that we have an extension as in (i), split by $f\colon H \to G$. Let φ be the composition $H \xrightarrow{f} G \xrightarrow{c} \mathrm{Aut}(N)$ of f with the normal action homomorphism and set $G' = N \rtimes_\varphi H$. Define a function $a\colon G' \to G$ by $a(n, h) = nf(h)$. This is a group homomorphism as

$$a(n_0(n_1)^{\varphi(h_0)}, h_0h_1) = n_0(n_1)^{\varphi(h_0)}f(h_0h_1) = n_0f(h_0)n_1f(h_0)^{-1}f(h_0)f(h_1) = n_0f(h_0)n_1f(h_1) = a(n_0, h_0)a(n_1, h_1).$$

It is injective as $a(n, h) = nf(h) = e_G$ implies $q(nf(h)) = q(n)q(f(h)) = h = e_H$, so $h = e_H$ and then $n = e_N$. It is surjective as any element of G is isomorphic to $nf(h)$ for some n and h. To see this, fix $g \in G$ and then note that $gf(q(g))^{-1}$ is in N. This completes the proof of (i). The proof of (ii) is left to the reader as Exercise 21.3. □

21.1 Exercises

Exercise 21.1. Prove that if $\varphi\colon H \to \mathrm{Aut}(N)$ is a homomorphism, then the binary operation of Construction 21.6 is associative. This completes the proof of Lemma 21.7.

Exercise 21.2. Let G be a group with subgroups N and H. Find necessary and sufficient conditions for the function $f\colon N \times H \to G$ defined by $f(n, h) = nh$ to be a group isomorphism.

Exercise 21.3. Prove part (ii) of Proposition 21.12.

22 Groups of order pq (11/13)

We need the following theorem as a black box.

Theorem 22.1. *If p is a prime number, then $(\mathbf{Z}/p)^\times$ is cyclic.*

Proof. This proof will be given in the second or third quarters of this course. □

Remark 22.2. It turns out that $(\mathbf{Z}/p)^\times$ is isomorphic to the group of elements of the complex plane $\mathbf{C}$ of the form $e^{\frac{2\pi k}{p-1}}$ where $k = 0, \ldots, p-2$. I do not know of a truly elementary proof of Theorem 22.1, i.e., which does not use certain polynomials in a crucial way.

Corollary 22.3. *If p is a prime number, then $(\mathbf{Z}/p)^\times \cong \mathbf{Z}/(p-1)$.*

Proof. We already know that $(\mathbf{Z}/p)^\times$ has $p-1$ elements; by Theorem 22.1, the corollary follows. □

Example 22.4. We call an element $i \in (\mathbf{Z}/n)^\times$ a multiplicative generator if $(\mathbf{Z}/n)^\times$ is cyclic **and** it is generated by i. For example,

- $(\mathbf{Z}/3)^\times$ is multiplicatively generated by 2;
- $(\mathbf{Z}/5)^\times$ is multiplicatively generated by 2 or 8;
- $(\mathbf{Z}/7)^\times$ is multiplicatively generated by 3 or 5.

Example 22.5 (Groups of order pq)**.** Let $p < q$ be distinct primes. There is a unique abelian group of order pq, up to isomorphism, which is $\mathbf{Z}/(pq) \cong \mathbf{Z}/q \times \mathbf{Z}/p$. When is there a non-abelian group of order pq? This occurs if and only if $p \mid q-1$. Indeed, we know that a group G of order pq has a normal q-Sylow subgroup, say N, which is isomorphic to $\mathbf{Z}/q$. The quotient of G by N is isomorphic to $\mathbf{Z}/p$. So, G is an extension of $\mathbf{Z}/p$ by $\mathbf{Z}/q$. This extension is in fact split. Indeed, G has an element of order p which must map to a non-zero element of the quotient $\mathbf{Z}/p$. By Proposition 21.12, G is isomorphic to $\mathbf{Z}/q \rtimes_\varphi \mathbf{Z}/p$. Now, $\mathrm{Aut}(\mathbf{Z}/q)$ is a group of order $(q-1)$. If p does not divide $q-1$, then the only group homomorphism $\mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/q)$ is the identity and it follows, from Exercise 21.2, that in this case G is the product $\mathbf{Z}/q \times \mathbf{Z}/p$. On the other hand, if p does divide $(q-1)$, then by Cayley's theorem there is an element of $\mathrm{Aut}(\mathbf{Z}/q)$ of order p and hence a non-trivial homomorphism $\varphi\colon \mathbf{Z}/p \to \mathbf{Z}/q$. The associated semidirect product $\mathbf{Z}/q \rtimes_\varphi \mathbf{Z}/p$ is non-abelian.

