CHAPTER 5

Groups

Semigroups are very common in mathematics, but they have so little structure—just an associative binary operator—that it is difficult to prove wide ranging theorems about them. If we instead look at semigroups with identity and inverses we are able to prove a wealth of results.

5.1. Definition of a Group

5.1.1 Definition A *group* G is a semigroup with identity in which every element has an inverse.

If we unravel this definition, a group G is a non-empty set, together with binary operation $*$ on G satisfying

Associativity	$a*(b*c)=(a*b)*c$ for every $a,b,c\in G$
Identity	There exists $1\in G$ with $1a=a=a1$ for every $x\in G$
Inverses	For every $a\in G$ there exists $b\in G$ with $ab=1=ba$.

Groups are essential in modern mathematics. They occur in crystallography, in particle physics, in solving polynomial equations and everywhere in algebra. One of the great successes of twentieth century mathematics was to classify all the finite “simple” groups (see below for definition); this took decades.

5.1.2 Example

- ★ The integers, rationals and real numbers all form groups under $+$. $\mathbb{Z}/n\mathbb{Z}$ is another example of a group under addition.
- ★ The non-zero rationals and the non-zero reals both form groups under multiplication. The non-zero integers $\mathbb{Z}\setminus\{0\}$ do not form a group under multiplication, because most elements in $\mathbb{Z}\setminus\{0\}$ do not have inverses in $\mathbb{Z}\setminus\{0\}$. For example the inverse of 2 is 1/2 which is not an integer.
- ★ The natural numbers do not form a group under addition or multiplication, since elements do not have additive or multiplicative inverses in $\mathbb{N}$.
- ★ The set G consisting of a single element e is a group. Here multiplication is defined by $e\cdot e=e$. This is (trivially) a binary operation on G. It is clearly associative and commutative (*any* product is e). Also e is the identity, and e is its own inverse. This group is called the *trivial group* . Often e is denoted by 0, and then G is also denoted 0 (instead of $\{0\}$) and called the *zero group.* Sometimes e and G are both denoted by 1.
- ★ The set $\mathscr{F}$ of functions $\mathbb{R}\to\mathbb{R}$ forms a group under addition (see example 4.1.3). $\mathscr{F}$ does not form a group under multiplication since any function that is 0 at any point will not be invertible.
- ★ $M_n(\mathbb{R})$ is a group under $+$. It is not a group under multiplication, because some matrices are not invertible (those with determinant 0). However the subset of invertible matrices does form a group, denoted $GL_n(\mathbb{R})$. “GL” stands for “General Linear”.

  Proof If A and B are invertible, so is AB since $(AB)^{-1}=B^{-1}A^{-1}$. Thus matrix multiplication is a binary operation on $GL_n(\mathbb{R})$. Matrix multiplication is associative, so $(GL_n(\mathbb{R}),\cdot)$ is a semigroup, with identity I. Finally every element of $GL_n(\mathbb{R})$ is invertible, by definition.
- ★ Let A be a set. The set of bijections from $A\to A$ forms a group under composition.

Proof The composition of two bijections is a bijection. Composition is associative by theorem 3.2.13, the identity function 1_A is the identity, and every bijection is invertible by theorem 3.4.5.

The last two examples are special cases of the following observation.

5.1.3 Theorem Let S be a semigroup with identity, and let G be the subset of S consisting of all invertible elements. Then G is a group.

Proof $1 \in G$ so G is non-empty, and indeed contains the identity. If a and b are invertible so is ab, by theorem 4.3.5, so G is closed under multiplication. Multiplication in S is associative, so it is still associative in the subset G. Every element of G is invertible by definition. □

Another example along these lines.

5.1.4 Example We have seen that $\mathbb{Z}/n\mathbb{Z}$ is a group under addition. It is not a group under multiplication, since not every element is invertible (0 is not).

Consider the semigroup $\mathbb{Z}/n\mathbb{Z}$ under multiplication. The subset of invertible elements, denoted $(\mathbb{Z}/n\mathbb{Z})^\times$ forms a group.

For example, consider $\mathbb{Z}/12\mathbb{Z}$. The invertible elements are $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$. These form a group under multiplication.

5.1.5 Definition A group G is *finite* if G is a finite set. If G is finite then the number of elements in G is called the *order* of G, denoted $|G|$.

5.1.6 Example $\mathbb{Z}/n\mathbb{Z}$ (under addition) is a group of order n. $(\mathbb{Z}/n\mathbb{Z})^\times$ (under multiplication) is a group of order $\varphi(n)$.

5.1.7 Example Let n be a positive integer. Let $\zeta = e^{2\pi i/n}$. Let G be the following set of complex numbers: $G = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$. Then G is a finite group (of order n) under multiplication.

Proof Obviously G is finite. We first show that multiplication is a binary operation on G; that is, if we multiply two elements of G we stay inside G. Intuitively this is clear because $\zeta^n = 1$, $\zeta^{n+1} = \zeta \cdot \zeta^n = \zeta$, $\zeta^{n+2} = \zeta^2$ and so on.

