6 Cosets & Factor Groups

In this chapter[19] we partition a group into subsets so that the *set of subsets* inherits a natural group structure. This will likely feel extremely abstract and difficult. However, it is really nothing new; it is precisely the idea behind modular arithmetic.

Example 6.1. In $\mathbb{Z}_3 = \{0,1,2\}$ the elements are really *subsets* $[0],[1],[2]$ of the *integers* $\mathbb{Z}$:

$$[0] = \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\} = \{\ldots,-3,0,3,6,\ldots\}$$
$$[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\} = \{\ldots,-2,1,4,7,\ldots\}$$
$$[2] = \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\} = \{\ldots,-1,2,5,8,\ldots\}$$

When we write $1 +_3 2 = 0 \in \mathbb{Z}_3$, we really mean

$$\forall x \in [1], y \in [2] \text{ we have } x + y \in [0]$$

Addition on $\mathbb{Z}$ naturally induces addition modulo 3 on the set of subsets $\mathbb{Z}_3 = \{[0],[1],[2]\}$.

6.1 Cosets & Normal Subgroups

Our main goal is to generalize the example. Start by observing that the identity element $[0]$ is a *subgroup* of $\mathbb{Z}$ from which the sets $[1]$, $[2]$ may be obtained by *translation*.

Definition 6.2. Let H be a subgroup of G and $g \in G$. The *left coset* of H containing g is

$$gH := \{gh : h \in H\} \qquad (x \in gH \iff \exists h \in H \text{ such that } x = gh)$$

This is a subset of G. The *right coset* of H containing g is defined similarly:

$$Hg := \{hg : h \in H\}$$

The *identity coset* $H = eH = He$ is the left & right coset of H containing the identity e.
H is a *normal subgroup* of G, written $H \triangleleft G$, if the left and right cosets containing g are always equal

$$H \triangleleft G \iff \forall g \in G,\ gH = Hg$$

If G is written additively, then the left and right cosets of H containing g are instead written

$$g + H := \{g + h : h \in H\} \qquad H + g := \{h + g : h \in H\}$$

Example (6.1 cont). Let $G = \mathbb{Z}$ and $H = [0] = 3\mathbb{Z}$. The left and right cosets of H are precisely the elements of $\mathbb{Z}_3$:

$$3\mathbb{Z} = 0 + 3\mathbb{Z} = 3\mathbb{Z} + 0 = [0] = \{\ldots,-3,0,3,6,\ldots\}$$
$$1 + 3\mathbb{Z} = 3\mathbb{Z} + 1 = [1] = \{\ldots,-2,1,4,7,\ldots\}$$
$$2 + 3\mathbb{Z} = 3\mathbb{Z} + 2 = [2] = \{\ldots,-1,2,5,8,\ldots\}$$

Since the left and right cosets are equal, $H = 3\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.

[19] The examples are everything in this chapter: write everything out by hand until it becomes easy—there is no shortcut!

The last observation is in fact general—we leave the proof as a straightforward exercise.

Lemma 6.3. *Every subgroup of an abelian group G is normal.*

For non-abelian groups, most subgroups are typically *not* normal: see Example 6.4.2 below.

Examples 6.4. 1. Consider the subgroup $H = \langle 4 \rangle = \{0, 4, 8\} \leq \mathbb{Z}_{12}$. This is cyclic with order 3. The distinct cosets of $\langle 4 \rangle$ are as follows (left = right since $\mathbb{Z}_{12}$ is abelian!):

$$\begin{aligned} \langle 4 \rangle &= \{0,4,8\} && (= 4 + \langle 4 \rangle = 8 + \langle 4 \rangle) \\ 1 + \langle 4 \rangle &= \{1,5,9\} && (= 5 + \langle 4 \rangle = 9 + \langle 4 \rangle) \\ 2 + \langle 4 \rangle &= \{2,6,10\} && (= 6 + \langle 4 \rangle = 10 + \langle 4 \rangle) \\ 3 + \langle 4 \rangle &= \{3,7,11\} && (= 7 + \langle 4 \rangle = 11 + \langle 4 \rangle) \end{aligned}$$

Observe that the cosets *partition* $\mathbb{Z}_{12}$ into equal-sized subsets.

2. By revisiting the multiplication table for D_3 (Example 1.2) or using cycle notation, we verify that the left and right cosets of the subgroup $H = \{e, \mu_1\}$ are as follows:

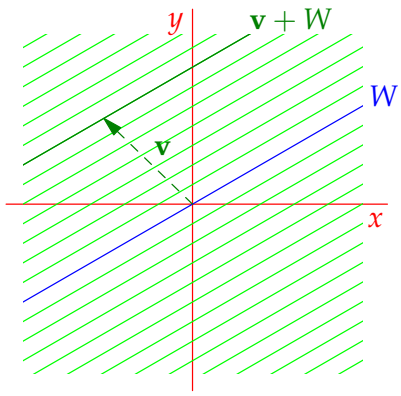
Left cosets	Right cosets
$H = \mu_1 H = \{e, \mu_1\}$	$H = H\mu_1 = \{e, \mu_1\}$
$\rho_1 H = \mu_3 H = \{\rho_1, \mu_3\}$	$H\rho_1 = H\mu_2 = \{\rho_1, \mu_2\}$
$\rho_2 H = \mu_2 H = \{\rho_2, \mu_2\}$	$H\rho_2 = H\mu_3 = \{\rho_1, \mu_3\}$

This time the left and right cosets of H are not all the same: H is *not* a normal subgroup of D_3. The partitioning observation still holds: the left cosets partition D_3 into three equal-sized subsets; the right cosets also partition into equal-sized subsets, just different ones.

3. Consider a 1-dimensional subspace $W \leq \mathbb{R}^2$; this is a line through the origin. The coset

$$\mathbf{v} + W = \{\mathbf{v} + \mathbf{w} : \mathbf{w} \in W\}$$

is a line parallel to W. The cosets thus comprise all lines parallel to W. Note again that these *partition* $\mathbb{R}^2$: every point in $\mathbb{R}^2$ lies in precisely one coset.



More generally, if W is a subspace of a vector space V, then the cosets $\mathbf{v} + W$ are the sets parallel to W. Only the zero coset $W = \mathbf{0} + W$ is a sub*space*.

4. Recall Theorem 5.24. If we generalize the argument, we see that, for any $\alpha \in A_n$ and $\sigma \in S_n$,

$$\alpha\sigma \text{ even} \iff \sigma \text{ even} \iff \sigma\alpha \text{ even}$$

Otherwise said, for any $\sigma \in S_n$, the cosets of A_n containing σ are

$$\sigma A_n = A_n \sigma = \begin{cases} A_n & \text{if } \sigma \text{ even} \\ B_n & \text{if } \sigma \text{ odd} \end{cases}$$

where B_n is the set of odd permutations in S_n. In particular, A_n is a normal subgroup of S_n.

As observed in the examples, the cosets of any subgroup $H \leq G$ seem to partition G.

Theorem 6.5. *Let H be a subgroup of G. Then the left cosets of H partition G. Moreover,*

$$y \in xH \iff x^{-1}y \in H \iff xH = yH$$

The right cosets partition G similarly: indeed

$$y \in Hx \iff yx^{-1} \in H \iff Hx = Hy$$

The blue criterion is particularly useful as it is often very easy to check. Before reading the proof, convince yourself that each previous example satisfies the result. When H is non-normal (e.g. Example 2), the right cosets partition G in a *different way* to the left cosets!

Proof. We start by verifying the first connective.

$$y \in xH \iff \exists h \in H \text{ such that } y = xh \iff x^{-1}y = h \in H$$

Now define a relation $\sim$ on G via $x \sim y \iff y \in xH$. We claim this is an equivalence relation:

Reflexivity: $x \sim x$ since $x^{-1}x = e \in H$.
Symmetry: $x \sim y \implies x^{-1}y \in H \implies (x^{-1}y)^{-1} \in H$, since H is a subgroup. But then

$$y^{-1}x \in H \implies y \sim x$$

Transitivity: If $x \sim y$ and $y \sim z$ then $x^{-1}y \in H$ and $y^{-1}z \in H$. But H is closed, whence

$$x^{-1}z = (x^{-1}y)(y^{-1}z) \in H \implies x \sim z$$

The equivalence classes therefore partition G. Since $x \sim y \iff y \in xH$, the equivalence class of x is indeed the left coset xH, as required. ∎

It is precisely the fact that H is a subgroup which guarantees a partition (compare Theorem 2.19)!

Reflexivity: H contains the identity (and is thus non-empty).
Symmetry: H satisfies the inverse axiom.
Transitivity: H is closed under the group operation.

When H is not a subgroup, the coset construction is unlikely to produce a partition.

Example 6.6. The *subset* $H = \{0, 1\} \subseteq \mathbb{Z}_3$ is not a subgroup. Its left 'cosets' fail to partition $\mathbb{Z}_3$:

$$H = \{0, 1\}, \quad 1 + H = \{1, 2\}, \quad 2 + H = \{2, 1\}$$

We finish this section with a technical result which will be useful in future sections.

Corollary 6.7. *Normal subgroups are precisely those which are closed under* conjugation*:*

$$H \triangleleft G \iff \forall g \in G,\ h \in H,\ \text{we have } ghg^{-1} \in H$$

Proof. Start by using the above criteria to observe:

(a) $gH \subseteq Hg \iff \forall h \in H,\ gh \in Hg \iff \forall h \in H,\ ghg^{-1} \in H$

(b) $Hg \subseteq gH \iff \forall h \in H,\ hg \in gH \iff \forall h \in H,\ g^{-1}hg \in H$

We may now complete the proof in two parts:

($\Rightarrow$) $H \triangleleft G \implies$ part (a) for all $g \in G$.

($\Leftarrow$) If $ghg^{-1} \in H$ for all g, h, then this is also true for g^{-1}: that is $g^{-1}hg \in H$. We now have the right side of both (a) and (b). Otherwise said, $gH = Hg$ for all $g \in G$, whence H is normal in G. ∎

Exercises 6.1. Key concepts:

Left/right cosets *normal subgroup* *(left) cosets partition group*

1. Find the cosets of the following subgroups: since the groups are abelian, left and right cosets are identical.
   (a) $4\mathbb{Z} \leq 2\mathbb{Z}$ (b) $\langle 4 \rangle \leq \mathbb{Z}_{10}$
   (c) $\langle 6 \rangle \leq \mathbb{Z}_{30}$ (d) $\langle 20 \rangle \leq \mathbb{Z}_{30}$
2. Find the cosets of $H = \{(0,0), (2,0), (0,2), (2,2)\} \leq \mathbb{Z}_4 \times \mathbb{Z}_4$
3. Find the left and right cosets of $\{\rho_0, \rho_1, \rho_2\} \leq D_3$. Is the subgroup normal?
4. (a) Find the left and right cosets of $H := \{e, (1\,2\,3), (1\,3\,2)\} \leq A_4$. Is the subgroup normal?
   (b) Repeat the question for the subgroup $V := \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$
5. (a) Find the left and right cosets of the subgroup $\{\rho_0, \delta_1\} \leq D_4$. Is the subgroup normal?
   (b) Repeat part (a) for the subgroup $\{\rho_0, \rho_2\}$.
   (*Hint: use cycle notation (Exercises 5.1.5.7), or look up the Cayley table*)
6. Prove Lemma 6.3: every subgroup of an abelian group is normal.
7. Suppose H is a *subset* of G, but not necessarily a subgroup.
   (a) If H has only one element, show that the sets $gH = \{gh : h \in H\}$ do partition G.
   (b) Show that the 'cosets' of $H = \{1, 3\}$ also partition $\mathbb{Z}_4$, even though H is not a subgroup.
8. Let $H = \{\sigma \in S_4 : \sigma(4) = 4\}$.
   (a) Show that H is a subgroup of S_4: we call this the *stabilizer* of 4.
   (b) Using Corollary 6.7, or otherwise, determine whether H is a normal subgroup of S_4.
9. Let H, K be subgroups of G. Define $\sim$ on G by
   $$a \sim b \iff a = hbk \quad \text{for some} \quad h \in H,\ k \in K.$$
   (a) Prove that $\sim$ is an equivalence relation on G.
   (b) Describe the elements of the equivalence class of $a \in G$; this is a *double coset*.
   (c) Consider $H = \{e, (1\,2)\}$ and $K = \{e, (1\,3)\}$ as subgroups of S_3. Compute the double cosets.

6.2 Lagrange's Theorem & Indices

We've been inching up to a powerful result; with luck you've hypothesized this already!

Theorem 6.8 (Lagrange). *In a finite group, the order of a subgroup divides the order of the group.*[20] *Otherwise said*

$$H \leq G \implies |H| \,\Big|\, |G|$$

Proof. Suppose $H \leq G$ and fix $g \in G$. The function

$$\phi_g : H \to gH : h \mapsto gh$$

is a bijection (with inverse $\phi_g^{-1} : gh \mapsto h$). Every left coset of H therefore has the same cardinality as H. Since the left cosets partition G (Theorem 6.5), we conclude that

$$|G| = (\text{number of left cosets of } H) \cdot |H| \implies |H| \,\Big|\, |G|$$

■

We could similarly have proved this using the right coset partition. Here is an example of its power.

Corollary 6.9. *Up to isomorphism, there is a unique group of prime order p, namely $\mathbb{Z}_p$.*

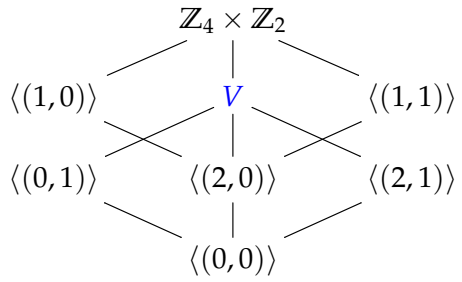
Proof. Suppose G is a group with prime order p. Since $p \geq 2$, we may choose some element $g \neq e$. The order of the cyclic subgroup $\langle g \rangle \leq G$ satisfies:

- $|\langle g \rangle| \geq 2$ since $g \neq e$.
- $|\langle g \rangle| = 1$ or p by Lagrange, since p is prime.