Example 22.6. There are no non-abelian groups of order 15.

22.1 Exercises

Exercise 22.1. Find multiplicative generators of $\mathbf{Z}/11$ and $\mathbf{Z}/13$.

Exercise 22.2. Show that if p is a prime number, then $(\mathbf{Z}/p^2)^\times$ is cyclic.

Exercise 22.3. Find an integer $n > 1$ such that $(\mathbf{Z}/n)^\times$ is *not* cyclic.

Exercise 22.4. Make a list of the first 10 primes. Then, make a list of all products pq where p and q are on your list such that every group of order pq is abelian. For example, every group of order 15 is abelian.

23 Groups of small order (11/15)

23.1 Groups of order pq

Proposition 23.1. *Suppose that p and q are primes and that p divides $q-1$. There is a unique non-abelian group of order pq up to isomorphism.*

Proof. We have seen most of the proof in the course of Example 22.5. In particular, we have seen that any such group is a semi-direct product $\mathbf{Z}/q \rtimes_\varphi \mathbf{Z}/p$ for *some* $\varphi\colon \mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/q)$ and that there are non-trivial such φ. The only thing that remains to be seen is uniqueness. There are $p-1$ choices of a non-trivial homomorphism $\varphi\colon \mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/q)$, corresponding to the $p-1$ choices of an element of order p in $\mathrm{Aut}(\mathbf{Z}/q) \cong (\mathbf{Z}/q)^\times \cong \mathbf{Z}/(q-1)$. Suppose that φ_0 and φ_1 are two such homomorphism, corresponding to elements $k_0, k_1 \in (\mathbf{Z}/q)^\times$. In particular, there is some integer $c \in \{1, \dots, p-1\}$ such that $k_1^c = k_0$ since they generate the same subgroup. In particular, $c \in (\mathbf{Z}/p)^\times$. Let $G_0 = \mathbf{Z}/q \rtimes_{\varphi_0} \mathbf{Z}/p$ and $G_1 = \mathbf{Z}/q \rtimes_{\varphi_1} \mathbf{Z}/p$. Define a function $f\colon G_0 \to G_1$ as follows. Of course, as sets, both G_0 and G_1 are $\mathbf{Z}/q \times \mathbf{Z}/p$. So, write an element as (a, b). We let

$$f(a, b) = (a, cb).$$

Now, we check that this defines a group homomorphism. On the one hand,

$$f(x_0, y_0)f(x_1, y_1) = (x_0, cy_0) \cdot_{G_1} (x_1, cy_1) = (x_0 + k_1^{cy_0} x_1, cy_0 + cy_1) = (x_0 + k_0^{y_0}, c(y_0 + y_1))$$

since $k_1^{cy_0} = k_0^{y_0}$, and on the other hand

$$f((x_0, y_0) \cdot_{G_0} (x_1, y_1)) = f(x_0 + k_0^{y_0} x_1, y_0 + y_1) = (x_0 + k_0^{y_0}, c(y_0 + y_1)).$$

It follows that f is a group homomorphism. As $c \in (\mathbf{Z}/p)^\times \cong \mathrm{Aut}(\mathbf{Z}/p)$, it is an isomorphism, with inverse $g(a, b) = (a, db)$ where $cd \equiv 1 \mod p$. This completes the proof. □

Example 23.2. There are no non-abelian groups of order 33.

Example 23.3. There is a unique (up to isomorphism) non-abelian group of order 57.