Claim: Every positive power of ζ is actually in G, so G is closed under multiplication.

Proof Given $m \in \mathbb{N}$, write $m = qn + r$ with $0 \leq r < n$ using the division algorithm. Then $\zeta^m = \zeta^{qn+r} = (\zeta^n)^q \cdot \zeta^r = 1 \cdot \zeta^r = \zeta^r \in G$ since $0 \leq r < n$.

Multiplication of complex numbers is associative, so G is a semigroup. $1 \in G$ is the identity. If $a = \zeta^k \in G$ let $b = \zeta^{n-k} \in G$. Then $ab = ba = \zeta^n = 1$, so b is the inverse of a. Thus G is a group. □

Note the order of proof: first we must show that the binary operation is well defined on G. (Otherwise it makes no sense to talk about associativity, inverses etc). Next we show associativity. Then we prove there is an identity—otherwise there is no notion of inverse. Finally we show that inverses exist.

Geometrically, the points of G form the vertices of a regular n-gon in the complex plane.

5.1.8 Definition The group of nth roots of 1 is denoted μ_n. This is a finite group with n elements.

Given two groups G and H there is an easy way to form a new group from them called the product.

5.1.9 Definition Let $(G, *)$ and $(H, \circ)$ be groups. The[1] *(direct) product* of G and H is the set $G \times H$ with binary operation $\odot$ defined by

$$(g_1, h_1) \odot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$$

[1] Sometimes called the external direct product.

Note that if G has m elements and H has n elements then $G \times H$ has mn elements:

$$|G \times H| = |G| \cdot |H|.$$

5.1.10 Theorem $G \times H$ is a group.

Proof If $(g_1, h_1), (g_2, h_2) \in G \times H$ then $(g_1 * g_2, h_1 \circ h_2) \in G \times H$, so $\odot$ is a binary operation on $G \times H$.

Associativity: If $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$ then

$$\begin{aligned}
&\Big((g_1, h_1) \odot (g_2, h_2)\Big) \odot (g_3, h_3) \\
&\qquad = (g_1 * g_2, h_1 \circ h_2) \odot (g_3, h_3) && \text{Def } \odot \\
&\qquad = \Big((g_1 * g_2) * g_3, (h_1 \circ h_2) \circ h_3\Big) && \text{Def}\odot \\
&\qquad = (g_1 * (g_2 * g_3), h_1 \circ (h_2 \circ h_3)) && *, \circ \text{ associative} \\
&\qquad = (g_1, h_1) \odot (g_2 * g_3, h_2 \circ h_3) && \text{Def } \odot \\
&\qquad = (g_1, h_1) \odot \Big((g_2, h_2) \odot (g_3, h_3)\Big) && \text{Def } \odot
\end{aligned}$$

so $\odot$ is associative.

Identity: If $(g, h) \in G \times H$ then

$$\begin{aligned}
(g, h) \odot (1_G, 1_H) &= (g * 1_G,\ h \circ 1_H) && \text{Def } \odot \\
&= (g, h) && \text{Def } 1_G,\ 1_H \\
&= (1_G * g,\ 1_H \circ h) && \text{Def } 1_G,\ 1_H \\
&= (1_G, 1_H) \odot (g, h) && \text{Def } \odot
\end{aligned}$$

Thus $(1_G, 1_H)$ is the identity in $G \times H$.

Inverses: If $(g, h) \in G \times H$ then

$$\begin{aligned}
(g, h) \odot (g^{-1}, h^{-1}) &= (g * g^{-1},\ h \circ h^{-1}) && \text{Def } \odot \\
&= (1_G, 1_H) && \text{Def } g^{-1},\ h^{-1} \\
&= (g^{-1} * g,\ h^{-1} \circ h) && \text{Def } g^{-1},\ h^{-1} \\
&= (g^{-1},\ h^{-1}) \odot (g, h) && \text{Def } \odot
\end{aligned}$$

So the inverse of (g, h) is (g^{-1}, h^{-1}). □

We can iterate this process to form $G_1 \times G_2 \times \cdots \times G_n$. This consists of all n-tuples $(g_1, \ldots, g_n)$ with $g_i \in G_i$ and multiplication in the ith position given by multiplication in G_i.

47 Exercise For each of the following, prove that G is a group under operation $*$, or explain why it is not:

(a) $G = \mathbb{Q}$, $a * b = a + b + 3$.
(b) $G = \mathbb{Q} \setminus \{0\}$, $a * b = ab/3$.
(c) $G = \mathbb{R} \setminus \{0\}$, $a * b = |a|b$.
(d) $G = \mathbb{Q} \setminus \{-1\}$, $a * b = a + b + ab$.
(e) $G = \mathbb{R} \setminus \{0\}$ with operation $*$ defined by

$$a * b = \begin{cases} ab, & \text{if } a > 0 \\ a/b, & \text{if } a < 0. \end{cases}$$

(f) Let $G = \mathbb{R} \setminus \{0\} \times \mathbb{R}$ with operation defined by $(a, b) * (c, d) = (ac, bc + d)$.
(g) Let

$$G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

with operation matrix multiplication.