We conclude that $|\langle g \rangle| = p \implies G = \langle g \rangle$ is cyclic and thus isomorphic to $\mathbb{Z}_p$ (Theorem 3.13). ■

Example 6.10. $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ has order 8 so its non-trivial proper subgroups can only have orders 2 or 4 and are thus isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_4$ or V. These can be identified by thinking about all possible generators; V requires three elements of order 2 which we indeed have! Here is the subgroup diagram: all proper subgroups are cyclic except $V = \{(0,0),(2,0),(0,1),(2,1)\}$.

generator	order	subgroup
$(1,0)$ or $(3,0)$	4	$\{(0,0),(1,0),(2,0),(3,0)\}$
$(1,1)$ or $(3,1)$	4	$\{(0,0),(1,1),(2,0),(3,1)\}$
$(2,0)$	2	$\{(0,0),(2,0)\}$
$(0,1)$	2	$\{(0,0),(0,1)\}$
$(2,1)$	2	$\{(0,0),(2,1)\}$
$(0,0)$	1	$\{(0,0)\}$



[20] This is sometimes misremembered as 'the order of an element divides the order of the group.' This is the special case when H is a *cyclic subgroup* of G. The even more special case when G is cyclic is Corollary 3.20: $\langle s \rangle \leq \mathbb{Z}_n$ has order $\frac{n}{\gcd(s,n)}$ (certainly divides n). The converse to Lagrange is *false*: e.g. A_4 has order 12, but no subgroup of order 6 (Exercise 5.3.7).

The proof of Lagrange tells us that the *number* of left and right cosets of $H \leq G$ is *identical:* both equal the quotient $\frac{|G|}{|H|}$. This motivates a new concept.

Definition 6.11. The *index* $(G : H)$ of a subgroup $H \leq G$ is the cardinality of the set of (left) cosets:

$$(G : H) = |\{gH : g \in G\}|$$

The index is also the cardinality of the set of *right* cosets (Exercise 8). If G is finite, then $(G : H) = \frac{|G|}{|H|}$.

Examples 6.12. 1. If $G = \mathbb{Z}_{20}$ and $H = \langle 2 \rangle$, then there are $(G : H) = \frac{20}{10} = \frac{|G|}{|H|} = 2$ cosets:

$$H = \langle 2 \rangle = \{0, 2, 4, \ldots, 18\} \quad \text{and} \quad 1 + H = \{1, 3, 5, \ldots, 19\}$$

2. Recall (Example 2.21 & Exercise 2.2.10 the orthogonal and special orthogonal groups

$$\mathrm{O}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A^T A = I\}, \qquad \mathrm{SO}_n(\mathbb{R}) = \{A \in \mathrm{O}_n(\mathbb{R}) : \det A = 1\}$$

Since every orthogonal matrix has determinant ± 1, it feels as if $\mathrm{SO}_n(\mathbb{R})$ should be 'half' of $\mathrm{O}_2(\mathbb{R})$. Since both groups are infinite (indeed uncountable), we need the index to confirm this intuition. Recall Theorem 6.5: given $A, B \in \mathrm{O}_n(\mathbb{R})$,

$$A\,\mathrm{SO}_n = B\,\mathrm{SO}_n(\mathbb{R}) \iff B^{-1}A \in \mathrm{SO}_n(\mathbb{R}) \iff \det(B^{-1}A) = 1 \iff \det B = \det A$$

We conclude that there are precisely two cosets $\big(\mathrm{O}_n(\mathbb{R}) : \mathrm{SO}_n(\mathbb{R})\big) = 2$.

Theorem 6.13. *If $K \leq H \leq G$ is a sequence of subgroups, then*

$$(G : K) = (G : H)(H : K)$$

If G is a finite group then the result is essentially trivial:

$$(G : K) = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = (G : H)(H : K)$$

Our proof also covers infinite groups and infinite indices. You are *strongly* encouraged to work through the following examples, which are written in the language of the proof.

Proof. Choose an element g_i from each left coset of H in G and an element h_j from each left coset of K in H. Plainly

$$(G : H) = |\{g_i\}| \qquad \text{and} \qquad (H : K) = \big|\{h_j\}\big|$$

We claim that the left cosets of K in G are precisely the sets $(g_i h_j)K$. Certainly each such is a *coset*; we show that these cosets *partition* G, whence the collection $\{(g_i h_j)K\}$ must comprise *all* left cosets.

- Every $g \in G$ lies in some left coset of H, so $\exists g_i \in G$ such that $g \in g_i H$.
  ${g_i}^{-1} g \in H$ lies in some left coset of K in H, so $\exists h_j \in H$ such that ${g_i}^{-1} g \in h_j K$.
  But then $g \in (g_i h_j)K$ so that every $g \in G$ lies in at least one set $(g_i h_j)K$.

- Suppose $y \in g_i h_j K \cap g_\alpha h_\beta K$. Since $K \leq H$ and the left cosets of H partition G, we have

$$y \in g_i H \cap g_\alpha H \implies g_\alpha = g_i$$

But then ${g_i}^{-1} y \in h_j K \cap h_\beta K \implies h_\beta = h_j$ similarly, since the left cosets of K in H partition H. It follows that the sets $(g_i h_j)K$ are disjoint.

Since the left cosets of K in G are given by $\{(g_i h_j)K\}$, it is immediate that

$$(G : K) = \big|\{g_i h_j\}\big| = |\{g_i\}|\,\big|\{h_j\}\big| = (G : H)(H : K)$$

■

Examples 6.14. 1. Recall Example 6.12.1: let $G = \mathbb{Z}_{20}$, $H = \langle 2 \rangle$ and $K = \langle 10 \rangle$. Plainly

$$K = \{0, 10\} \leq H = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\} \leq G = \{0, 1, 2, 3, \ldots, 19\}$$

so we have the required subgroup relationship. Here are the indices and cosets in each case:

- $(G : H) = 2$ with cosets H and $1 + H$. In the language of the proof, $g_0 = 0$ and $g_1 = 1$.
- $(H : K) = \frac{10}{2} = 5$ cosets, with representatives $h_0 = 0$, $h_1 = 2$, $h_2 = 4$, $h_3 = 6$, $h_4 = 8$:

$$K = \{0, 10\},\ \ 2 + K = \{2, 12\},\ \ 4 + K = \{4, 14\},\ \ 6 + K = \{6, 16\},\ \ 8 + K = \{8, 18\}$$

- $(G : K) = \frac{20}{2} = 10 = (G : H)(H : K)$: the cosets are

$$K = \{0, 10\}, \quad 1 + K = \{1, 11\}, \quad 2 + K = \{2, 12\}, \quad \ldots, \quad 9 + K = \{9, 19\}$$

In the language of the proof these cosets all have the form $(g_i + h_j) + K$.

2. Consider the sequence of subgroups $K \leq H \leq S_4$ where

$$K = \{e, (1\,2\,3), (1\,3\,2)\} \cong \mathbb{Z}_3 \quad \text{and} \quad H = \{\sigma \in S_4 : \sigma(4) = 4\} \cong S_3$$

The $(H : K) = \frac{6}{3} = 2$ left cosets of K in H are

$$K = eK = \{e, (1\,2\,3), (1\,3\,2)\} \quad \text{and} \quad (1\,2)K = \{(1\,2), (2\,3), (1\,3)\}$$

with representatives $h_0 = e$ and $h_1 = (1\,2)$. The $(S_4 : H) = \frac{24}{6} = 4$ left cosets of H in S_4 are

$$\begin{aligned}
H &= eH = \{e, (1\,2\,3), (1\,3\,2), (1\,2), (2\,3), (1\,3)\} \\
(1\,4)H &= \{(1\,4), (1\,2\,3\,4), (1\,3\,2\,4), (1\,2\,4), (1\,4)(2\,3), (1\,3\,4)\} \\
(2\,4)H &= \{(2\,4), (1\,4\,2\,3), (1\,3\,4\,2), (1\,4\,2), (2\,3\,4), (1\,3)(2\,4)\} \\
(3\,4)H &= \{(3\,4), (1\,2\,4\,3), (1\,4\,3\,2), (1\,2)(3\,4), (2\,4\,3), (1\,4\,3)\}
\end{aligned}$$

with representatives $g_0 = e$, $g_1 = (1\,4)$, $g_2 = (2\,4)$, $g_3 = (3\,4)$. The *eight* left cosets of K in S_4 are therefore

$$\begin{aligned}
eeK &= K = \{e, (1\,2\,3), (1\,3\,2)\} & e(1\,2)K &= (1\,2)K = \{(1\,2), (2\,3), (1\,3)\} \\
(1\,4)eK &= (1\,4)K = \{(1\,4), (1\,2\,3\,4), (1\,3\,2\,4)\} & (1\,4)(1\,2)K &= \{(1\,2\,4), (1\,4)(2\,3), (1\,3\,4)\} \\
(2\,4)eK &= (2\,4)K = \{(2\,4), (1\,4\,2\,3), (1\,3\,4\,2)\} & (2\,4)(1\,2)K &= \{(1\,4\,2), (2\,3\,4), (1\,3)(2\,4)\} \\
(3\,4)eK &= (3\,4)K = \{(3\,4), (1\,2\,4\,3), (1\,4\,3\,2)\} & (3\,4)(1\,2)K &= \{(1\,2)(3\,4), (2\,4\,3), (1\,4\,3)\}
\end{aligned}$$

Exercises 6.2. Key concepts:

Lagrange's Theorem *index of a subgroup*

1. Find the indices of the following subgroups:

   (a) $\langle 9 \rangle \leq \mathbb{Z}_{12}$ (b) $6\mathbb{Z} \leq 2\mathbb{Z}$ (c) $(\mathbb{Q}^+, \cdot) \leq (\mathbb{Q}^\times, \cdot)$

2. Let $G = \mathbb{Z}_8$, $H = \langle 2 \rangle$ and $K = \langle 4 \rangle$. Write out all the cosets for the three subgroup relations $K \leq H$, $H \leq G$ and $K \leq G$, and verify the index multiplication formula.

3. Let G have order pq where p, q are both prime. Show that every proper subgroup of G is cyclic.

4. Use Lagrange's Theorem to prove that all proper subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ are cyclic. Hence construct its subgroup diagram.

5. Find the subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_2$ and draw its subgroup diagram.

   (*Hint: At least one subgroup here is* non-cyclic*!*)

6. Suppose $(G : H) = 2$. Prove that H is a normal subgroup of G.

7. Prove that $\{e\}$ and G are both normal subgroups of G: what are the cosets and the indices in each case?

   (*Remember that G could be infinite!*)

8. For each left coset gH of H in G, choose a representative g_j. Prove that the function

   $$\Phi : g_j H \mapsto H g_j^{-1}$$

   defines an injective function from the set of left cosets to the set of right cosets.

   With the reverse argument this shows that the sets of left and right cosets have the same cardinality

9. Let $G = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

   (a) Prove that G is a group under addition.

   (b) Prove that $H = \{3m + 2n\sqrt{2} : m, n \in \mathbb{Z}\}$ is a subgroup of index six in G.
   (*Hint: what does it mean for $a + b\sqrt{2}$ and $c + d\sqrt{2}$ to lie in the same coset of H?*)

10. The sets $\mathbb{Q}$ and $\mathbb{Z}$ are both groups under addition. Show that there is precisely one coset of $\mathbb{Z}$ in $\mathbb{Q}$ for each rational number in the interval $[0, 1)$. Hence conclude that $(\mathbb{Q} : \mathbb{Z}) = \aleph_0$ is countably infinite.

6.3 Factor Groups

Given a subgroup $H \leq G$, we ask whether the *set of left cosets* $\{gH : g \in G\}$ can be viewed as a group *in a natural way.* By this, we mean that the group structure on should be *inherited* from that of G. To see how this works (or doesn't!), recall Examples 6.1.

Examples (6.4.1 cont). 1. The set of (left) cosets for $H = \langle 4 \rangle = \{0, 4, 8\} \leq \mathbb{Z}_{12}$ is

$$\{H,\ 1+H,\ 2+H,\ 3+H\} = \Big\{\{0,4,8\}, \{1,5,9\}, \{2,6,10\}, \{3,7,11\}\Big\}$$

It feels like we have the cyclic group $\mathbb{Z}_4$ in disguise! To see this we need a binary operation: the natural approach is to use the addition we already have in $\mathbb{Z}_{12}$ and define addition of cosets via

$$(a+H) \oplus (b+H) := (a+b) + H$$

The process for computing $(a+H) \oplus (b+H)$ contains a potential snag:

(a) *Choose representatives*: Make a choice of elements a and b in the respective cosets.
(b) *Add within the original group*: Compute $a + b \in \mathbb{Z}_{12}$.
(c) *Take the coset*: Return the left coset $(a+b) + H$.

If $\oplus$ is to make sense, the outcome must be *independent of the choices* made in step (a). In this case there is no problem, as you can tediously check for yourself: for example, to verify

$$(2+H) \oplus (3+H) = 1 + H$$

there are *nine* possibilities, of which one is

$$6 +_{12} 11 = 17 = 5 \in 1 + H$$

Rather than verify these independently, we proceed in general. If $x \in a + H$ and $y \in b + H$, then $x - a$ and $y - b \in H$, whence

$$(x-a) + (y-b) = (x+y) - (a+b) \in H \implies (x+y) + H = (a+b) + H$$

The operation is well-defined and we'll shortly see that the set of left cosets forms a group under $\oplus$. Indeed $\phi(x) = x + H$ defines an isomorphism of $\mathbb{Z}_4$ with this *factor group.*

2. Unfortunately, this sort of behavior isn't universal. Let us repeat the process with the subgroup $H = \{e, \mu_1\} \leq D_3$, whose left cosets are

$$H = \mu_1 H = \{e, \mu_1\}, \quad \rho_1 H = \mu_3 H = \{\rho_1, \mu_3\}, \quad \rho_2 H = \mu_2 H = \{\rho_2, \mu_2\}$$

This time, if we attempt to define the 'natural' operation on the set $\{\sigma H\}$ of left cosets via

$$aH \otimes bH := (ab)H$$

then the problem is real. There are *four choices* for how to compute $\rho_1 H \otimes \rho_1 H$, of which two suffice for a contradiction:

$$\rho_1\rho_1 H = \rho_2 H \quad \text{and} \quad \mu_3\mu_3 H = H$$

The freedom of choice (part (a)) in the definition of $\otimes$ leads to different outcomes, whence $\otimes$ is *not well-defined*, and the set of left cosets does not form a group in a natural way.

Well-definition of the Factor Group Structure

As the examples show, some subgroups $H \leq G$ behave better than others when trying to view the set of left cosets as a group. But which subgroups? To answer this, we repeat some of our discussion in the abstract.