23.2 A group of order $(q-1)q$

Example 23.4. A kind of maximal semi-direct product of something something by a group N is given by

$$1 \to N \to N \rtimes_{\mathrm{id}} \mathrm{Aut}(N) \to \mathrm{Aut}(N) \to 1,$$

where we use the identity homomorphism $\mathrm{Aut}(N) \xrightarrow{\mathrm{id}} \mathrm{Aut}(N)$ for the "action" homomorphism. In the case when $N = \mathbf{Z}/q$ for a prime q, we know that $\mathrm{Aut}(N) = \mathrm{Aut}(\mathbf{Z}/q) \cong (\mathbf{Z}/q)^\times \cong \mathbf{Z}/(q-1)$ is cyclic, so we get a semi-direct product

$$1 \to \mathbf{Z}/q \to \mathbf{Z}/q \rtimes \mathbf{Z}/(q-1) \to \mathbf{Z}/(q-1) \to 1.$$

By construction, if p divides q, then there is a homomorphism $\varphi\colon \mathbf{Z}/p \to \mathbf{Z}/(q-1)$ and hence a group homomorphism $\mathbf{Z}/q \rtimes_\varphi \mathbf{Z}/p \to \mathbf{Z}/q \rtimes \mathbf{Z}/(q-1)$.

Warning 23.5. These are not typically the only groups of order $(q-1)q$.

23.3 Groups of small order checklist

$\lvert G\rvert$		known groups	complete?	simple group?
2	p	$\mathbf{Z}/2$	x	x
3	p	$\mathbf{Z}/3$	x	x
4	p^2	$\mathbf{Z}/4$, $(\mathbf{Z}/2)^2$	x	o
5	p	$\mathbf{Z}/5$	x	x
6	pq	S_3, $\mathbf{Z}/6$	x	o
7	p	$\mathbf{Z}/7$	x	x
8	p^3	D_8, $\mathbf{Z}/8$, $\mathbf{Z}/4 \times \mathbf{Z}/2$, $(\mathbf{Z}/2)^3$	o	o
9	p^2	$\mathbf{Z}/9$, $(\mathbf{Z}/3)^2$	x	o
10	pq	D_{10}, $\mathbf{Z}/10$	x	o
11	p	$\mathbf{Z}/11$	x	x
12	p^2q	$\mathbf{Z}/12$, $\mathbf{Z}/6 \times \mathbf{Z}/2$, D_12	o	o

23.4 Groups of order p^3

Example 23.6. Let p be a prime number. Up to isomorphism, there are three abelian groups of order p^3. They are $\mathbf{Z}/p^3$, $\mathbf{Z}/p^2 \times \mathbf{Z}/p$, and $\mathbf{Z}/p \times \mathbf{Z}/p \times \mathbf{Z}/p$.

Lemma 23.7. *Let p be a prime number. If G is a non-abelian group of order p^3, then the center $Z(G)$ of G has order p.*

Proof. Since G is a p-group, its center is non-trivial, and thus has order p, p^2, or p^3. However, G is abelian, so $Z(G) \neq G$ and thus the center has order p or p^2. Suppose the center of G has order p^2. It is a normal subgroup of G and $G/Z(G)$ has order p and is thus isomorphic to $\mathbf{Z}/p$. Let $x \in G$ map to $1 \in \mathbf{Z}/p$. Let $y \in Z(G)$. Then, $xy = yx$ since y is in the center. There are p^3 elements of the form $x^i y$ for $i \in \{0, \ldots, p-1\}$ and $y \in Z(G)$. Thus, every element of G is of this form. As x commutes with all of these elements, it follows that x is in the center of G, so that $Z(G) = G$, a contradiction. □

Lemma 23.8. *Let p be a prime number. Suppose that G is a non-abelian group of order p^3. Then, every element of G has order 1, p, or p^2.*

Proof. The only thing to check is that there is no element of order p^3. If there were, there would be an injective group homomorphism $\mathbf{Z}/p^3 \to G$, which would be an isomorphism, in contradiction to the assumption that G is non-abelian. □

Lemma 23.9. *Let p be a prime number. If G is a non-abelian group of order p^3, then $G/Z(G) \cong \mathbf{Z}/p \times \mathbf{Z}/p$.*