(h) Let $A = \mathbb{R}\backslash\{0,1\}$. Let G consist of the following six functions from A to A: $f_1(x) = 1/(1-x)$, $f_2(x) = (x-1)/x$, $f_3(x) = 1/x$, $f_4(x) = x$, $f_5(x) = 1-x$, $f_6(x) = x/(x-1)$. Is G a group?

48 Exercise Suppose G is a group under $*$. Define a new operation $\circ$ by $a \circ b = b * a$. Show that G is a group under $\circ$.

49 Exercise Let $(G, *)$ be a semigroup. Show that G is a group iff for each a, $b \in G$ the equations $a * x = b$ and $y * a = b$ have unique solutions x, $y \in G$.

5.2. Abelian Groups

5.2.1 Definition A group G is *abelian* or *commutative* if its operation is commutative, that is if

$$xy = yx \qquad \text{for all } x, y \in G.$$

5.2.2 Example

- ★ $\mathbb{Z}$ and $\mathbb{R}$ are abelian groups under addition. $\mathbb{R} \setminus \{0\}$ is an abelian group under multiplication.
- ★ The group μ_n of complex nth roots of 1 is abelian. See example 5.1.7.
- ★ $\mathbb{Z}/n\mathbb{Z}$ is an abelian group with respect to addition.
- ★ The group of invertible $n \times n$ real matrices $GL_n(\mathbb{R})$ is not abelian, since $AB \neq BA$ in general for matrices.
- ★ Let V be any vector space. Then V is an abelian group under addition. Indeed, a vector space is an abelian group together with scalar multiplication.
- ★ $f \circ g \neq g \circ f$ for functions (see example 3.6.4), so the group of bijections from $\mathbb{R} \to \mathbb{R}$ (or from A to A more generally) is not abelian.

In an abelian group we are free to rearrange the order of products in any way we please, by theorem 3.6.6. Thus in an abelian group

$$(ab)^n = a^n b^n$$

which is false in a general group.

50 Exercise Let G be a group.

(a) Prove that G is abelian iff $aba^{-1}b^{-1} = 1$ for every a, $b \in G$. The element $aba^{-1}b^{-1}$ is called the *commutator* of a and b, denoted $[a, b]$.

(b) Prove that G is abelian iff $(ab)^2 = a^2b^2$.

(c) Prove that if $a^2 = 1$ for every element $a \in G$ then G is abelian.

51 Exercise Suppose G is a finite group with an even number of elements. Prove that G contains an element $a \neq 1$ with $a^2 = 1$. Hint: Show that $a^2 = 1$ iff $a = a^{-1}$.

Now we come to a confusing convention.

5.2.3 Convention If a group G is abelian then we often denote the binary operation by $+$ (unless it has a well established other name). We then denote the identity by 0. We denote the inverse of x by $-x$ and denote $x + x + \cdots + x$ by nx. This is called *additive notation* .

If the group is not abelian [2] we write it *multiplicatively* denoting the binary operation by juxtaposition or $\cdot$, the identity by 1, $xx\cdots x$ by x^n and the inverse of x by x^{-1}. See Convention 4.1.4.

[2] Or not necessarily abelian

	Additive Notation	Multiplicative Notation
Group Operation	$a+b$	ab or $a \cdot b$
Repeated Operations	na	a^n
Identity	0	1
Inverses	$-a$	a^{-1}
Left cosets (see later)	$a+H$	aH

5.3. Basic Properties of Groups

5.3.1 Theorem Let G be a group.

(a) Left and right cancellation: if $ab = ac$ then $b = c$. If $ba = ca$ then $b = c$.
(b) If $a^2 = a$ then $a = 1$.
(c) For each $a \in G$, $\left(a^{-1}\right)^{-1} = a$.
(d) $(ab)^{-1} = b^{-1}a^{-1}$.

Proof

(a) If $ab = ac$ then multiplying by a^{-1} on the left, $a^{-1}(ab) = a^{-1}(ac)$ so $(a^{-1}a)b = (a^{-1}a)c$ so $1b = 1c$ so $b = c$. Similarly for right cancellation.

(b) Special case of (a): $aa = a = a1$ so by left cancellation, $a = 1$.

(c), (d) We proved this in theorem 4.3.5. □

Note that $(ab)(a^{-1}b^{-1})$ does not simplify further. For example, suppose you are given driving directions to (a) turn left then (b) turn right. To undo these directions (to find your way back to the start), first undo the right turn, and then undo the left turn. That is: $(ab)^{-1} = b^{-1}a^{-1}$.