Let H be a subgroup of G and define the natural operation on the set of left cosets:

$$aH \cdot bH := (ab)H$$

This is well-defined if and only if

$$\forall a, b \in G,\ \forall x \in aH,\ y \in bH, \quad \text{we have} \quad (ab)H = (xy)H$$

Let us trace through what this means for the subgroup H, using the fact that

$$x \in aH \iff \exists h \in H \text{ such that } x = ah$$

The natural operation is well-defined if and only if

$$\begin{aligned}
&\forall a, b \in G,\ h, h_1 \in H,\ (ab)H = (ahbh_1)H = (ahb)H \\
\iff &\forall a, b \in G,\ h \in H,\ (ab)^{-1}(ahb) \in H && \text{(Theorem 6.5)} \\
\iff &\forall b \in G,\ h \in H,\ b^{-1}hb \in H \\
\iff &H \triangleleft G && \text{(Corollary 6.7)}
\end{aligned}$$

We have proved the critical part of an amazing result!

Theorem 6.15. *Suppose $H \leq G$. The set of left cosets forms a group under the natural operation*

$$aH \cdot bH := (ab)H$$

if and only if H is a normal subgroup of G.

Definition 6.16. If $H \triangleleft G$, then the set of (left) cosets is a *factor group*, written ${}^{G}/_{H}$ ('G mod H').

Since the group structure on ${}^{G}/_{H}$ arises naturally from that on G, we typically use the *same notation* for the operation. The notation meshes with the index: if G is finite, then $\left|{}^{G}/_{H}\right| = (G : H) = \frac{|G|}{|H|}$.

Proof. The above discussion shows that the natural operation on ${}^{G}/_{H}$ is well-defined if and only if H is normal in G. It remains only to check that ${}^{G}/_{H}$ is a group in such cases.

Closure: $aH \cdot bH = (ab)H$ is a coset, whence $\left({}^{G}/_{H}, \cdot\right)$ is closed.

Associativity: $aH \cdot (bH \cdot cH) = aH \cdot (bc)H = a(bc)H$. Similarly $(aH \cdot bH) \cdot cH = (ab)cH$. By the associativity of G these cosets are identical.

Identity: $eH \cdot aH = (ea)H = aH = (ae)H = aH \cdot eH$ therefore the *identity coset* $eH = H$ is the identity.

Inverse: $a^{-1}H \cdot aH = (a^{-1}a)H = eH = H$, etc., therefore $(aH)^{-1} = a^{-1}H$. ∎

Factor Groups of $\mathbb{Z}$: modular arithmetic done right!

For each positive integer n, the integer multiples $n\mathbb{Z} = \langle n \rangle$ form a normal subgroup of $\mathbb{Z}$. The coset of $n\mathbb{Z}$ containing $x \in \mathbb{Z}$ is therefore

$$x + n\mathbb{Z} = \{x + kn : k \in \mathbb{Z}\} = \{y \in \mathbb{Z} : y \equiv x \pmod{n}\}$$

This is precisely what we are used to calling 'x' in $\mathbb{Z}_n$! Indeed this is the formal definition, superseding Definition 3.4 and trivially proving Theorem 3.5.

Definition 6.17. Let $n \in \mathbb{N}$. The group $\mathbb{Z}_n$ is the *factor group* $\mathbb{Z}/n\mathbb{Z}$

Since remainders are so familiar, we typically drop $n\mathbb{Z}$ when calculating, thus

$$4 + 5 = 2 \in \mathbb{Z}_7 \quad \text{means} \quad (4 + 7\mathbb{Z}) + (5 + 7\mathbb{Z}) = 2 + 7\mathbb{Z} \in \mathbb{Z}/7\mathbb{Z}$$

Factor Groups of Finite Cyclic Groups

Our first example in this section showed that $\mathbb{Z}_{12}/\langle 4 \rangle \cong \mathbb{Z}_4$. Here is another.

Example 6.18. $\langle 5 \rangle = \{0, 5, 10, 15\} \leq \mathbb{Z}_{20}$ has factor group

$$\mathbb{Z}_{20}/\langle 5 \rangle = \{0 + \langle 5 \rangle,\ 1 + \langle 5 \rangle,\ 2 + \langle 5 \rangle,\ 3 + \langle 5 \rangle,\ 4 + \langle 5 \rangle\}$$

This is isomorphic to $\mathbb{Z}_5$ via the isomorphism

$$\psi : \mathbb{Z}_5 \to \mathbb{Z}_{20}/\langle 5 \rangle : x \mapsto x + \langle 5 \rangle$$

Theorem 6.19. *If $d \mid n$, then $\mathbb{Z}_n/\langle d \rangle \cong \mathbb{Z}_d$.*

If s is not a divisor of n, recall that $\langle s \rangle = \langle d \rangle$ where $d = \gcd(s, n)$, whence $\mathbb{Z}_n/\langle s \rangle \cong \mathbb{Z}_{\gcd(s,n)}$.

Proof. Define $\psi : \mathbb{Z}_d \to \mathbb{Z}_n/\langle d \rangle : x \mapsto x + \langle d \rangle$: our goal is to see that this is an isomorphism.

Well-definition/injectivity:[21] The former is required since the domain is a set of *equivalence classes*!

$$x = y \in \mathbb{Z}_d \iff x - y \in \langle d \rangle \iff x + \langle d \rangle = y + \langle d \rangle \iff \psi(x) = \psi(y)$$

Surjectivity: Any coset $x + \langle d \rangle = \psi(x) \in \mathrm{Im}(\psi)$.

Homomorphism: For any $x, y \in \mathbb{Z}_d$,

$$\psi(x + y) = (x + y) + \langle d \rangle = \big(x + \langle d \rangle\big) + \big(y + \langle d \rangle\big) = \psi(x) + \psi(y)$$

■

[21] That these arguments are converses is typical: for a given function $\mu : A \to B$,

- Well-definition means: $a = b \implies \mu(a) = \mu(b)$
- Injectivity means: $\mu(a) = \mu(b) \implies a = b$

Finite Abelian Examples

If G is a finite abelian group, then any subgroup H is normal and G/H is also a finite abelian group (exercise). By the Fundamental Theorem (4.9) there exist positive integers $m_1, \ldots, m_k$ for which

$$G/H \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \quad \text{and} \quad m_1 \cdots m_k = (G:H) = \frac{|G|}{|H|}$$

Our goal in these examples is to *identify* G/H as a direct product by finding suitable integers m_k.

Examples 6.20. For $G = \mathbb{Z}_4 \times \mathbb{Z}_8$ and three subgroups H, we identify the factor group G/H.

1. If $H = \langle (0,1) \rangle = \{(0,0), (0,1), (0,2), \ldots, (0,7)\}$, then the index of H in G is $(G:H) = \frac{4 \cdot 8}{8} = 4$. The factor group is abelian with order four and thus isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

   Here are two strategies for deciding which.

   (a) Identify the cosets:

   $$(x,y) + H = (v,w) + H \iff (x,y) - (v,w) = (x-v, y-w) \in H \iff x = v$$

   Each coset contains a unique element $(x,0)$ where $x \in \mathbb{Z}_4$, whence,

   $$G/H = \Big\{ H,\ (1,0) + H,\ (2,0) + H,\ (3,0) + H \Big\}$$

   It can be checked that this is isomorphic to $\mathbb{Z}_4$ via $\psi : \mathbb{Z}_4 \to G/H : x \mapsto (x,0) + H$.

   (b) Observe that there exists an element in G/H with order 4. If $k \in \mathbb{N}$, then

   $$k\big((1,0) + H\big) = (k,0) + H = H \iff (k,0) \in H \iff 4 \mid k$$

   This identifies $G/H \cong \mathbb{Z}_4$ by elimination: every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order *at most* 2.

2. $H = \langle (0,2) \rangle = \{(0,0), (0,2), (0,4), (0,6)\}$ has order 4 with index $(G:H) = \frac{4 \cdot 8}{4} = 8$. The factor group is abelian with order 8 and thus isomorphic to one of $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

   We again follow our strategies:

   (a) Identify the cosets:

   $$(x,y) + H = (v,w) + H \iff (x-v, y-w) \in H \iff \begin{cases} x = v, \text{and} \\ y - w = 2k \text{ is even} \end{cases}$$

   from which the distinct cosets may be written

   $$G/H = \Big\{ H,\ (1,0) + H,\ (2,0) + H,\ \ldots\ (3,1) + H \Big\} = \Big\{ (x,y) + H : x \in \mathbb{Z}_4, y \in \mathbb{Z}_2 \Big\}$$

   We have an isomorphism $\psi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to G/H : (x,y) \mapsto (x,y) + H$.

   (b) Alternatively, consider orders of elements:

   - G/H contains an element $(1,0) + H$ of order 4.
   - All elements of G/H have order dividing 4:

   $$4\big((x,y) + H\big) = (4x, 4y) + H = (0, 4y) + H = 2y\big((0,2) + H\big) = H$$

   By elimination, $G/H \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ ($\mathbb{Z}_8$ has an element of order 8, while elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ have maximum order 2).

3. Consider $H = \langle(2,4)\rangle = \{(0,0),(2,4)\}$. The previous examples may have lulled you into a false sense of security: ${}^{G}\!/_{H}$ is *not*

$$\mathbb{Z}_4/\langle 2\rangle \times \mathbb{Z}_8/\langle 4\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

The fact that there are $(G:H) = \frac{4\cdot 8}{2} = 16$ cosets immediately rules out this naïve possibility!

The Fundamental Theorem gives *five* non-isomorphic options for the factor group:

$$\mathbb{Z}_{16},\ \mathbb{Z}_2 \times \mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

We again follow our strategies:

(a) Identify the cosets. This is a little trickier than before.

- If $x = 2n$ is even, then

$$(x,y) + H = (2n,y) + H = n(2,4) + (0,y-4n) + H = (0,y-4n) + H$$

- If $x = 2n+1$ is odd, then

$$(x,y) + H = (2n+1,y) + H = n(2,4) + (1,y-4n) + H = (1,y-4n) + H$$

There is precisely one representative of each coset whose first entry is either 0 or 1, whence the sixteen elements

$$(0,0),\ (0,1),\ \ldots,\ (0,7),\ (1,0),\ \ldots,\ (1,7)$$

lie in distinct cosets of H. It seems reasonable to claim that the factor group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_8$. Indeed

$$\psi : \mathbb{Z}_2 \times \mathbb{Z}_8 \to {}^{G}\!/_{H} \to : (x,y) \mapsto (x,y-2x) + H$$

is an explicit isomorphism. We leave it as an exercise to verify this. It requires some creativity to invent such a function from nothing, particularly at the moment!

(b) The coset $(0,1) + H$ has order 8 in ${}^{G}\!/_{H}$, since

$$k\big((0,1)+H\big) = (0,k) + H = H \iff 8 \mid k$$

which reduces our options to $\mathbb{Z}_{16}$ and $\mathbb{Z}_2 \times \mathbb{Z}_8$. Moreover, any coset has order dividing 8:

$$8\Big((x,y)+H\Big) = (8x,8y) + H = (0,0) + H$$

This rules out $\mathbb{Z}_{16}$, leaving $\mathbb{Z}_2 \times \mathbb{Z}_8$ as the only possibility.

Strategy (b) might seem easier right now, but it has some drawbacks; for instance, it cannot distinguish between groups such as $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$: both groups contain an element of order 4, and the maximum order of an element is also 4.

Other Examples

There are many other examples of factor groups, with varied strategies required for their identification. Here are just a few, and we'll see more in later chapters.

Examples 6.21. 1. $\langle 2\pi \rangle = 2\pi\mathbb{Z} = \{2\pi n : n \in \mathbb{Z}\}$ is a subgroup of the abelian group $(\mathbb{R}, +)$.

In any given coset $x + 2\pi\mathbb{Z}$, there is a unique x such that $0 \leq x < 2\pi$ (this is like taking the remainder of x modulo 2π!). It follows that

$$\mathbb{R}/_{2\pi\mathbb{Z}} = \{x + 2\pi\mathbb{Z} : x \in [0, 2\pi)\}$$

Moreover, the function

$$\mu : \mathbb{R}/_{2\pi\mathbb{Z}} \to S^1 : x + 2\pi\mathbb{Z} \mapsto e^{ix}$$

is an isomorphism of groups. The factor group construction therefore corresponds to wrapping the real line infinitely many times around a circle of circumference 2π.

2. Exercise 6.1.4, tells us that the Klein four-group

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

is a normal subgroup of the alternating group A_4. The factor group has order $(A_4 : V) = \frac{12}{4} = 3$ and so $A_4/_V \cong \mathbb{Z}_3$: can you find an explicit isomorphism?

It's a lot harder to prove, but we'll see later that $S_4/_V \cong S_3$.

3. Consider $H = \langle (2,1) \rangle \leq \mathbb{Z} \times \mathbb{Z}_4 = G$. Since G and H are infinite, we cannot simply apply the index formula to count cosets. Instead we use the 2 in the subgroup H to find a simple representative of each coset.

$$(x, y) + H = \begin{cases} (2n, y) + H = (0, y - n) + H & \text{if } x = 2n \text{ is even} \\ (2n + 1, y) + H = (1, y - n) + H & \text{if } x = 2n + 1 \text{ is odd} \end{cases}$$

There is a *unique representative* in each coset either of the form $(0, z)$ or $(1, z)$, where $z \in \mathbb{Z}_4$. We conclude that there are $2 \cdot 4 = 8$ cosets. Since $G/_H$ is abelian (Exercise 6), it must be isomorphic to one of $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. To identify which, compute

$$4\big((x, y) + H\big) = (4x, 4y) + H = (0, -2x) + H = H \iff 2 \mid x$$

We conclude that $(1, 0) + H$ has order 8, whence $G/_H \cong \mathbb{Z}_8$.

4. Let $H = \langle (1, 2) \rangle \leq \mathbb{Z} \times \mathbb{Z} = G$. We play a similar trick as above

$$(x, y) + H = (0, y - 2x) + H$$

Since the choice of y is free, we see that there is a unique representative in each coset of the form $(0, z)$. We conclude that $G/_H \cong \mathbb{Z}$. In fact it can be checked that $\psi\big((x, y) + H\big) = y - 2x$ defines an isomorphism.

Exercises 6.3. Key concepts:

Factor group *well-definition* $\iff H \triangleleft G$ $\mathbb{Z}_n := {}^{\mathbb{Z}}/_{n\mathbb{Z}}$ *identifying* ${}^{G}/_{H}$

1. List the cosets of the subgroup $H = \langle 3 \rangle$ in $G = \mathbb{Z}_{15}$. Verify directly that the function

   $$\psi : \mathbb{Z}_3 \mapsto {}^{G}/_{H} : x \mapsto x + H$$

   is a well-defined homomorphism (mimic the proof of Theorem 6.19!).

2. Identify the factor group ${}^{\mathbb{Z}_4 \times \mathbb{Z}_4}/_{H}$, where $H = \{(0,0), (0,2), (2,0), (2,2)\}$ (Exercise 6.1.2).