Proof. If not, then $G/Z(G) \cong \mathbf{Z}/p^2$. In this case, the corresponding extension

$$1 \to Z(G) \to G \to G/Z(G) \to 1$$

must be split, meaning just that a generator of $G/Z(G) \cong \mathbf{Z}/p^2$ lifts to an order p^2 element of G. (Otherwise, it would lift to an order p^3 element and G would be abelian, a contradiction.) Thus, G is a semi-direct product $\mathbf{Z}/p \rtimes \mathbf{Z}/p^2$. But, as there are no non-trivial homomorphisms $\mathbf{Z}/p^2 \to \mathrm{Aut}(\mathbf{Z}/p) \cong (\mathbf{Z}/p)^\times$, it follows that G is the product $\mathbf{Z}/p \times \mathbf{Z}/p^2$ and is abelian, a contradiction. □

23.5 Exercises

Exercise 23.1. Suppose that $p < q$ are primes and that $p \mid (q-1)$. Prove that there is a non-abelian subgroup of $\mathbf{GL}_2(\mathbf{F}_q)$ of order pq by writing down explicit conditions on 2×2-matrices, checking that these conditions define a subgroup, and counting the resulting elements.

Exercise 23.2. Find 10 triples $p < q < r$ of prime numbers such that every group of order pqr is abelian.

24 Groups of order p^3 (11/17)

Remark 24.1. If p is a prime number and G is a non-abelian group of order p^3, then there are $p+1$ proper subgroups of $G/Z(G) \cong \mathbf{Z}/p \times \mathbf{Z}/p$, each isomorphic to $\mathbf{Z}/p$. Pulling back along $G \to G/Z(G)$, we see that there are $p+1$ subgroups of order p^2 inside G; each contains $Z(G)$. There are two cases to analyze: (a) when one of these subgroups is isomorphic to $\mathbf{Z}/p^2$ and (b) when all of these subgroups are isomorphic to $\mathbf{Z}/p \times \mathbf{Z}/p$.

Lemma 24.2. *Let G be a group of order p^3 where p is an* odd *prime number. The pth power function $f\colon G \to G$ given by $f(x) = x^p$ is a group homomorphism. Moreover, the kernel of f contains $Z(G)$ and the image of f is contained in $Z(G)$, so f induces a homomorphism $f'\colon G/Z(G) \to Z(G)$.*

Proof. We want to show that $f(xy) = f(x)f(y)$ for any $x, y \in G$. Claim: x and y commute with $[x,y]$. Indeed, $[x,y]$ maps to the identity element in $G/Z(G)$ since this group is abelian. Thus, $[x,y]$ is in $Z(G)$ and hence commutes with all elements of G. It follows from Exercise 24.1 that $f(xy) = (xy)^p = x^p y^p [y,x]^{\frac{p(p-1)}{2}} = f(x)f(y)$, as p divides $\frac{p(p-1)}{2}$ and $[y,x]$ has order dividing p. □

Definition 24.3. Let G be a finite group. The exponent of G is the smallest integer n such that $x^n = e$ for all $x \in G$. It is the least common multiple of the orders of all elements of G and it divides $|G|$.

Example 24.4. If G is a non-abelian group of order p^3 where p is a prime number, then G has exponent p or p^2.

The following results will be proved next time.

Lemma 24.5. *Let p be an* odd *prime number. Suppose that G is a non-abelian group of order p^3. If G has an element of order p^2, then G is isomorphic to a semi-direct product $\mathbf{Z}/p^2 \rtimes_\varphi \mathbf{Z}/p$.*

Proposition 24.6. *Let p be an* odd *prime number. Up to isomorphism, there is a unique non-abelian group of order p^3 with an element of order p^2. It is isomorphic to $\mathbf{Z}/p^2 \rtimes_\varphi \mathbf{Z}/p$ where $\varphi\colon \mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/p^2) \cong \mathbf{Z}/(p(p-1))$ is any non-trivial homomorphism.*

Proposition 24.7. *Let p be an* odd *prime number. Up to isomorphism, there is a unique non-abelian group of order p^3 with no elements of order p^2.*

Example 24.8 (Groups of order p^3 for odd primes p)**.** It follows from the results above that, up to isomorphism, there are 5 groups of order p^3 if p is an odd prime. The one from Proposition 24.7 is called the **Heisenberg group** He_p.