5.3.2 Definition Suppose $G = \{g_1, \ldots, g_n\}$ is a finite group. We can list all possible products g_ig_j in an $n \times n$ table. This table is called the *Cayley table* or *group table* of G.

5.3.3 Example Give the Cayley table for the additive group $\mathbb{Z}/4\mathbb{Z}$.

Solution: In position (i, j) of the table the entry is $i + j \pmod 4$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

In this example, each row and column of the main part of table contains each of 0, 1, 2, 3 exactly once. This is true in general.

5.3.4 Theorem If G is a finite group, the Cayley table of G contains each element of G exactly once in each row and column.

Proof Fix $g_i \in G$ and consider the ith row of the Cayley table $g_ig_1, g_ig_2, \ldots g_ig_n$. By left cancellation[3] (theorem 5.3.1) these n elements will be distinct. (If $g_ig_j = g_ig_k$ then multiplying by g_i^{-1} on the left on each side, $g_j = g_k$.)

Thus $g_ig_1, \ldots, g_ig_n$ is a permutation of the elements of G, so each element of G occurs exactly once in each row. Similarly each element of G occurs exactly once in each column. □

Of course it is only possible to give the Cayley table of G if $|G|$ is small. Larger groups can be described using *generators* (see § 5.8).

[3] An elegant way to state this is: the map $G \to G$ sending x to g_ix is injective, hence is bijective by theorem 3.3.7.

52 Exercise Give the Cayley table for the groups μ_4 and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. How do they compare to the table for $\mathbb{Z}/4\mathbb{Z}$?

53 Exercise Suppose $G = \{a, b, c, d\}$ is a group. Suppose part of the Cayley table for G is as follows:

	a	b	c	d
a	a	b	c	d
b	b	a		
c	c		a	
d				

Complete the table. How does this table compare to the tables for $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

54 Exercise Define the *quaternion group* to consist of the 8 elements $\{\pm 1, \pm i, \pm j, \pm k\}$ with multiplication given by $i^2 = j^2 = k^2 = -1$, $(-1)^2 = 1$ and $ij = k$. Give the Cayley table for Q_8.

Hints: $-i = i^2 \cdot i = i \cdot i^2$ and similarly for j and k, so we can always move $-$ signs to the front. Now show $ik = -j$, $kj = -i$ and finally $ji = -k$ (square $ij = k$ to get this one).

5.4. Example: The Symmetric Groups

Let A be a set. We have seen (example 5.1.2) that the set of bijections $A \to A$ forms a group under composition. A special case is obtained by taking $A = \{1, 2, \dots, n\}$.

5.4.1 Definition Let S_n be the set of bijections $\{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ under composition. Then S_n forms a group, called the nth *symmetric group.* The elements of S_n are called *permutations* on n letters.

An element of S_n is a bijection $\sigma \colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. We can describe such a function by simply listing all the pairs $(a, \sigma(a))$ in a $2 \times n$ matrix:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

A bijection is an exact matching between elements, so the bottom row will contain each of $\{1, 2, \dots, n\}$, but in some permuted order.

How many elements are there in S_n? If $\sigma \in S_n$ there are n choices for $\sigma(1)$. There are $n-1$ choices for $\sigma(2)$ because $\sigma(1) \neq \sigma(2)$ (σ is injective). There are $n-2$ choices for $\sigma(3)$ etc. Altogether there are $n(n-1)(n-2) \cdots 2 \cdot 1 = n!$ choices.

5.4.2 Theorem S_n is a group with $n!$ elements.

5.4.3 Example Let $\sigma \colon \{1, 2, 3\} \to \{1, 2, 3\}$ be given by $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$. Then

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Similarly let

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Then $\sigma, \tau \in S_3$. The group operation is composition. For example $\sigma\tau$ maps 2 to $\sigma(\tau(2)) = \sigma(3) = 1$. Note that because function composition is written with the inner function to the right, if we write down $\sigma\tau$ as matrices, we find $\tau(1)$ in the right matrix and then find $\sigma(\tau(1))$ using the left matrix.

$$\overset{\sigma}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}} \overset{\tau}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}} \qquad \overset{\sigma\tau}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}.$$

Similarly

$$\overset{\tau}{\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}}\ \overset{\sigma}{\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}} \qquad \overset{\tau\sigma}{\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}}.$$

Note that S_3 is not abelian.

5.4.4 Example With further calculation one can check that $S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.

55 Exercise In S_3

(a) Show that $\sigma^2 \neq 1$ but $\sigma^3 = 1$ and $\tau^2 = 1$.
(b) Show that $\tau\sigma = \sigma^2\tau$.
(c) Hence show that $\tau\sigma^2 = \sigma\tau$.
(d) Conclude that $S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. (We already know that S_3 has 6 elements, so we just have to make sure that all of these are distinct.)