3. (a) Identify the factor group ${}^{G}/_{H}$ where $H = \langle (2,4) \rangle \leq G = \mathbb{Z}_4 \times \mathbb{Z}_6$.
   (b) Repeat with the subgroup $H = \langle 2 \rangle \times \langle 4 \rangle$ (*this is a trick question!*)

4. (a) Let $G = \mathbb{Z}_9 \times \mathbb{Z}_9$ and $H = \langle (3,6) \rangle$. Identify ${}^{G}/_{H}$ by showing that every element of the factor group has order at most 9 and that it contains an element of order 9.
   (b) Repeat with $H = \langle 3 \rangle \times \langle 6 \rangle$ (*this isn't a trick question!*)

5. Let G be any group. To what groups are ${}^{G}/_{\{e\}}$ and ${}^{G}/_{G}$ isomorphic?

6. (a) If G is abelian and $H \leq G$, prove that ${}^{G}/_{H}$ is abelian.
   (b) If ${}^{G}/_{H}$ is abelian, can we conclude that G and/or H is abelian? Explain.

7. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_8$. Prove that each function in Examples 6.20 is a well-defined homomorphism.
   (a) $H = \langle (0,1) \rangle$, $\psi : \mathbb{Z}_4 \to {}^{G}/_{H} : x \mapsto (x,0) + H$
   (b) $H = \langle (0,2) \rangle$, $\psi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to {}^{G}/_{H} : (x,y) \mapsto (x,y) + H$
   (c) $H = \langle (2,4) \rangle$, $\psi : \mathbb{Z}_2 \times \mathbb{Z}_8 \to {}^{G}/_{H} : (x,y) \mapsto (x, y - 2x) + H$

   (*Bijectivity follows from the description of the cosets, though proving injectivity might be instructive.*)

8. Recall Exercise 6.2.9. The factor group ${}^{G}/_{H}$ is abelian and of order 6, whence it is cyclic. Prove this explicitly by finding a generator.

9. (a) Let G be a cyclic group with subgroup H. Prove that ${}^{G}/_{H}$ is cyclic.
   (b) If ${}^{G}/_{H}$ is cyclic, does it follow that G is cyclic? Prove or disprove.

10. In Example 6.21.2 we saw that $\mathbb{Z}_3 \cong {}^{A_4}/_{V}$. Find an explicit isomorphism.

11. Exercise 6.1.5 showed that $\{\rho_0, \rho_2\}$ is a normal subgroup of D_4. To what well-known group is the factor group ${}^{D_4}/_{\{\rho_0, \rho_2\}}$ isomorphic? Prove your assertion.

12. Let $H = \langle (2,3) \rangle \leq G = \mathbb{Z}_5 \times \mathbb{Z}$. Prove that ${}^{G}/_{H} \cong \mathbb{Z}_{15}$.

13. Verify the claim in Example 6.21.4 that $\psi\big((x,y) + H\big) = y - 2x$ is an isomorphism.

14. (Hard!) Let $G = \mathbb{Z}_{10} \times \mathbb{Z}_6 \times \mathbb{Z}$ and $H = \langle (4,2,3) \rangle$. Identify the factor group ${}^{G}/_{H}$ as a direct product $\mathbb{Z}_m \times \mathbb{Z}_n$.

    (*Hint: use the division algorithm $z = 3q + r$ to show that there is exactly one representative of each coset $(x,y,z) + H$ where z is either 0, 1 or 2.*)

7 Homomorphisms and the First Isomorphism Theorem

In this chapter we further discuss homomorphisms. Of particular importance is the relationship between normal subgroups, homomorphisms and factor groups.

Unless otherwise stated, in this chapter all homomorphisms are between *groups.*

7.1 Kernels and Images

Definition 7.1. Let $\phi : G \to L$ be a homomorphism. The *kernel* and *image* (or *range*) of ϕ are the sets

$$\ker\phi = \{g \in G : \phi(g) = e_L\} \qquad \operatorname{Im}\phi = \{\phi(g) : g \in G\}$$

The image is sometimes denoted $\phi(G)$. Note that $\ker\phi \subseteq G$ while $\operatorname{Im}\phi \subseteq L$.

Examples 7.2. 1. $\phi(x) = 2x \pmod 4$ defines a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_4$, with

$$\ker\phi = \{x \in \mathbb{Z} : 2x \equiv 0 \pmod 4\} = 2\mathbb{Z}, \quad \operatorname{Im}\phi = \{0, 2\}$$

2. The kernel should feel familiar from linear algebra: if $\mathrm{T} : V \to W$ is a linear map between vector spaces, then the kernel is simply the *nullspace*

$$\ker \mathrm{T} = \{\mathbf{v} \in V : \mathrm{T}(\mathbf{v}) = \mathbf{0}\}$$

Moreover, if $\mathrm{T} = \mathrm{L}_A : M_n(\mathbb{R}) \to M_m(\mathbb{R})$ is left-multiplication by a matrix A, then $\operatorname{Im}\mathrm{T}$ is the *column space* of A.

Lemma 7.3. *Let $\phi : G \to L$ be a homomorphism. Then,*

1. $\phi(e_G) = e_L$ *(ϕ maps identity to identity)*
2. $\forall g \in G,\ (\phi(g))^{-1} = \phi(g^{-1})$ *(ϕ maps inverses to inverses)*
3. $\ker\phi \triangleleft G$ *($\ker\phi$ is a normal subgroup of G)*
4. $\operatorname{Im}\phi \leq L$ *($\operatorname{Im}\phi$ is a subgroup of L)*

Proof. 1 & 2 were in Exercise 2.3.6 and we leave 4 as an exercise. We prove 3 explicitly.

3. Suppose $k_1, k_2 \in \ker\phi$. Then

$$\phi(k_1k_2) = \phi(k_1)\phi(k_2) = e_L \implies k_1k_2 \in \ker\phi$$
$$\phi(k_1^{-1}) = (\phi(k_1))^{-1} = e_L \implies k_1^{-1} \in \ker\phi$$

It follows that $\ker\phi$ is a subgroup of G.

To see that $\ker\phi$ is normal, recall Corollary 6.7: if $g \in G$ and $k \in \ker\phi$, then

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_L \implies gkg^{-1} \in \ker\phi$$

■

Examples 7.4. 1. For the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_4 : x \mapsto 2x$, we see that $\ker \phi = 2\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$, and $\operatorname{Im} \phi = \{0, 2\} = \langle 2 \rangle$ a subgroup of $\mathbb{Z}_4$.

2. The nullspace of a linear map $\mathrm{T} : V \to W$ is indeed a *subspace* and thus a subgroup $\ker \mathrm{T} \leq V$: since V is abelian, this is a normal subgroup. Moreover, $\operatorname{Im} \mathrm{T}$ is also a subspace/group of W.

3. $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism, whence we obtain a normal subgroup

$$\ker \det = \mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det A = 1\} \triangleleft \mathrm{GL}_n(\mathbb{R})$$

4. $\phi : \mathbb{Z} \to \mathbb{Z}_{20} : x \mapsto 4x \pmod{20}$ is a homomorphism, as may be checked:

$$\phi(x + y) = 4(x + y) = 4x + 4y = \phi(x) + \phi(y) \in \mathbb{Z}_{20}$$

Its kernel and image are $\ker \phi = 5\mathbb{Z} \leq \mathbb{Z}$ and $\operatorname{Im} \phi = \langle 4 \rangle = \{0, 4, 8, 12, 16\} \leq \mathbb{Z}_{20}$

Since every kernel is a normal subgroup, it is worth identifying the distinct cosets with a view to describing the factor group ${}^{G}\!/_{\ker \phi}$.

Lemma 7.5. *Let $\phi : G \to L$ be a homomorphism. Then*

$$g_1 \ker \phi = g_2 \ker \phi \iff \phi(g_1) = \phi(g_2)$$

There is precisely one coset of $\ker \phi$ for each element of $\operatorname{Im} \phi$; otherwise said $(G : \ker \phi) = |\operatorname{Im} \phi|$.

Proof. For all $g_1, g_2 \in G$, we have

$$\begin{aligned} g_1 \ker \phi = g_2 \ker \phi &\iff g_2^{-1} g_1 \in \ker \phi && \text{(Theorem 6.5)} \\ &\iff \phi(g_2^{-1} g_1) = e_L && \text{(Definition 7.1)} \\ &\iff \phi(g_2)^{-1} \phi(g_1) = e_L && \text{(Lemma 7.3)} \\ &\iff \phi(g_1) = \phi(g_2) \end{aligned}$$

■

We'll extend this idea shortly; for the moment we use it to aid in finding homomorphisms.

Theorem 7.6. *Let $\phi : G \to L$ be a homomorphism. If G (or L) is finite, then $\operatorname{Im} \phi$ is a finite group whose order divides that of G (or L). Otherwise said:*

$$|G| < \infty \implies |\operatorname{Im} \phi| \,\Big|\, |G| \quad \textit{and} \quad |L| < \infty \implies |\operatorname{Im} \phi| \,\Big|\, |L|$$

Proof. If G is a finite group, then $\ker \phi \leq G$ is finite. Now apply Lemma 7.5:

$$|\operatorname{Im} \phi| = (G : \ker \phi) = \frac{|G|}{\ker \phi}$$

is a divisor of $|G|$. The second case $|\operatorname{Im} \phi| \,\Big|\, |L|$ is Lagrange's Theorem (6.8).

■

Examples 7.7. 1. How many distinct homomorphisms are there $\phi : \mathbb{Z}_{17} \to \mathbb{Z}_{13}$?

If ϕ is such a homomorphism, the Theorem says that $|\operatorname{Im}\phi|$ divides both 17 and 13. The only such positive integer is 1. Since $\operatorname{Im}\phi$ must contain the identity, we conclude that there is only one homomorphism!

$$\forall x \in \mathbb{Z}_{17},\ \phi(x) = 0$$

More generally, if $\gcd(|G|, |L|) = 1$, then the only homomorphism $\phi : G \to L$ is the trivial function $\phi : g \mapsto e_L$.

2. Describe all homomorphisms $\phi : \mathbb{Z}_4 \to S_3$.

Since the domain $\mathbb{Z}_4$ is cyclic, we need only describe what happens to a generator (e.g. 1) to obtain the entire homomorphism $\phi(x) = \big(\phi(1)\big)^x$. There are at most *six* homomorphisms; one for each possible element $\phi(1) \in S_3$. Not all of these cases are however possible.

The Theorem says that $|\operatorname{Im}\phi| = 1$ or 2; the only common divisors of $4 = |\mathbb{Z}_4|$ and $6 = |S_3|$.

If $\operatorname{Im}\phi$ has one element, we obtain the trivial homomorphism $\phi_(x) = e,\ \forall x \in \mathbb{Z}_4$.

If $|\operatorname{Im}\phi| = 2$, then $\operatorname{Im}\phi$ is a subgroup of order 2 of which S_3 contains exactly three: $\{e, (2\,3)\}$, $\{e, (1\,3)\}$, $\{e, (1\,2)\}$. We therefore have three further homomorphisms

$$\phi_1(x) = (2\,3)^x, \quad \phi_2(x) = (1\,3)^x, \quad \phi_3(x) = (1\,2)^x$$

for a grand total of four distinct homomorphisms.

We now consider the general question of homomorphisms between finite cyclic groups $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$. Two facts make this relatively simple:

1. It is enough to define $\phi(1)$, for then $\phi(x) = \phi(1) + \cdots + \phi(1) = \phi(1) \cdot x$.
2. $|\operatorname{Im}\phi|$ must divide $d := \gcd(m, n)$. Since $\mathbb{Z}_n$ has exactly one subgroup of each order dividing n (Corollary 3.20), $\operatorname{Im}\phi$ must be a subgroup of the unique subgroup of $\mathbb{Z}_n$ of order d:

$$\operatorname{Im}\phi \leq \left\langle \frac{n}{d} \right\rangle = \left\{ 0, \frac{n}{d}, \frac{2n}{d}, \ldots, \frac{(d-1)n}{d} \right\}$$

We need only try letting $\phi(1)$ be each element of this group in turn…

Corollary 7.8. *There are $d = \gcd(m, n)$ distinct homomorphisms $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$, defined by*

$$\phi_k(x) = \frac{kn}{d}x \quad \textit{where} \quad k = 0, \ldots, d-1$$

Proof. Following the above, it remains only to check that each ϕ_k is a well-defined function. For this, note first that $x = y \in \mathbb{Z}_m \iff y = x + \lambda m$ for some $m \in \mathbb{Z}$, from which

$$\phi_k(y) = \phi_k(x + \lambda m) = \frac{kn}{d}(x + \lambda m) = \frac{kn}{d}x + \lambda k \frac{m}{d} n = \frac{kn}{d}x = \phi_k(x) \qquad (\text{in } \mathbb{Z}_n)$$

where we used the fact that $\frac{m}{d}$ is an *integer.* ∎

Example 7.9. We describe all homomorphisms $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$.
Since $\gcd(12, 20) = 4$, we see that $\operatorname{Im}\phi \leq \langle 5 \rangle = \{0, 5, 10, 15\} \leq \mathbb{Z}_{20}$. There are four choices:

$$\phi_0(x) = 0, \qquad \phi_1(x) = 5x, \qquad \phi_2(x) = 10x, \qquad \phi_3(x) = 15x \pmod{20}$$

Reversing the argument, we see that there are also four distinct homomorphisms $\psi : \mathbb{Z}_{20} \to \mathbb{Z}_{12}$:

$$\psi_0(x) = 0, \qquad \psi_1(x) = 3x, \qquad \psi_2(x) = 6x, \qquad \psi_3(x) = 9x \pmod{12}$$

Exercises 7.1. Key concepts:

Image *kernels are normal subgroups* $(G : \ker\phi) = |\operatorname{Im}\phi|$ $|\operatorname{Im}\phi| \,\Big|\, \gcd(|G|, |L|)$