Example 24.9 (Groups of order 8)**.** Something funny happens for $p = 2$. The two non-trivial semi-direct products

$$\mathbf{Z}/4 \rtimes \mathbf{Z}/2 \quad \text{and} \quad (\mathbf{Z}/2 \times \mathbf{Z}/2) \rtimes \mathbf{Z}/2$$

are isomorphic. Indeed, one sees that the dihedral group D_8 can be described as a semi-direct product in both ways. So, it seems like there might only by 4 isomorphism classes of groups of order 8. However, there is another group, the quaternion group Q_8, which we discuss next.

Example 24.10 (The quaternions)**.** We denote by Q_8 the set $\{1, -1, i, -i, j, -j, k, -k\}$ and define a binary operation as $1 \cdot x = x$, $(-1)^2 = 1$, $(-1) \cdot x = -x$, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -jk = i$, and $ki = -ik = j$. These imply that $ijk = -1$ as well. It is straightforward to see that this defines a binary

operation with inverses and an identity element. Associativity is cumbersome to prove directly. However, we can find elements in $\mathbf{GL}_2(\mathbf{C})$ satisfying the same relations:

$$\pm 1 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm i = \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \pm j = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \pm k = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

These satisfy the same relations and since matrix multiplication is associative, so is the binary operation on Q_8.

24.1 Exercises

Exercise 24.1. Let G be a group and $x, y \in G$ elements which both commute with $[x, y] = xyx^{-1}y^{-1}$. Show that for each $n \geqslant 1$, the equality $(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$ holds.

Exercise 24.2. Show that Q_8 is not a non-trivial semi-direct product.

Exercise 24.3. Show that any non-abelian group of order 8 is isomorphic to D_8 or Q_8.

25 End of groups of order p^3 (11/20)

25.1 Groups of order p^3

Lemma 25.1. *Let p be an* odd *prime number. Suppose that G is a non-abelian group of order p^3. If G has an element of order p^2, then G is isomorphic to a semi-direct product $\mathbf{Z}/p^2 \rtimes_\varphi \mathbf{Z}/p$.*

Proof. We assume that G has an element of order p^2. How many elements of order p^2 does G have? In this case, the homomorphism of Lemma 24.2 from $G \to Z(G)$ is surjective. The elements of order p^2 are the elements $x \in G$ such that x^p is not the identity element in $Z(G)$ under the homomorphism of Lemma 24.2. There are $(p-1)$ non-identity elements in the image and each of them is hit by p^2 elements since the kernel of $G \to Z(G)$ has order p^2. Thus, there are $p^3 - p^2$ elements of order p^2. There are therefore $p^2 - 1$ elements of order p.

Choose an element x of order p^2. Then, x generates a subgroup N of G isomorphic to $\mathbf{Z}/p^2$. In fact, N is normal. Indeed, N must contain $Z(G)$ since otherwise N and $Z(G)$ would generate G and G would be abelian. Thus, N is the inverse image of some subgroup of $G/Z(G)$. But, $G/Z(G)$ is a group of order p^2 (isomorphic to $\mathbf{Z}/p \times \mathbf{Z}/p$) and is thus abelian, so every subgroup is normal, and then N is normal. Thus, G fits into an exact sequence

$$1 \to \mathbf{Z}/p^2 \to G \to \mathbf{Z}/p \to 1.$$

To complete the proof, we have only to see that the sequence is split. But, N contains only $p-1$ elements of order p. Since there are $p^2 - 1$ elements of order p, some of them are not in N and thus the sequence is split, as desired. □

Proposition 25.2. *Let p be an* odd *prime number. Up to isomorphism, there is a unique non-abelian group of order p^3 with an element of order p^2. It is isomorphic to $\mathbf{Z}/p^2 \rtimes_\varphi \mathbf{Z}/p$ where $\varphi\colon \mathbf{Z}/p \to \mathrm{Aut}(\mathbf{Z}/p^2) \cong \mathbf{Z}/(p(p-1))$ is any non-trivial homomorphism.*