With further calculations we find the entire group table:

S_3	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
1	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	1	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	1	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	1	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	1	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	1

Note: To calculate this table we do not have to calculate 36 products. Instead we use the identities in the previous example. For example to calculate the product $(\sigma^2\tau)(\sigma\tau)$, use the fact that $\tau\sigma = \sigma^2\tau$: $(\sigma^2\tau)(\sigma\tau) = \sigma^2(\tau\sigma)\tau = \sigma^2(\sigma^2\tau)\tau = \sigma^4\tau^2 = \sigma \cdot \sigma^3 \cdot \tau^2 = \sigma$.

56 Exercise Describe the groups S_1 and S_2. Are they abelian? How do they compare to groups we have seen earlier?

5.5. Subgroups

Often we encounter a smaller group within a larger one. For example, the group $(\mathbb{Z}, +)$ is contained in the larger group $(\mathbb{R}, +)$.

Let G be a group. Suppose H is a non-empty subset of G. It is natural to consider whether or not H forms a group.

5.5.1 Definition Let G be a group and H a non-empty subset of G. We say that H is a *subgroup* of G if

(a) For every x, $y \in H$, $xy \in H$ (closure under multiplication),
(b) $1 \in H$,
(c) For every $z \in H$, $z^{-1} \in H$.

These properties imply that H is a group in its own right, under the group operation on G: (a) ensures that the group operation on H restricts to a binary operation on H. That is, when we multiply elements in H we stay in H, not just in G. Since the operation is associative on all of G, it will certainly be associative on H. (b) and (c) ensure that the identity and inverses are in H.

5.5.2 Example

★ $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$ and $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$.

★ $\mathbb{N}$ is not a subgroup of $(\mathbb{Z}, +)$. It is closed under the group operation $+$, but it lacks the identity 0 and inverses.

★ For any group G, G is a subgroup of G and the trivial group consisting only of the identity is a subgroup of G. *Proof* If $x, y \in \{1\}$ then $x = y = 1$ so $x \cdot y$, x^{-1} and 1 are all in $\{1\}$.

Warning: it is possible that $(G, *)$ is a group, $H \subseteq G$ and H is a group under some other binary operation, but not under $*$. In this case H is not said to be a subgroup of G.

5.5.3 Example $(\mathbb{R} \setminus \{0\}, \cdot)$ is not a subgroup of $(\mathbb{R}, +)$, even though both are groups. The group operation (multiplication) in $\mathbb{R} \setminus \{0\}$ is not the restriction of the operation (addition) on $\mathbb{R}$.

Also, $\mathbb{Z}/n\mathbb{Z}$ under $+$ is *not* a subgroup of the integers. $\mathbb{Z}/n\mathbb{Z}$ is a consists of congruence classes of integers, so is not a subset of $\mathbb{Z}$. And addition mod n is not the restriction of the usual operation on $\mathbb{Z}$.

5.5.4 Example Let $G = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. Let $H = \{0, 2\}$. Then H is a subgroup of G.

Proof H is non-empty. If x, $y \in H$ then $x + y = 0 + 0$ or $0 + 2$ or $2 + 0$ or $2 + 2 \equiv 0 \in H$, so H is closed under addition. And $-0 = 0$, $-2 \equiv 2$ so (c) holds also.

5.5.5 Example Let $G = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. Let $H = \{0, 3\}$. Then H is not a subgroup of G.

Proof $3 + 3 \equiv 2 \notin H$. So H is not closed under addition. □

We can combine the three subgroup properties into a single test:

5.5.6 Theorem Let G be a group and let H be a non-empty subset of G. Then H is a subgroup of G iff for every x, $y \in H$ we have $xy^{-1} \in H$.

Proof

$\Longrightarrow$ If H is a subgroup of G and x, $y \in H$ then $y^{-1} \in H$ by (c), and hence by (a), $xy^{-1} \in H$.

$\Longleftarrow$ Since H is non-empty, there exists some $x \in H$. Then $1 = xx^{-1} \in H$ by hypothesis. This proves (b) above. Now let $z \in H$ be arbitrary. Then $1z^{-1} \in H$ so $z^{-1} \in H$. This proves (c). Finally if x, $y \in H$ then by (c) (proved above) $x, y^{-1} \in H$ so $x(y^{-1})^{-1} \in H$ so $xy \in H$. This proves (a). □

5.5.7 Example Let $\mathscr{F}$ be the set of all functions $\mathbb{R} \to \mathbb{R}$ under addition (example 4.1.3). Let $\mathscr{D}$ be the set of differentiable functions $\mathbb{R} \to \mathbb{R}$. Then $\mathscr{D}$ is non-empty, and if f and g are differentiable, so is $f - g$. Hence $\mathscr{D}$ is a subgroup of $\mathscr{F}$.