1. Check that you have a homomorphism (use Corollary 7.8) and compute its kernel and image.
   (a) $\phi : \mathbb{Z}_8 \to \mathbb{Z}_{14}$ defined by $\phi(x) = 7x \pmod{14}$.
   (b) $\phi : \mathbb{Z}_{36} \to \mathbb{Z}_{20}$ defined by $\phi(x) = 5x \pmod{20}$.
2. Describe all homomorphisms between the groups:
   (a) $\phi : \mathbb{Z}_{15} \to \mathbb{Z}_{80}$ (b) $\phi : \mathbb{Z} \to \mathbb{Z}_3$
   (c) $\phi : \mathbb{Z}_6 \to D_4$ (d) $\phi : \mathbb{Z}_{15} \to A_4$
3. Find the kernel and image of each homomorphism.
   (a) The *trace* of a matrix: $\operatorname{tr} : M_2(\mathbb{R}) \to \mathbb{R}$ defined by $\operatorname{tr}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = a + d = a + d$
   (b) $\mathrm{T} : \mathbb{R}^3 \to \mathbb{R}^4 : \mathbf{x} \mapsto \begin{pmatrix} 1 & 1 & -1 \\ 0 & 3 & -1 \\ 1 & 4 & -2 \\ 2 & 5 & -3 \end{pmatrix}$ (*Hint: remember row operations...*)
4. Explain why the map ϕ is a homomorphism and find $\ker\phi$:
$$\phi : S_n \to \big(\{1, -1\}, \cdot\big) : \sigma \mapsto \begin{cases} 1 & \text{if } \sigma \text{ even} \\ -1 & \text{if } \sigma \text{ odd} \end{cases}$$
5. (a) Prove Part 4 of Lemma 7.3: if $\phi : G \to L$ is a homomorphism, then $\operatorname{Im}\phi \leq L$.
   (b) If $H \leq G$ and $\phi : G \to L$ a homomorphism, prove that $\phi(H) := \{\phi(h) : h \in H\} \leq \operatorname{Im}\phi$.
   (c) Give an example to show that $\operatorname{Im}\phi$ need not be a normal subgroup of L.
6. Prove that the number of distinct *isomorphisms* $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ equals the cardinality of the group of units in $\mathbb{Z}_n$ (see Exercise 3.2.10))
$$\left|\mathbb{Z}_n^\times\right| = |\{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}|$$
7. Prove that $\phi : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ is a well-defined homomorphism if and only if there exist integers a, b, c, d for which
$$\phi(x, y) = \big(ax + by, cx + dy\big), \quad m \mid bn \quad \text{and} \quad n \mid cm$$
(*Hint: let* $(a, c) = \phi(1, 0)$, *etc.*)
8. Find all homomorphisms $\phi : \mathbb{Z}_2 \times \mathbb{Z}_7 \to \mathbb{Z}_2 \times \mathbb{Z}_5$. How do you know that there are no more?
9. Consider $\phi : D_4 \to D_4 : \sigma \mapsto \sigma^2$. Show that ϕ is *not* a homomorphism.

7.2 The First Isomorphism Theorem

We've seen that all kernels of group homomorphisms are normal subgroups. In fact *all* normal subgroups are the kernel of some homomorphism.

Theorem 7.10 (Canonical Homomorphism). *Let G be a group and $H \triangleleft G$. Then the function*

$$\gamma : G \to {}^{G}\!/_{H} \quad \textit{defined by} \quad \gamma(g) = gH$$

is a homomorphism with $\ker \gamma = H$.

Proof. Since H is normal, ${}^{G}\!/_{H}$ is a group. By the definition of multiplication in ${}^{G}\!/_{H}$,

$$\gamma(g_1)\gamma(g_2) = g_1H \cdot g_2H = (g_1g_2)H = \gamma(g_1g_2)$$

whence γ is a group homomorphism. Moreover, the identity in the factor group is H, whence

$$\ker \gamma = \{g \in G : \gamma(g) = H\} = \{g \in G : gH = H\} = H$$

■

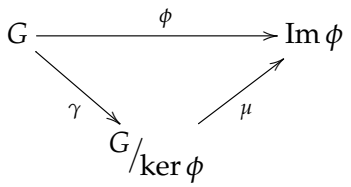
This might feel a little sneaky and unsatisfying; we'd perhaps have preferred a homomorphism that doesn't have a factor group as its image! However, the following companion result says that, among homomorphisms with the same kernel, γ is unavoidable.

Theorem 7.11 (1st Isomorphism Thm). *Let $\phi : G \to L$ be a homomorphism with kernel H. Then*

$$\mu : {}^{G}\!/_{H} \to \operatorname{Im}\phi \quad \textit{defined by} \quad \mu(gH) = \phi(g)$$

is an isomorphism. Otherwise said, ${}^{G}\!/_{\ker\phi} \cong \operatorname{Im}\phi$.

The results may be summarized in a *commutative diagram:* any homomorphism $\phi : G \to L$ *factors* as $\phi = \mu \circ \gamma$ where γ is the canonical homomorphism with kernel $\ker\phi$. There are analogues in several other parts of mathematics; in particular, the rank–nullity theorem from linear algebra is of close kin.



Proof. The factor group exists since $\ker\phi \triangleleft G$ (Lemma 7.3). We check the isomorphism properties:

Well-definition and Bijectivity: These are immediate from Lemma 7.5 after writing $H = \ker\phi$:

$$g_1H = g_2H \iff \phi(g_1) = \phi(g_2) \iff \mu(g_1H) = \mu(g_2H)$$

Homomorphism: For all $g_1H, g_2H \in {}^{G}\!/_{H}$,

$$\begin{aligned} \mu(g_1H \cdot g_2H) &= \mu(g_1g_2H) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) && (\phi \text{ is a homomorphism}) \\ &= \mu(g_1H)\mu(g_2H) \end{aligned}$$

We conclude that μ is an isomorphism.

■

Examples 7.12. 1. Let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$ be the homomorphism $\phi(x) = 5x \pmod{20}$ (Example 7.9). Its kernel and image are

$$\ker\phi = \{x \in \mathbb{Z}_{12} : 5x \equiv 0 \pmod{20}\} = \{0,4,8\} = \langle 4\rangle \leq \mathbb{Z}_{12}$$
$$\operatorname{Im}\phi = \{5x \in \mathbb{Z}_{20} : x \in \mathbb{Z}_{12}\} = \{0,5,10,15\} = \langle 5\rangle \leq \mathbb{Z}_{20}$$

The relevant factor group is

$$\mathbb{Z}_{12}/_{\ker\phi} = \Big\{\{0,4,8\},\{1,5,9\},\{2,6,10\},\{3,7,11\}\Big\} = \{\langle 4\rangle, 1+\langle 4\rangle, 2+\langle 4\rangle, 3+\langle 4\rangle\}$$

The canonical homomorphism γ and the isomorphism μ are

$$\gamma(x) = x + \langle 4\rangle \qquad \mu\big(x+\langle 4\rangle\big) = 5x$$

$$\begin{array}{ccccc} \mathbb{Z}_{12} & \xrightarrow{\quad\gamma\quad} & \mathbb{Z}_{12}/_{\langle 4\rangle} & \xrightarrow{\quad\mu\quad} & \operatorname{Im}\phi \\ x & \longmapsto & x+\langle 4\rangle & \longmapsto & 5x \end{array} \qquad \phi = \mu\circ\gamma$$

2. (Example 6.21.1) Let $H = \langle 2\pi\rangle \leq \mathbb{R}$ and define $\phi : \mathbb{R} \to (\mathbb{C}^\times, \cdot)$ by $\phi(x) = e^{ix}$. This is a homomorphism with

$$\ker\phi = \{x \in \mathbb{R} : e^{ix} = 1\} = H \quad \text{and} \quad \operatorname{Im}\phi = S^1$$

The canonical homomorphism is

$$\gamma : \mathbb{R} \to \mathbb{R}/_H : x \mapsto x + \langle 2\pi\rangle$$

while the isomorphism we saw previously

$$\mu : \mathbb{R}/_H \to S^1 : x + \langle 2\pi\rangle \mapsto e^{ix}$$

is precisely that arising from the 1st isomorphism theorem.

3. The map $\phi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ defined by $\phi(x,y) = 3x - 2y$ is a homomorphism. Moreover

$$\phi(x,y) = (0,0) \iff 3x = 2y \iff (x,y) = (2n,3n) \text{ for some } n \in \mathbb{Z}$$

We conclude that $\ker\phi = \langle(2,3)\rangle$. The canonical homomorphism is

$$\gamma : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}/_{\langle(2,3)\rangle} : (x,y) \mapsto (x,y) + \langle(2,3)\rangle$$

Since ϕ is surjective, we see that

$$\mathbb{Z}\times\mathbb{Z}/_{\langle(2,3)\rangle} \cong \mathbb{Z} \quad \text{via} \quad \mu\big((x,y)+\langle(2,3)\rangle\big) = 3x - 2y$$

With a little creativity, the theorem can be applied to the identification of factor groups: given $H \triangleleft G$, cook up a homomorphism $\phi : G \to L$ with $\ker\phi = H$, then $G/_H \cong \operatorname{Im}\phi$. We revisit some examples from the previous section in this context.

Examples (6.20, mk.II). Let $G = \mathbb{Z}_4 \times \mathbb{Z}_8$. For each subgroup H, we describe a homomorphism $\phi : G \to L$ with $\ker \phi = H$. There are many possible choices for ϕ; while ours will line up with what we saw in the original incarnation of these examples, hopefully you'll feel that the reasons for such choices are independent of our earlier discussion.

1. Given $H = \langle (0,1) \rangle$, we need a homomorphism where $\phi(0,1)$ is the identity. A simple way to do this is to ignore y and define

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 : (x,y) \mapsto x$$

   This indeed has kernel $\ker \phi = \{(0,y) : y \in \mathbb{Z}_8\} = H$, whence

   $$G/_H \cong \operatorname{Im} \phi = \mathbb{Z}_4$$

   via the isomorphism $\mu : (x,y) + H \mapsto x$.

   Note that μ is precisely the *inverse* of the isomorphism $\psi : x \mapsto (x,0) + H$ stated in the original version of this example; $(x,y) + H = (x,0) + H$ for this subgroup!

2. Given $H = \langle (0,2) \rangle$ we require $\phi(0,2)$ to be the identity. We may easily do this by taking y modulo 2 and defining

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 \times \mathbb{Z}_2 : (x,y) \mapsto (x,y)$$

   This is a homomorphism with the correct kernel $\ker \phi = H$. Indeed ϕ is also surjective, whence

   $$G/_H \cong \operatorname{Im} \phi = \mathbb{Z}_4 \times \mathbb{Z}_2$$

   via the isomorphism $\mu\big((x,y) + H\big) = (x,y)$. Once again μ is the inverse of $\psi(x,y) = (x,y) + H$ in the original example.

3. If $H = \langle (2,4) \rangle = \{(0,0),(2,4)\}$, it is significantly trickier to find a suitable homomorphism. One approach is to observe that

   $$(x,y) \in H \iff x \equiv 0 \pmod 2 \text{ and } y - 2x \equiv 0 \pmod 8$$

   We therefore choose the homomorphism

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_2 \times \mathbb{Z}_8 : (x,y) \mapsto \big(x, y - 2x\big)$$

   It is worth checking that this is well-defined: the $2x$ in the second factor is crucial! Certainly ϕ has the correct kernel. It is moreover surjective, e.g. $(p,q) = \phi(p, q + 2p)$, whence

   $$G/_H \cong \operatorname{Im} \phi = \mathbb{Z}_2 \times \mathbb{Z}_8$$

   via the isomorphism $\mu\big((x,y) + H\big) = (x, y - 2x)$.

Other homomorphisms are possible in all the above examples. This approach requires a little creativity! In general, it can be very difficult to *construct* a simple homomorphism with the correct kernel.

Exercises 7.2. Key concepts:

Canonical homomorphism $\gamma : G \to {}^{G}\!/_{H}$ *1st isomorphism theorem* $\mu : {}^{G}\!/_{H} \cong \operatorname{Im}\phi$

1. Let $\phi : \mathbb{Z}_{18} \to \mathbb{Z}_{12}$ be the homomorphism $\phi(x) = 10x$.
   (a) Find the kernel of and image of ϕ.
   (b) List the elements of the factor group ${}^{\mathbb{Z}_{18}}\!/_{\ker\phi}$.
   (c) State an explicit isomorphism $\mu : {}^{\mathbb{Z}_{18}}\!/_{\ker\phi} \to \operatorname{Im}\phi$.
   (d) To what basic group $\mathbb{Z}_n$ is the factor group isomorphic?
2. Repeat the previous question for the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_{20} : x \mapsto 8x$.
3. For each function $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, find the kernel and identify the factor group ${}^{\mathbb{Z}\times\mathbb{Z}}\!/_{\ker\phi}$.
   (a) $\phi(x,y) = 3x + y$ (b) $\phi(x,y) = 2x - 4y$
4. (a) If a subgroup H of $G = \mathbb{Z}_{15} \times \mathbb{Z}_3$ has order 5, find its elements.
   (b) Show that $\phi(x,y) = (x,y)$ is a homomorphism $\phi : G \to \mathbb{Z}_3 \times \mathbb{Z}_3$ with $\ker\phi = H$.
   (c) What does the 1st isomorphism theorem tell us about the factor group ${}^{G}\!/_{H}$?
5. Suppose G is a finite group with normal subgroup H and that $\phi : G \to L$ is a homomorphism with $\ker\phi = H$. Prove that $(G : H) \leq |L|$ with equality if and only if ϕ is surjective.
6. Consider the map $\phi : \mathbb{Z} \times \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_6$ defined by
   $$\phi(x,y) = \big(2x + y, y\big)$$
   (a) Verify that ϕ is a well-defined homomorphism.
   (b) Compute $\ker\phi$ and identify the factor group ${}^{\mathbb{Z}\times\mathbb{Z}_{12}}\!/_{\ker\phi}$
7. Let $H = \langle(3,1)\rangle \leq G = \mathbb{Z}_9 \times \mathbb{Z}_3$. Find an explicit homomorphism $\phi : G \to \mathbb{Z}_9$ whose kernel is H, and thus identify the factor group ${}^{G}\!/_{H}$.
   (*Hint:* $(x,y) \in H = \{(0,0),(3,1),(6,2)\} \iff \ldots$)
8. Consider $H = \langle(3,3)\rangle \leq G = \mathbb{Z}_9 \times \mathbb{Z}_9$. Find a surjective homomorphism $\phi : G \to \mathbb{Z}_3 \times \mathbb{Z}_9$ whose kernel is H and hence prove that ${}^{G}\!/_{H} \cong \mathbb{Z}_3 \times \mathbb{Z}_9$.
9. Let $\phi : S^1 \to S^1 : z \mapsto z^2$.
   (a) Find the kernel of ϕ and describe the canonical homomorphism $\gamma : S_1 \to {}^{S^1}\!/_{\ker\phi}$.
   (b) What does the first isomorphism theorem say about the factor group ${}^{S^1}\!/_{\ker\phi}$.
   (c) For each n, identify the factor group ${}^{S^1}\!/_{U_n}$, where U_n is the group of n^{th} roots of unity.

7.3 Conjugation, Cycle Types, Centers and Automorphisms

In this section we consider an important type of homomorphism and some its consequences.