Proof. Existence follows from the computation of $\mathrm{Aut}(\mathbf{Z}/p^2)$. Uniqueness follows from an argument similar to the proof of Proposition 22.1. □

Proposition 25.3. *Let p be an* odd *prime number. Up to isomorphism, there is a unique non-abelian group of order p^3 with no elements of order p^2.*

Proof. As $\mathrm{Aut}(\mathbf{Z}/p \times \mathbf{Z}/p) \cong \mathbf{GL}_2(\mathbf{F}_p)$ has order $(p-1)^2 p(p+1)$, there is a non-trivial homomorphism $\varphi\colon \mathbf{Z}/p \to \mathbf{GL}_2(\mathbf{F}_p)$ and hence there is a semi-direct product $(\mathbf{Z}/p \times \mathbf{Z}/p) \rtimes_\varphi \mathbf{Z}/p$ which is non-abelian.

Suppose that G is a non-abelian group of order p^3 with no elements of order p^2. Then, the inverse image of any subgroup of the form $\mathbf{Z}/p$ in $G \to G/Z(G) \cong \mathbf{Z}/p \times \mathbf{Z}/p$ is a normal subgroup of G isomorphic to $\mathbf{Z}/p \times \mathbf{Z}/p$ (and contains the center). Thus, G fits into an extension

$$1 \to \mathbf{Z}/p \times \mathbf{Z}/p \to G \to \mathbf{Z}/p \to 1.$$

Since every element of G has order 1 or p, the extension is split, and G is a semi-direct product, as above.

Uniqueness is left to the reader as Exercise 25.2, which shows that any two non-trivial semi-direct products are isomorphic. (This part works for $p = 2$ as well.)

The last thing to prove is that some such semi-direct product has no elements of order p^2. However, the pth power homomorphism $G \to Z(G)$ must send all of $\mathbf{Z} \times \mathbf{Z}$ to the identity and thus it factors through $G/(\mathbf{Z}/p \times bZ/p) \cong \mathbf{Z}/p$. However, since the extension is split, we see that this factorization is also trivial. More precisely, letting $f''\colon G/(\mathbf{Z}/p \times \mathbf{Z}/p) \to Z(G)$ be the factorization, we have that $f'' = f \circ g$ where $g\colon \mathbf{Z}/p \to G$ is a splitting of the exact sequence. But, the image of g consists of elements of order dividing p. □

Example 25.4 (Groups of order p^3 for odd primes p)**.** It follows from the results above that, up to isomorphism, there are 5 groups of order p^3 if p is an odd prime. The one from Proposition 25.3 is called the **Heisenberg group** He_p.

25.2 Remark on semi-direct products of the form $p^\alpha q^\beta$

Remark 25.5. Let G be a finite group of order $p^\alpha q^\beta$ where $p < q$. If G has a normal Sylow subgroup, then it is a semi-direct product. Sometimes, this is guaranteed. This is the case for example when p^γ is not congruent to 1 mod q for any $1 \leqslant \gamma \leqslant \alpha$, or when q^γ is not congruent to 1 mod p for any $1 \leqslant \gamma \leqslant \beta$.

25.3 Exercises

Exercise 25.1. Find a subgroup of $\mathbf{GL}_2(\mathbf{Z}/p^2)$ isomorphic to the group of Proposition 25.2.

Exercise 25.2. Let p be a prime and let $\varphi_i \colon \mathbf{Z}/p \to \mathbf{GL}_2(\mathbf{F}_p)$ be non-trivial homomorphisms for $i = 1, 2$. Show that the corresponding semi-direct products $(\mathbf{Z}/p \times \mathbf{Z}/p) \rtimes_{\varphi_i} \mathbf{Z}/p$ are isomorphic.

Exercise 25.3. Let p be a prime number and consider the group $\mathbf{U}_3(\mathbf{F}_p)$ of Example 19.2. This is a non-abelian group of order p^3. Describe it as a semi-direct product and, when p is odd, determine whether it has an element of order p^2 or not.

Exercise 25.4. Classify groups of order 63.

Exercise 25.5. Show that every group of order 1225 is abelian.