57 Exercise Is $(\mathbb{Z}/n\mathbb{Z})^{\times}$ a subgroup of $\mathbb{Z}/n\mathbb{Z}$?

58 Exercise Find all subgroups of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Hint: there are five.

5.6. Example: Dihedral Groups

We give another important family of groups. One place that groups first arose is in geometry. Consider the unit square in the plane, with vertices at positions labelled 1, 2, 3, 4. It is natural to consider the rigid motions of the square that leave it in the same position. (We are not allowed to rip or twist the square, only move it around.) Such motions are called *symmetries* of the square. We can rotate the square through any multiple of $\pi/2$. Or we can flip the square about a vertical or horizontal or diagonal axis. We can keep track of these motions, by listing where the corners start and finish. In other words, we can think of the symmetries as described by functions $\{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$. These functions are bijections, because we can always undo a symmetry (rotate in the opposite direction etc).

For example, let σ be the rotation through $\pi/2$ (anticlockwise) symmetry. Then we can write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

This means that corner 1 goes to position previously occupied by corner 2, corner 2 goes to position 3 and so on.

If σ and τ are symmetries, then we can perform σ and then τ. The corner in the nth position will then go to position $\tau(\sigma(n))$. That is, we can compose symmetries.

5.6.1 Definition Let $n \geq 3$. The set of symmetries of the regular n-gon is denoted D_n.

5.6.2 Theorem D_n is a subgroup of S_n, $n \geq 3$.

Proof If we compose two symmetries (that is, perform one after the other), we still end with a symmetry. So D_n is closed under composition. The identity "do nothing" symmetry is in D_n. Finally if σ is a symmetry, then we can undo σ (rotate in the opposite direction etc), so $\sigma \in D_n \implies \sigma^{-1} \in D_n$. □

5.6.3 Example Consider the symmetries of the equilateral triangle. First we have the three rotations, by 0, $2\pi/3$ and $4\pi/3$. Let σ be rotation by $2\pi/3$. Then σ moves corners 1 to 2, 2 to 3 and 3 to 1. That is,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Then

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 1.$$

Let τ be a flip about an axis through the vertex 1:

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

We can also form $\sigma\tau$ and $\sigma^2\tau$:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

So D_3 contains these 6 elements. But these are all $3! = 6$ elements of S_3, so D_3 is equal to S_3.

5.6.4 Example Consider D_4. Let σ be rotation through $\pi/2$ and τ be the flip described below:

$$1, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$\sigma^3\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

There are another 16 elements of S_4, but none of them are in D_4. To see this, note that no symmetry can change the position of the vertices with respect to each other. Corner 2 must always end up between corners 1 and 3. For example, a bijection sending 1 to 1 and 2 to 3 is not a valid symmetry of the square.

In fact, a symmetry σ can map corner 1 to any position a, but then must map corner 2 to position $a + 1$ or $a - 1$, and then the position of all the remaining corners is fixed. So altogether there are 4 choices for $\sigma(1)$, but then only two remaining choices for $\sigma(2)$ and this fixes σ completely. Altogether there are 8 choices, and we have listed all 8 elements above.

In general this argument proves:

5.6.5 Theorem D_n has $2n$ elements. Indeed, $D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$. Geometrically σ is a rotation through angle $2\pi/n$ and τ is a flip about an axis through the centre of the n-gon.

Note: Because D_n has $2n$ elements, some authors denote it by D_{2n}. Thus some authors write D_8 for what we have called D_4 etc.

5.7. Order

5.7.1 Definition Let G be a group, $a \in G$. We say that a has *finite order* if $a^m = 1$ for some positive integer m. In this case, the *order* of a in G is the smallest such positive integer. If no such m exists we say that a has infinite order.

This generalizes the definition of order in the group $(\mathbb{Z}/n\mathbb{Z})^\times$, §2.9. There does not seem to be a uniform notation for the order of an element in a group. We shall soon see the rationale for using the same word for the order of an element and the order of a group.

Note that in an abelian group, a has order n if $a + \cdots + a = 0$ with n copies of a added together, and no smaller number of a's adds to 0.

5.7.2 Example

- ★ In any group the identity has order 1, and no other element has order 1.
- ★ In $(\mathbb{R} \setminus \{0\}, \cdot)$, -1 has order 2, 1 has order 1 and no other element has finite order. *Proof* If $x^m = 1$ then taking absolute values $|x|^m = 1$ so $x = \pm 1$.
- ★ In μ_n, $\zeta = e^{2\pi i/n}$ has order n.
- ★ In the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $(1,1)$ has order 6. *Proof* : Repeatedly adding $(1,1)$ we get $(1,1)$, $(2,2) = (0,2)$, $(1,3) = (1,0)$, $(2,1) = (0,1)$, $(1,2)$, $(2,3) = (0,0)$, so the first time we get to the identity $(0,0)$ is with 6 copies of $(1,1)$. %

Warning: If $a^n = 1$ it does not mean that a has order n. It does mean that the order of a is at most n, but it may be smaller. In fact, n must be a multiple of the actual order (see below).