Definition 7.13. Let G be a group and $x, y \in G$. We say that y is *conjugate to* x if

$$\exists g \in G \quad \text{such that} \quad y = gxg^{-1}$$

If $g \in G$ is fixed, then *conjugation by* g is the map $c_g : G \to G : x \mapsto gxg^{-1}$.

We've met this notion before: recall that a subgroup H is normal if and only if $c_g(h) \in H$ for all $g \in G$ (Corollary 6.7). It should also be familiar from linear algebra, in the form of *similarity*. Recall that square matrices A, B are similar if $B = MAM^{-1}$ for some invertible M. Such matrices have the same eigenvalues and, essentially, 'do the same thing' with respect to different bases. An explicit group theory analogue of this is Theorem 7.17 below.

Lemma 7.14. *Conjugation by g is a isomorphism $c_g : G \cong G$.*

Proof. Conjugation by g^{-1} is the inverse function of c_g^{-1}:

$$c_{g^{-1}}\big(c_g(x)\big) = g^{-1}gxg^{-1}(g^{-1})^{-1} = x, \text{ etc.}$$

We moreover have a homomorphism:

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

■

Lemma 7.15. *Conjugacy is an equivalence relation ($x \sim y \iff \exists g \in G$ such that $y = gxg^{-1}$).*

The proof is an exercise. The equivalence classes under conjugacy are termed *conjugacy classes*.

Examples 7.16. 1. If G is abelian then every conjugacy class contains only one element:

$$x \sim y \iff \exists g \in G \quad \text{such that} \quad y = gxg^{-1} = xgg^{-1} = x$$

2. The smallest non-abelian group is S_3 has conjugacy classes

$$\{e\}, \quad \{(12),(13),(23)\}, \quad \{(123),(132)\}$$

This can be computed directly, but it follows immediately from...

Theorem 7.17. *The conjugacy classes of S_n are the* cycle types*: elements are conjugate if and only if they have the same cycle type.*

If an element $\sigma \in S_n$ is written as a product of disjoint cycles, then its cycle type is clear. For instance:

- $(123)(45)$ has the same cycle type as $(156)(23)$: we might call these 3,2-cycles.
- $(12)(34)$ has a different cycle type; 2,2.

Before seeing the proof it is beneficial to try an example.

Example 7.18. If $\rho = (243)$ and $\sigma = (12)(34)$ in S_4, then

$$\rho\sigma\rho^{-1} = (243)(12)(34)(234) = (14)(23)$$

Not only does this have the same cycle type as σ, but if may be obtained simply by applying ρ to the entries of σ!

$$\rho\sigma\rho^{-1} = (14)(23) = \big(\rho(1)\,\rho(2)\big)\big(\rho(3)\,\rho(4)\big)$$

This also tells us how to reverse the process: given 2,2-cycles $\sigma = (12)(34)$ and $\tau = (14)(23)$ simply place σ on top of τ in a table to define a suitable $\rho = (243)$ for which $\rho\sigma\rho^{-1} = \tau$.

x	1	2	3	4
$\rho(x)$	1	4	2	3

The proof is nothing more than the example done abstractly!

Proof. ($\Rightarrow$) We consider conjugation by $\rho \in S_n$. First let $\sigma = (a_1 \cdots a_k)$ be a k-cycle and write

$$A = \{a_1, \ldots, a_k\}, \qquad R = \{\rho(a_1), \ldots, \rho(a_k)\}$$

Since ρ is a bijection, $|R| = k$ are distinct and $x \in R \iff \rho^{-1}(x) \in A$. There are two cases:

If $x \in R$: Let $x = \rho(a_j)$, then

$$\rho\sigma\rho^{-1}\big(\rho(a_j)\big) = \rho\sigma(a_j) = \rho(a_{j+1})$$

where a_{k+1} is understood to be a_1.

If $x \notin R$: Since $\rho^{-1}(x) \notin A$ it is unmoved by σ, whence

$$\rho\sigma\rho^{-1}(x) = \rho\sigma(\rho^{-1}(x)) = \rho\rho^{-1}(x) = x$$

We conclude that $\rho\sigma\rho^{-1} = \big(\rho(a_1)\cdots\rho(a_k)\big)$ is also a k-cycle!

More generally, if $\sigma = \sigma_1 \cdots \sigma_l$ is a product of disjoint cycles, then

$$\rho\sigma\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1})\cdots(\rho\sigma_l\rho^{-1})$$

has the same cycle type as σ.

($\Leftarrow$) Suppose $\sigma = \sigma_1 \cdots \sigma_l$ and $\tau = \tau_1 \cdots \tau_l \in S_n$ have the same cycle type, written so that the corresponding orbits have the same length. Moreover, assume we've included all necessary 1-cycles so that $\bigcup \sigma_i = \{1, \ldots, n\} = \bigcup \tau_i$. Define a permutation ρ by writing the orbits of σ and τ on top each other

x	σ_1	σ_2	$\cdots$	σ_l
$\rho(x)$	τ_1	τ_2	$\cdots$	τ_l

If $s_{i,j}$ and $t_{i,j}$ are the j^{th} elements of the orbits σ_i and τ_i, then

$$\rho\sigma\rho^{-1}(t_{i,j}) = \rho\sigma(s_{i,j}) = \rho\big(s_{i,j+1}\big) = t_{i,j+1} = \tau\big(t_{i,j}\big)$$

We conclude that $\rho\sigma\rho^{-1} = \tau$, as required. ∎

Examples 7.19. 1. The permutations $\sigma = (145)(276)$ and $\tau = (165)(347)$ in S_7 are conjugate: the table defines a suitable ρ.

x	1	4	5	2	7	6	3
$\rho(x)$	1	6	5	3	4	7	2

$$\Longrightarrow \rho = (23)(467)$$

Indeed

$$\rho\sigma\rho^{-1} = (23)(467)(145)(276)(23)(476) = (165)(347) = \tau$$

There are other possible choices of ρ; just write the orbits of σ, τ in different orders.

2. (Example 6.3.2) We've checked previously that $V = \{e, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of A_4. It is moreover a normal subgroup of S_4: since V contains the identity and all 2,2-cycles it is closed under conjugacy and thus a normal subgroup of both A_4 and S_4.

Automorphisms

We've already seen that conjugation $c_g : G \to G$ by a fixed element is an isomorphism. We now consider all such maps.

Definition 7.20. An *automorphisms* of a group G is an isomorphism of G with itself. The set of such is denoted $\operatorname{Aut} G$. The *inner automorphisms* are the conjugations

$$\operatorname{Inn} G = \{c_g : G \to G \text{ where } c_g(x) = gxg^{-1}\}$$

Example 7.21. There are four homomorphisms $\phi_k : \mathbb{Z}_4 \to \mathbb{Z}_4$ (Corollary 7.8);

$$\phi_0(x) = 0, \quad \phi_1(x) = x, \quad \phi_2(x) = 2x, \quad \phi_3(x) = 3x$$

of which two are automorphisms: $\operatorname{Aut}\mathbb{Z}_4 = \{\phi_1, \phi_3\}$. Observe that ϕ_1 is the identity function and that $\phi_3 \circ \phi_3 = \phi_1$. The automorphisms therefore comprise a *group* (necessarily isomorphic to $\mathbb{Z}_2$) under composition of functions.

As for conjugations, observe that for any $g \in \mathbb{Z}_4$,

$$c_g(x) = g + x + (-g) = x$$

since $\mathbb{Z}_4$ is abelian. There is only one inner automorphism of $\mathbb{Z}_4$, the identity function ϕ_1.

Hunting for automorphisms can be difficult. Here is a helpful observation for narrowing things down; the proof is an exercise.

Lemma 7.22. *If $\phi \in \operatorname{Aut} G$ and $x \in G$, then the orders of x and $\phi(x)$ are identical.*

This helps to streamline the previous example: $\phi(1)$ must have the same order (four) as 1 and so our only possibilities are $\phi(1) = 1$ or $\phi(1) = 3$. These possibilities generate the two observed automorphisms.

Example 7.23. We describe all automorphisms ϕ of S_3. Consider $\sigma = (12)$ and $\tau = (123)$. Since the order of an element is preserved by ϕ, we conclude that

$$\phi(e) = e, \quad \phi(\sigma) \in \{(12), (13), (23)\}, \quad \phi(\tau) \in \{(123), (132)\}$$

We therefore have a maximum of *six* possible automorphism; it is tedious to check, but *all* really do define automorphisms! Indeed all may be explicitly realized as conjugations whence $\operatorname{Aut} S_3 = \operatorname{Inn} S_3$. Here is the data; verify some of it for yourself:

element g	$c_g(e)$	$c_g(12)$	$c_g(13)$	$c_g(23)$	$c_g(123)$	$c_g(132)$
e	e	(12)	(13)	(23)	(123)	(132)
(12)	e	(12)	(23)	(13)	(132)	(123)
(13)	e	(23)	(13)	(12)	(132)	(123)
(23)	e	(13)	(12)	(23)	(132)	(123)
(123)	e	(23)	(12)	(13)	(123)	(132)
(132)	e	(13)	(23)	(12)	(123)	(132)

As the next result shows, the automorphisms again form a group under composition, in this case a group of order 6 which is easily seen to be *non-abelian*: for instance

$$c_{(12)}c_{(13)} = c_{(132)} \neq c_{(123)} = c_{(13)}c_{(12)}$$

By process of elimination, we conclude that $\operatorname{Aut} S_3 \cong S_3$.

Theorem 7.24. *$\operatorname{Aut} G$ and $\operatorname{Inn} G$ are groups under composition. Moreover $\operatorname{Inn} G \triangleleft \operatorname{Aut} G$.*

Proof. That $\operatorname{Aut} G$ is a group is simply the fact that composition and inverses of isomorphisms are isomorphisms: you should already have made this argument when answering Exercise 2.3.13. By Lemma 7.14, every conjugation is an isomorphism, and it is simple to check that $c_g \circ c_h = c_{gh}$ and $c_g^{-1} = c_{g^{-1}}$: we conclude that $\operatorname{Inn} G \subseteq \operatorname{Aut} G$.
For normality, we check that $\operatorname{Inn} G$ is closed under conjugation! Let $\tau \in \operatorname{Aut} G$ and $c_g \in \operatorname{Inn} G$. For any $x \in G$, we have[22]

$$\begin{aligned}
(\tau c_g \tau^{-1})(x) &= \tau\Big(c_g\big(\tau^{-1}(x)\big)\Big) && \text{(definition of } c_g\text{)} \\
&= \tau\Big(g\big(\tau^{-1}(x)\big)g^{-1}\Big) \\
&= \Big(\tau(g)\Big)\Big(\tau\big(\tau^{-1}(x)\big)\Big)\Big(\tau(g^{-1})\Big) && \text{(since } \tau \text{ is a homomorphism)} \\
&= \big(\tau(g)\big)x\big(\tau(g)\big)^{-1} && \text{(again since } \tau \text{ is an homomorphism)} \\
&= c_{\tau(g)}(x)
\end{aligned}$$

We conclude that $\tau c_g \tau^{-1} = c_{\tau(g)} \in \operatorname{Inn} G$, from which $\operatorname{Inn} G \triangleleft \operatorname{Aut} G$. ∎

[22] The challenge in reading the proof is simply to keep track of where everything lives. To help, the inverse symbol is colored: τ^{-1} means the inverse *function*, whereas g^{-1} means the inverse of an *element* in G.

Centers

We say that an element g in a group G *commutes* with another element $x \in G$ if the order of multiplication is irrelevant: i.e. if $gx = xg$. Otherwise said, if $c_g(x) = x$. It natural to ask whether there are any elements which commute with *all others.* There are two very simple cases:

- If G is abelian, then every element commutes with every other element!
- The identity e commutes with everything, regardless of G.

In general, the set of such elements will fall somewhere between these extremes. This subset will turn out to be another normal subgroup of G.

Definition 7.25. The *center* of a group G is the subset of G which commutes with everything in G:

$$Z(G) := \{g \in G : \forall h \in G,\ gh = hg\}$$

We will prove that $Z(G) \triangleleft G$ shortly. First we give a few examples; unless G is abelian, the center is typically difficult to compute, so we omit more of the details.

Examples 7.26. 1. $Z(G) = G \iff G$ is abelian.

2. $Z(S_n) = \{e\}$ if $n \geq 3$. This is straightforward to check when $n = 3$ since there are only six elements. In general, think about the proof of Theorem 7.17…
3. $Z(D_{2n+1}) = \{e\}$ and $Z(D_{2n}) = \{e, \rho_{n/2}\}$, where $\rho_{n/2}$ is rotation by 180°. For instance, it is easy to see in D_{2n+1} that any rotation and reflection fail to commute.
4. $Z\big(\mathrm{GL}_n(\mathbb{R})\big) = \{\lambda I_n : \lambda \in \mathbb{R}^\times\}$. If you've done enough linear algebra, an argument is reasonably straightforward (Exercise 12)

Theorem 7.27. *For any group G:*

1. $Z(G) \triangleleft G$
2. $G/Z(G) \cong \operatorname{Inn} G$

Proof. 1. The function $\phi : G \to \operatorname{Inn} G$ defined by $\phi(g) = c_g$ is a homomorphism:

$$c_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = c_g(c_h(x))$$
$$\implies \phi(gh) = \phi(g)\phi(h)$$

Now observe that

$$g \in \ker\phi \iff \forall x \in G,\ c_g(x) = gxg^{-1} = x \iff g \in Z(G)$$

from which $\ker\phi = Z(G)$ is a normal subgroup of G.

2. Since ϕ is surjective, the 1st isomorphism theorem tells us that

$$G/Z(G) \cong \operatorname{Im}\phi = \operatorname{Inn} G$$

■

Exercises 7.3. Key concepts:

Conjugation *conjugacy classes* *cycle types are conjugacy classes in S_n*
(inner) automorphism *center of a group*

1. Either find some $\rho \in G$ such that $\rho\sigma\rho^{-1} = \tau$, or explain why no such element exists:
   (a) $\sigma = (1\,2\,3)$, $\tau = (1\,3\,2)$ where $G = S_3$.
   (b) $\sigma = (1\,4\,5\,6)(2\,3)(5\,6)$, $\tau = (1\,2\,3\,4)(5\,6)(2\,6)$ where $G = S_6$.
   (c) $\sigma = (1\,4\,5\,6)(2\,3)(5\,6)$, $\tau = (1\,2)(3\,5\,6)$ where $G = S_6$.
2. Recall Example 7.19.1. Find another element $\nu \neq \rho$ for which $\nu\sigma\nu^{-1} = \tau$.
3. Prove Lemma 7.15. Prove that the relation

   $$x \sim y \iff y \text{ is conjugate to } x$$

   is an equivalence relation on any group G.
4. (a) Suppose y is conjugate to x in a group G. Prove that the orders of x and y are identical.
   (b) Show that the converse to part (a) is *false* by exhibiting two non-conjugate elements of the same order in some group.
5. Let $H \leq G$, fix $a \in G$ and define the *conjugate subgroup* $K = c_a(H) = \{aha^{-1} : h \in H\}$.
   (a) Prove that K is indeed a subgroup of G.
   (b) Prove that the function $\psi : H \to K : h \mapsto aha^{-1}$ is an isomorphism of groups.
   (c) If $H \triangleleft G$, what can you say about $c_a(H)$?
   (d) Let $H = \{e, (1\,2)\} \leq S_3$ and $a = (1\,2\,3)$. Compute the conjugate subgroup $K = c_a(H)$.
6. We've already seen that $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a normal subgroup of S_4.
   (a) Show that *normal subgroup* is not transitive by giving an example of a normal subgroup $K \triangleleft V$ which is *not normal* in S_4.
   (b) How many *other* subgroups does S_4 have which are isomorphic to V? Why are none of them normal in S_4?
   (c) Explain why S_4/V is a group of order six. Prove that

   $$(1\,2)V(1\,3)V \neq (1\,3)V(1\,2)V$$

   Hence conclude that $S_4/V \cong S_3$.
   (d) Why is it obvious that the following six left cosets are distinct.

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

   (*Hint: Think about how none of the representatives a of the above cosets move the number 4 and consider* $aV = bV \iff b^{-1}a \in V \ldots$)
   (e) Define an isomorphism $\mu : S_4/V \to S_3$ and prove that it is an isomorphism.

7. Prove Lemma 7.22: if $\phi \in \operatorname{Aut} G$ and $x \in G$, then $\phi(x)$ has the same order as x.

8. Describe all automorphisms of the Klein four-group V.
   (*Hint: use the previous question!*)

9. Recall Exercise 7.1.6. Explain why $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^\times$.
   (*Hint: consider* $\phi_k(x) = kx$ *where* $\gcd(k,n) = 1$ *and map* $\psi : k \mapsto \phi_k$)

10. Let G be a group. Prove directly that $Z(G) \triangleleft G$, *without* using Theorem 7.27. That is:
    (a) Prove that $Z(G)$ is closed under the group operation and inverses.
    (b) Prove that $gZ(G) = Z(G)g$ for all $g \in G$.

11. Suppose $n \geq 3$ and that $\sigma \in Z(S_n)$.
    (a) By considering $\sigma(1\,2)\sigma^{-1}$, prove that $\{\sigma(1), \sigma(2)\} = \{1, 2\}$.
    (b) If $\sigma(1) = 2$, repeat the calculation with $\sigma(1\,3)\sigma^{-1}$ to obtain a contradiction.
    (c) Hence, or otherwise, deduce that $Z(S_n) = \{e\}$.

12. We identify the center of the general linear group.
    The $n \times n$ matrix $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & & 0 \\ 0 & 0 & 0 & & & 0 \\ \vdots & & & \ddots & \ddots & \\ 0 & 0 & 0 & & 0 & 1 \\ 0 & 0 & 0 & \cdots & & 0 \end{pmatrix}$ has a single one-dimensional eigenspace: $A\mathbf{e}_1 = \mathbf{0}$.
    (a) Let $B \in Z\big(\mathrm{GL}_n(\mathbb{R})\big)$. Use the fact that $AB = BA$ to prove that $B\mathbf{e}_1 = \lambda \mathbf{e}_1$ for some $\lambda \neq 0$.
    (b) Let $\mathbf{x} \in \mathbb{R}^n$ be non-zero and X an invertible matrix for which $X\mathbf{e}_1 = \mathbf{x}$ (e.g. put $\mathbf{x}$ in the 1^{st} column of X). Prove that $B\mathbf{x} = \lambda \mathbf{x}$.
    (c) Since the observation in part (b) holds for *any* $\mathbf{x} \in \mathbb{R}^n$, what can we conclude about B? What is the group $Z\big(\mathrm{GL}_n(\mathbb{R})\big)$?

13. (a) Prove that D_4 has center $Z(D_4) = \{e, \rho_2\}$, where ρ_2 is rotation by 180°.
    (b) State the cosets of $Z(D_4)$. What is the order of each? Determine whether ${}^{D_4}\!/_{Z(D_4)}$ is isomorphic to $\mathbb{Z}_4$ or to the Klein four-group V.
    (c) (Hard) Can you find a homomorphism $\phi : D_4 \to D_4$ whose kernel is $Z(D_4)$?
    (*Hint: draw a picture and think about doubling angles of rotation and reflection!*)

8 Group Actions

8.1 Group Actions, Fixed Sets and Isotropy Subgroups

In this final chapter, we revisit a central idea: groups are interesting and useful often because of how they *transform sets.* Recall how the symmetric group S_n was defined in terms of what its elements do to the set $\{1, \ldots, n\}$. This is an example of a general situation.

Definition 8.1. A group G *acts*[23] on a set X via a map $\cdot : G \times X \to X$ if,

(a) $\forall x \in X,\ e \cdot x = x$, and,

(b) $\forall x \in X,\ g, h \in G,\ g \cdot (h \cdot x) = (gh) \cdot x$.

Part (b) says $g \mapsto g\cdot$ is a homomorphism of *binary structures* (the functions $X \to X$ needn't form a group).

Examples 8.2. 1. The symmetric S_n group acts on $X = \{1, 2, \ldots, n\}$. As a sanity check:

(a) $e(x) = x$ for all $x \in \{1, \ldots, n\}$.

(b) $\sigma\big(\tau(x)\big) = (\sigma\tau)(x)$ is composition of functions!

2. Any group G acts on itself by left multiplication. This is essentially Cayley's Theorem (5.8). It also acts on itself by conjugation ($c_g \circ c_h = c_{gh}$ is Theorem 7.24).

3. If X is the set of orientations of a regular n-gon such that one vertex is at $(1, 0)$ and the center is at $(0, 0)$, then D_n acts on X by rotations and reflections. Note that X has cardinality $2n$.

4. Matrix groups act on vector spaces by matrix multiplication. For example the orthogonal group $\mathrm{O}_2(\mathbb{R})$ can be seen to transform vectors via rotations and reflections.

$$\mathrm{O}_2(\mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2 : (A, \mathbf{v}) \mapsto A\mathbf{v}$$

5. A group can act on many different sets. Here are three further actions of the orthogonal group:

i. $\mathrm{O}_2(\mathbb{R})$ acts on the set $X = \{1, -1\}$ via $A \cdot x := (\det A)x$.

ii. $\mathrm{O}_2(\mathbb{R})$ acts on the set $X = \mathbb{R}^3$ via $A \cdot \mathbf{v} := A(v_1\mathbf{i} + v_2\mathbf{j}) + v_3\mathbf{k}$.

iii. $\mathrm{O}_2(\mathbb{R})$ acts on the unit circle $X = S^1 \subseteq \mathbb{R}^2$ via matrix multiplication $A \cdot \mathbf{v} := A\mathbf{v}$.

We often use an action to visualize a group; in this context, some actions are better than others. Consider the three actions of $\mathrm{O}_2(\mathbb{R})$ in part 5 above:

i. The set X is very small. Many matrices act in exactly the same way so the action is an unhelpful means of visualizing the group.

ii. The set X feels too large. The action leaves any vertical vector untouched.

iii. The circle $X = S^1$ is large enough so that the action of distinct matrices can be distinguished without being inefficiently large.[24]

[23] This is really a *left* action. There is an analogous definition of a *right action.* In this course, all actions will be left.

[24] A *Goldilocks* action, perhaps?

These notions can be formalized.

Definition 8.3. Let $G \times X \to X$ be an action.

1. The *fixed set* of $g \in G$ is the set

$$\mathrm{Fix}(g) := \{x \in X : g \cdot x = x\} \qquad \text{(also written } X_g\text{, though we won't do this)}$$

2. The *isotropy subgroup* or *stabilizer* of $x \in X$ is the set

$$\mathrm{Stab}(x) := \{g \in G : g \cdot x = x\} \qquad \text{(also written } G_x\text{)}$$

3. The action is *faithful* if the only element of G which fixes everything is the identity. This can be stated in two equivalent ways:

(a) $\mathrm{Fix}(g) = X \iff g = e$ (b) $\bigcap_{x \in X} \mathrm{Stab}(x) = \{e\}$

4. The action is *transitive* if any element of X may be transformed to any other:

$$\forall x, y \in X,\ \exists g \in G \text{ such that } y = g \cdot x$$

Examples (8.2 cont). 1. The action of S_n on $\{1, 2, \ldots, n\}$ is both faithful and transitive:

Faithful: if $\sigma(x) = x$ for all $x \in \{1, 2, \ldots, n\}$, then $\sigma = e$.
Transitive: if $x \neq y$, then the 2-cycle $(x\,y)$ maps $x \mapsto y$.

2. The action of a group on itself by left multiplication is both faithful and transitive. Conjugation is more complex: in most situations it is neither.

3. D_n acts faithfully and transitively on the orientations of the n-gon.

4. The action of $\mathrm{O}_2(\mathbb{R})$ on $\mathbb{R}^2$ is faithful but not transitive: for instance the zero vector cannot be transformed into any other vector so $\mathrm{Stab}(\mathbf{0}) = \mathrm{O}_2(\mathbb{R})$.

5. We leave these as exercises.

Lemma 8.4. *For each $x \in X$, the stabilizer $\mathrm{Stab}(x)$ is indeed a subgroup of G.*

Proof. $\mathrm{Stab}(x)$ is a non-empty subset of G since $e \in \mathrm{Stab}(x)$. It sufficient to show that it is closed under multiplication and inverses. Let $g, h \in \mathrm{Stab}(x)$, then

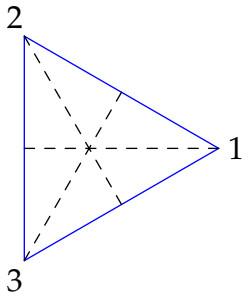
$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x \implies gh \in \mathrm{Stab}(x)$$

Moreover

$$x = g \cdot x \implies g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$

■

Example 8.5. The dihedral group $D_3 = \{e, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ acts on the set X of vertices of an equilateral triangle.[25] The fixed sets and stabilizers for this action are as follows:



Element g	Fix(g)
e	$\{1,2,3\}$
ρ_1	$\emptyset$
ρ_2	$\emptyset$
μ_1	$\{1\}$
μ_2	$\{2\}$
μ_3	$\{3\}$

Vertex x	Stab(x)
1	$\{e, \mu_1\}$
2	$\{e, \mu_2\}$
3	$\{e, \mu_3\}$

D_3 also acts on the set of *edges* of the triangle $Y = \{\{1,2\},\{1,3\},\{2,3\}\}$. You needn't write all these out since, by the symmetry of the triangle, stabilizing an edge is equivalent to stabilizing its opposite vertex. Still, here is the data:

Element g	Fix(g)
e	$\{1,2,3\}$
ρ_1	$\emptyset$
ρ_2	$\emptyset$
μ_1	$\{\{2,3\}\}$
μ_2	$\{\{1,3\}\}$
μ_3	$\{\{1,2\}\}$

Edge $\{x,y\}$	Stab$(\{x,y\})$
$\{1,2\}$	$\{e, \mu_3\}$
$\{1,3\}$	$\{e, \mu_2\}$
$\{2,3\}$	$\{e, \mu_1\}$

Exercises 8.1. Key concepts:

(left) action Fix(g) Stab$(x) \leq G$ *faithful/transitive actions*

1. For part 5 of Example 8.2, determine whether each action is faithful and/or transitive.
2. Let $G = \langle \sigma \rangle \leq S_6$ where $\sigma = (1\,2\,3\,4\,5\,6)$. G acts on the set $X = \{1,2,3,4,5,6\}$ in a natural way.
   (a) State the fixed sets and stabilizers for this action.
   (b) Is the action of G faithful? Transitive?
3. Repeat the previous question when $\sigma = (1\,3)(2\,4\,6)$.
4. Mimic Example 8.5 for the actions of D_4 on $X = \{\text{vertices}\}$ and $Y = \{\text{edges}\}$ of the square. (*Use whatever notation you like; ρ, μ, δ or cycle notation*)
5. Suppose G acts on X.
   (a) Let $Y \subseteq X$ and define Stab $Y = \{g \in G : \forall y \in Y, g \cdot y = y\}$. Prove that Stab Y is a subgroup of G.
   (b) Let G act on itself by conjugation ($X = G$!). What is another name for the subgroup Stab G?
6. Suppose G has a left action on X. Prove that G acts faithfully on X if and only if no two distinct elements of G have the same action on every element.

[25] Recall that ρ_1 rotates 120° counter-clockwise, that $\rho_2 = \rho_1^2$ and that μ_i reflects across the altitude through vertex i.

8.2 Orbits & Burnside's Formula

We first encountered orbits in the context of the symmetric groups S_n. The same idea applies to any action.

Definition 8.6. Let $G \times X \to X$ be an action. The *orbit* of $x \in X$ under G is the set of elements into which x may be transformed:

$$Gx = \{g \cdot x : g \in G\} \subseteq X$$

Examples 8.7. 1. If $X = \{1, 2, \dots n\}$ and $G = \langle \sigma \rangle \leq S_n$, then

$$Gx = \{\sigma^k(x) : k \in \mathbb{Z}\} = \text{orb}_x(\sigma)$$

The definition of orbits therefore coincides with that seen earlier in the course.

2. A transitive *action*[26] has only one orbit.

3. If $O_2(\mathbb{R})$ acts on $\mathbb{R}^2$ by matrix multiplication, then the orbits are circles centered at the origin!

Lemma 8.8. *The orbits of an action partition X.*

Since this is almost identical to the corresponding result for orbits in S_n (Theorem 5.11), we leave the proof as an exercise.

Our next result is analogous to Lemma 7.5, where we counted the number of (left) cosets of $\ker \phi$.