5.7.3 Example $2^6 = 64 \equiv 1 \pmod 7$. This does not mean that 2 has order 6 in $(\mathbb{Z}/7\mathbb{Z})^\times$. In fact its order is 3, since $2^3 = 8 \equiv 1$ and clearly 2^2 and $2^1 \not\equiv 1$.

We have already seen the following in $(\mathbb{Z}/n\mathbb{Z})^\times$ (theorem 2.9.8).

5.7.4 Theorem Let G be a group, $a \in G$ and $m \in \mathbb{N}$. Then $a^m = 1$ iff m is a multiple of the order of a.

Proof Let the order of a be n.

$\Longrightarrow$ Suppose $a^m = 1$. Use the division algorithm to write $m = qn + r$ with $0 \le r < n$. Then

$$1 = a^m = a^{qn+r} = (a^n)^q \cdot a^r = 1^q a^r = a^r.$$

Since $r < n$, the definition of order implies that $r = 0$. Thus m divides n.

$\Longleftarrow$ If $m = qn$ then $a^m = (a^n)^q = 1^q = 1$. □

Notice that we are using the word "order" in two different ways: as the order of the group (the number of elements in the group), or the order of an element of the group. These notions are related.

5.7.5 Theorem In a finite group G of order n, every element has order at most n.

Proof Let $a \in G$. Consider the list $a^0 = 1, a, a^2, \ldots, a^n$. This contains $n+1$ elements of G, so two must coincide. Say $a^k = a^m$. Without loss of generality $m > k$. Cancelling (theorem 4.3.7) $a^{m-k} = 1$, so a has order at most $m - k \le n$.
qed

In fact we shall show that the order of any element must be a divisor of n. This will follow from Lagrange's theorem 5.12.1 below.

59 Exercise (a) Find the order of $(8, 4, 10)$ in $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. Justify your answer.

(b) Let

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} \\ -\frac{3}{2} & -\frac{1}{2} \end{pmatrix} \in GL_2(\mathbb{R}).$$

Find the orders of A and B.

(c) Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R}).$$

Show that A has order 3, B has order 4 but AB has infinite order.

60 Exercise Prove that in any group aba^{-1} has the same order as b.

61 Exercise Let G be an abelian group. Let $T = \{g \in G \mid ng = 0\}$. Show that T is a subgroup of G. Does the set of elements of order n form a subgroup of G? Explain.

5.8. Generators

We have seen several examples of groups now. A more general way to present a group is by giving *generators* . This is something like giving a basis for a vector space.

By analogy, suppose $\{v_1, \ldots, v_n\}$ is a basis for a vector space V. There are two ways to view this: first, V is the smallest vector space containing v_1, …, v_n. Alternatively, V is the set of all linear combinations $\alpha_1 v_1 + \cdots + \alpha_n v_n$.

To talk about the smallest group containing some elements we need the following theorem.

5.8.1 Theorem Let G be a group. Any intersection of subgroups of G is a group.

Proof Let H_i be a collection of subgroups of G, where i runs over some indexing set I. Let

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

All of the H_i contain 1, so H contains 1, and hence is non-empty. If $a, b \in H$ then ab^{-1} is in every H_i, so ab^{-1} is in H and H is a subgroup of G.
qed

5.8.2 Definition Let G be a group, and S a non-empty set of elements of G. (We do not require S to be a subgroup). The *group generated by S* , denoted $\langle S \rangle$, is the intersection of all the subgroups of G that contain S.

If $S = \{a_1, \ldots, a_n\}$ is finite we write $\langle a_1, \ldots, a_n \rangle$ instead of $\langle \{a_1, \ldots, a_n\} \rangle$.

There is at least one subgroup containing S, namely G itself. The intersection of groups is a group, so $\langle S \rangle$ is a subgroup of G. Each group in the intersection contains S, so $\langle S \rangle$ contains S. In fact, $\langle S \rangle$ is the smallest subgroup of G containing S, because if K is any subgroup containing S, K is one of the groups in the intersection defining $\langle S \rangle$, so $\langle S \rangle \subseteq K$.

5.8.3 Definition Let G be a group and let S be a subset of G. If $\langle S \rangle = G$ then we say that G is *generated by S*.

5.8.4 Example S_3 is generated by σ and τ.

Proof Let H be any subgroup of S_3 containing σ and τ. Since H is a group, it will have to contain 1, σ, σ^2, τ, $\sigma\tau$, $\sigma^2\tau$. But these are all the elements of S_3, so $H = S_3$. Thus the intersection of all such H is again S_3. That is, the smallest subgroup of S_3 containing both σ and τ is all of S_3. □

It helps to have an explicit description of $\langle S\rangle$, analogous to the description of the span as the set of all linear combinations.

5.8.5 Theorem Let G be a group, and S a non-empty subset of G. The group $\langle S\rangle$ generated by S consists of all finite product of the form $a_1^{n_1}\cdots a_k^{n_k}$ where $a_1,\ldots,a_k\in S$ and $n_1,\ldots,n_k\in\mathbb{Z}$.