Lemma 8.9. *The cardinality of the orbit Gx is the index of the isotropy subgroup* $\text{Stab}(x)$*:*

$$|Gx| = \big(G : \text{Stab}(x)\big)$$

Proof. Observe that

$$g \cdot x = h \cdot x \iff h^{-1}g \cdot x = x \iff h^{-1}g \in \text{Stab}(x) \iff g\,\text{Stab}(x) = h\,\text{Stab}(x)$$

The contrapositive says that distinct elements of the orbit Gx correspond to distinct left cosets. ∎

Example 8.10. Let $\sigma = (14)(273) \in S_7$. Consider $X = \{1, 2, 3, 4, 5, 6, 7\}$ under the action of the cyclic group $G = \langle \sigma \rangle$. The orbits are precisely the disjoint cycles: $\{1, 4\}$, $\{2, 3, 7\}$, $\{5\}$, $\{6\}$. Observe that G has six elements:

$$e, \quad \sigma = (14)(273), \quad \sigma^2 = (237), \quad \sigma^3 = (14), \quad \sigma^4 = (273), \quad \sigma^5 = (14)(237)$$

The Lemma is easily verifiable: for instance if $x = 3$,

$$\text{Stab}(x) = \{\tau \in G : \tau(3) = 3\} = \{\sigma^k : \sigma^k(3) = 3\} = \{e, \sigma^3\}$$
$$\implies (G : \text{Stab}(x)) = \frac{6}{2} = 3 = |\{2, 3, 7\}| = |Gx|$$

[26] Unhelpfully, we now have two meanings of *transitive*; one for equivalence relations and one for actions.

It is often useful to count the *number* of orbits of an action. For *finite* actions, this turns out to be possible in two different ways.

Theorem 8.11 (Burnside's formula). *Let G be a finite group acting on a finite set X. Then the number of orbits in X under G satisfies*

$$\#\text{ orbits} = \frac{1}{|G|}\sum_{x\in X}|\text{Stab}(x)| = \frac{1}{|G|}\sum_{g\in G}|\text{Fix}(g)|$$

Proof. By Lemma 8.9, It follows that

$$\frac{1}{|G|}\sum_{x\in X}|\text{Stab}(x)| = \sum_{x\in X}\frac{|\text{Stab}(x)|}{|G|} = \sum_{x\in X}\frac{1}{(G:\text{Stab}(x))} = \sum_{x\in X}\frac{1}{|Gx|}. \qquad (*)$$

Consider a fixed orbit Gy. Since $|Gx| = |Gy|$ for each $x \in Gy$, we see that

$$\sum_{x\in Gy}\frac{1}{|Gx|} = \frac{|Gy|}{|Gy|} = 1$$

The sum $(*)$ therefore counts 1 for each distinct orbit in X and therefore returns the number of orbits. For the second equality, observe that

$$S = \{(g,x) \in G\times X : g\cdot x = x\}$$

has cardinality

$$|S| = \sum_{x\in X}|\text{Stab}(x)| = \sum_{g\in G}|\text{Fix}(g)|$$

■

Example (8.10 cont). When $G = \langle\sigma\rangle = \langle(1\,4)(2\,7\,3)\rangle$ acts on $X = \{1,2,3,4,5,6,7\}$, the stabilizers and fixed sets are as follows:

$x \in X$	$\text{Stab}(x)$
1	$\{e,\sigma^2,\sigma^4\}$
2	$\{e,\sigma^3\}$
3	$\{e,\sigma^3\}$
4	$\{e,\sigma^2,\sigma^4\}$
5	$G = \{e,\sigma,\sigma^2,\sigma^3,\sigma^4,\sigma^5\}$
6	G
7	$\{e,\sigma^3\}$

$g \in G$	$\text{Fix}(g)$
e	$X = \{1,2,3,4,5,6,7\}$
σ	$\{5,6\}$
σ^2	$\{1,4,5,6\}$
σ^3	$\{2,3,5,6,7\}$
σ^4	$\{1,4,5,6\}$
σ^5	$\{5,6\}$

Burnside's formula just sums the number of elements in all of the subsets in the right column of each table:

$$\begin{aligned} 4 = \#\text{ orbits} &= \frac{1}{|G|}\sum_{x\in X}|\text{Stab}(x)| = \frac{1}{6}(3+2+2+3+6+6+2) \\ &= \frac{1}{|G|}\sum_{g\in G}|\text{Fix}(g)| = \frac{1}{6}(7+2+4+5+4+2) \end{aligned}$$

One reason to count the number of orbits of an action is that we often want to consider objects as equivalent if they differ by the action of some simple group.

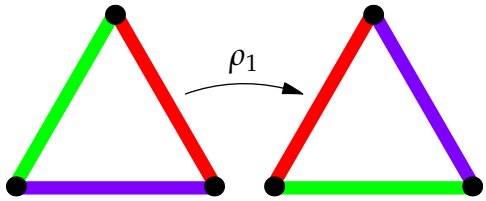
Example 8.12. A child's toy consists of a wooden equilateral triangle where the edges are to be painted using any choice of colors from the rainbow. How many distinct toys could we create?

There are two problems: we need to describe the variety of possible toys, and we need to know what *distinct* means!

We use group actions to address both problems:

- A toy may be considered as a subset of $X = \{\text{painted triangles}\} = \{\text{ordered color triples}\}$. Since there are 7 choices for the color of each edge, we see that $|X| = 7^3 = 343$ is a large set!
- Two toys are equivalent if they differ by a rotation in 3-dimensions. This amount to the natural action of D_3 on X: for instance

$$\rho_1 \cdot (\text{red,green,violet}) = (\text{violet,red,green})$$



The number of orbits is the number of distinct toys, which we may compute using Burnside. Since it would be time consuming to compute the stabilizer of each element of X, we use the fixed set approach.

- Identity e: Plainly $\text{Fix}(e) = X$, since e leaves every coloring unchanged.
- Rotations ρ_1, ρ_2: If a color-scheme is fixed by ρ_j, then all pairs of adjacent edges must be the same color. The only color-schemes fixed by ρ_j are those where all sides have the same color, whence $|\text{Fix}(\rho_i)| = 7$.
- Reflections μ_1, μ_2, μ_3: Since μ_j swaps two edges, anything in its fixed set must have these edges the same. We have 7 choices for the color of the switched edges, and an independent choice of 7 colors for the other edge, whence $\left|\text{Fix}(\mu_j)\right| = 7^2 = 49$.

The number of distinct toys is therefore

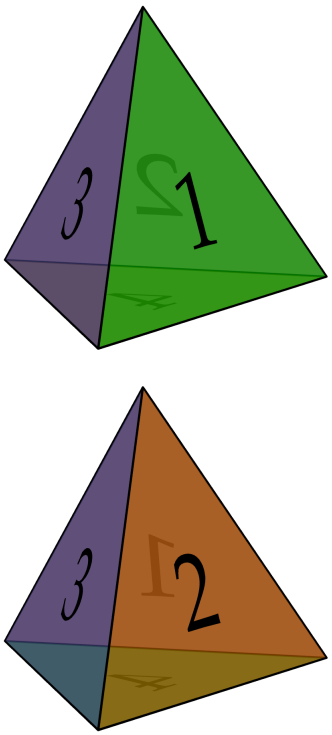
$$\begin{aligned} \#\text{ orbits} &= \frac{1}{|D_3|}\sum_{\sigma\in D_3}|\text{Fix}(\sigma)| = \frac{1}{6}(7^3+7+7+7^2+7^2+7^2) \\ &= \frac{7}{6}(49+1+1+7+7+7) = 84 \end{aligned}$$

The question was a little tricky because we are allowed multiple sides to have the same color. A simpler version would restrict to the situation where all sides had to be different colors. In this case D_3 acts on a set of color schemes with cardinality $|Y| = 7\cdot 6\cdot 5 = 210$. Moreover, only the identity element has a non-empty fixed set; in this situation the number of distinct toys would be

$$\#\text{ orbits} = \frac{1}{|D_3|}\sum_{\sigma\in D_3}|\text{Fix}(g)| = \frac{1}{6}(210+0+\cdots+0) = \frac{210}{6} = 35$$

Of course you could answer these questions by pure combinatorics without any resort to group theory!

Dice-rolling for Geeks!



Games like Dungeons & Dragons make use of several differently shaped dice: rather than simply using the standard 6-sided cubic die, situations might require rolling, say, a 4-sided tetrahedral die or a 20-sided icosahedral die.

Since dice are designed for rolling, we consider two dice to be the same if one can be rotated into the other. Play with the two tetrahedral dice on the right; you should be convinced that you cannot rotate one to make the other so these dice are distinct.

It is not difficult to see that, up to rotations, these are the *only* tetrahedral dice just by counting!

- Place face 4 on the table.
- When looking from above, the remaining faces are numbered 1, 2, 3 either clockwise or counter-clockwise.

For larger dice, this approach is not practical! However, with a little thinking about symmetry groups, Burnside's formula will ride to the rescue.

Suppose a regular polyhedron has f faces, each with n sides.

- The faces may be labelled 1 thorough f in $f!$ distinct ways: the set of distinct labellings is X.
- We may rotate the polyhedron so that any face is mapped to any other, *in any orientation.* It follows that the rotation group G has fn elements.
- Each non-identity element of the rotation group moves at least one face, whence

$$|\mathrm{Fix}(g)| = \begin{cases} X & \text{if } g = e \\ \varnothing & \text{if } g \neq e \end{cases}$$

- The number of distinct dice for a regular polyhedron is therefore

$$\#\text{ orbits} = \frac{1}{|G|}\,|\mathrm{Fix}(e)| = \frac{|X|}{|G|} = \frac{f!}{fn} = \frac{(f-1)!}{n}$$

We don't need to know what the rotation group is, only its *order*. For completeness, here are all the possibilities for the regular platonic solids.

Polyhedron	f	n	Rotation Group	# distinct dice
Tetrahedron	4	3	A_4	2
Cube	6	4	S_4	30
Octahedron	8	3	S_4	1,680
Dodecahedron	12	5	A_5	7,983,360
Icosahedron	20	3	A_5	40,548,366,802,944,000

Subgroups of Prime Order & the Class Equation

We finish with a taste of where group theory traditionally goes next.

Suppose G acts on a finite set X, that $x_1 \dots, x_r$ are representatives of the distinct orbits and that $x_1, \dots, x_s$ enumerate the 1-element orbits ($\text{Stab}(x_j) = G \iff j \leq s$). Then, by counting elements,

$$|X| = s + \sum_{j=s+1}^{r} |Gx_j| = s + \sum_{j=s+1}^{r} \big(G : \text{Stab}(x_j)\big)$$

When G acts on itself by conjugation, the 1-element orbits together comprise the center of G and we obtain the *class equation*:

$$|G| = |Z(G)| + \sum_{j=s+1}^{r} \big(G : \text{Stab}(x_j)\big)$$

Example 8.13. Since the conjugacy classes in S_4 are the cycle types, the class equation reads

$$24 = |\{e\}| + |\text{2-cycles}| + |\text{3-cycles}| + |\text{4-cycles}| + |\text{2,2-cycles}| = 1 + 6 + 8 + 6 + 3$$

Here is an example of how the class equation may be applied.

Lemma 8.14. *Suppose G is a non-abelian group whose order is divisible by a prime p. Then G has a* proper *subgroup whose order is divisible by p.*

Proof. Since G is non-abelian, $Z(G)$ is a proper subgroup. Let x be any element *not* in the center. Then

$$2 \leq |Gx| = \frac{|G|}{|\text{Stab}(x)|} \implies \text{Stab}(x) \text{ is a proper subgroup of } G$$

If p divides $|\text{Stab}(x)|$, then we're done. If not, then p divides $|Gx| = \big(G : \text{Stab}(x)\big)$. If this holds for all non-trivial orbits, the class equation says that $|Z(G)|$ is divisible by p. ∎

Theorem 8.15 (Cauchy). *If a prime p divides $|G|$, then G contains a subgroup/element of order p.*

It might feel as if we've done this already; Exercise 4.13 covers abelian groups, but this depends on the fundamental theorem, which first requires Cauchy for abelian groups!

Proof.

1. A proof for when G is abelian is in the exercises.
2. If G is non-abelian, apply the Lemma. If the resulting subgroup is abelian, part 1 finishes things off. Otherwise repeat. If we never reach an abelian subgroup, then we have an infinite sequence of proper subgroups and thus a decreasing sequence of positive integers; contradiction.

∎

Cauchy's Theorem may be extended to prove that if p^k divides G, then G has a subgroup of order p^k. This is the beginning of the Sylow theory of p-subgroups which has applications to group classification and the existence of sequences of normal subgroups.

[26] The two are equivalent: if y has order p, then $\langle y \rangle$ is a subgroup of order p. If $H \leq G$ has order p, then $H \cong \mathbb{Z}_p$ is cyclic.

Exercises 8.2. Key concepts:

Orbits of G partition X *Cardinality of orbit* $|Gx| = (G : \mathrm{Stab}(x))$ *divides* $|G|$
Burnside's formula for counting number of orbits

1. Determine the orbits of $G = \langle \sigma \rangle$ on $X = \{1, 2, 3, 4, 5, 6\}$ for each of Exercises 8.1.2 and 3. In both cases verify Burnside's formula.
2. Revisit Example 8.12. How may distinct toys may be created if:
   (a) A maximum of two colors can be used?
   (b) Exactly two colors must be used?
3. Prove Lemma 8.8: the orbits of a left action partition X.
4. A 10-sided die is shaped so that all faces are congruent *kites*: five faces are arranged around the north pole and five around the south, so that each face is adjacent to four others.
   (a) Argue that the group of rotational symmetries of such a die has ten elements.
   (*In fact it is non-abelian and is therefore isomorphic to* D_5).
   (b) Use Burnside's formula to determine how many distinct 10-sided dice may be produced.
5. A soccer ball is constructed from 20 regular hexagons and 12 regular pentagons as in the picture.
   Suppose the 20 hexagonal patches are all to have different colors, as are the 12 pentagonal patches. How many distinct balls may be produced?

6. The faces of a cuboid measuring $1 \times 1 \times 2$ in is to be painted using (at most) two colors. Up to equivalence by rotations, how many ways can this be done?
7. Repeat the previous question for a regular tetrahedron.
8. Suppose G is a finite group with order p^n where p is a prime. If $x \in G$ lies in a conjugacy class with at least 2 elements, prove that the order of $\mathrm{Stab}(x)$ divides p^{n-1}. Now use the class equation to prove that p divides the order of the center $Z(G)$.
9. We prove the abelian part of Cauchy's Theorem by induction on the order of G.
   (a) Explain why the base case $|G| = 2$ is true.
   (b) Suppose p divides $|G| \geq 3$ and assume the result holds for all abelian groups of order $< |G|$.
   - Choose any $x \neq e$; denote its order by $m = |\langle x \rangle|$ (necessarily $m \geq 2$).
   - Choose a prime q dividing m, define $y := x^{m/q}$ and let $H := \langle y \rangle$.

   Why are we done if $q = p$?
   (c) If $q \neq p$, explain why there exists a coset $zH \in {}^{G}/_{H}$ of order p.
   (d) Prove that z^q has order p in G.