5.8.6 Example For example, if $S=\{a,b,c\}$ then $\langle S\rangle$ contains terms such as $c^3a^{-2}ba$, $a^2b^{-3}a^2c^5a^{-7}$ and so on. (We cannot simplify these terms without further knowledge of G, since we cannot assume G is abelian for example.)

Proof Let K denote the set of all products of the form described. The group $\langle S\rangle$ contains each element in S, and—being a group—must then contain each a^n and all hence all products described. Thus

$$S\subseteq K\subseteq\langle S\rangle.$$

We must show $\langle S\rangle\subseteq K$. To prove this, we have only to show that K is a subgroup of G, since $\langle S\rangle$ is the *smallest* subgroup of G containing S.

First, let $a\in S$. Then $1=a^0\in K$. Next, if x and $y\in K$ then so is xy. Finally if $z\in K$ then z can be regarded as a product $a_1\cdots a_m$ with the $a_i\in S$ (where we "unwrap" powers like $a^3=a\cdot a\cdot a$). So $z^{-1}=a_m^{-1}\cdots a_1^{-1}\in K$. Hence $z^{-1}\in K$. So K is a subgroup of G. □

Suppose G is abelian and $S=\{a_1,\ldots,a_n\}$. Then $\langle S\rangle$ consists of all finite sums $m_1a_1+\cdots+m_na_n$ with $m_i\in\mathbb{Z}$, which is quite similar to the span in a vector space. If $S=\{a\}$ then G just consists of all ma with $m\in\mathbb{Z}$.

5.8.7 Example

- ★ In $(\mathbb{Z},+)$, $\langle 1\rangle$ is the set of all $m\cdot 1$ with $m\in\mathbb{Z}$, so $\langle 1\rangle=\mathbb{Z}$. Thus $\mathbb{Z}$ is generated by 1.
- ★ $\mathbb{Z}/n\mathbb{Z}$ is also generated by 1 by the same argument.
- ★ S_3 is generated by σ and τ. We saw by direct calculation (example 5.4.4) that all elements of S_3 are obtained by taking products of σ and τ.

5.9. Cyclic Groups

Theorem 5.8.5 implies

$$\langle a\rangle=\{a^n\mid n\in\mathbb{Z}\}$$

or in the abelian case $\langle a\rangle=\{na\mid n\in\mathbb{Z}\}$.

5.9.1 Definition If $G=\langle a\rangle$ then we say that G is *cyclic* , generated by a.

Thus G is cyclic exactly if every element of G can be written as a power (repeated sum in the abelian case) of some fixed generating element a.

5.9.2 Example

- ★ $\mathbb{Z}$ is cyclic, generated by 1.
- ★ $\mathbb{Z}/n\mathbb{Z}$ is cyclic, generated by 1.
- ★ $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic iff there exists a primitive root mod n. (Make sure you understand this statement.)
- ★ $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ is not cyclic. If $a=(1,0)$ then no multiple of a is $(0,1)$. Similarly $(0,0)$ and $(0,1)$ are not generators. Finally no multiple of $(1,1)$ is $(1,0)$.
- ★ S_3 is not cyclic (see the group table). Indeed S_3 has order 6, but all elements in S_3 have order 2 or 3.

Suppose a has order n. Then $\langle a\rangle$ contains $1 = a^0, a^1, \dots, a^{n-1}$ after which the powers of a repeat (and similarly for negative powers). This explains the two uses of the word order: *the order of an element is the order of the cyclic subgroup it generates.*

5.9.3 Theorem Every cyclic group is abelian.

Proof Let $\langle a\rangle$ be a cyclic group. If we pick two arbitrary elements a^n and a^m from this group then $a^n \cdot a^m = a^{n+m} = a^{m+n} = a^m \cdot a^n$. □

62 Exercise Let G be a finite group of order n. Then G is cyclic iff there exists an element of G of order n.

63 Exercise Let T be the group generated by a and b, subject to the relations $a^6 = 1$, $a^3 = b^2$, $ba = a^{-1}b$. Show that T is a non-abelian group of order 12.

5.10. Group Homomorphisms

Whenever we study mathematical objects it is very important to study the functions between them. When we study sets, we also study functions. When we examine vector spaces, we also examine linear maps (matrices), which are just special functions between vector spaces.

Since every group comes equipped with a binary operation, we should examine functions between groups that respect the binary operation (see below). Such a function is called a homomorphism: from “homo” meaning “the same” and “morphos” meaning “form” or “shape”.

Consider the following well known identity from linear algebra. The det function $\det\colon GL_n(\mathbb{R}) \to \mathbb{R}\setminus\{0\}$ satisfies

$$\det(AB) = \det(A)\det(B).$$

Here the product AB on the LHS is the product of two matrices, while the product $\det(A)\det(B)$ on the RHS is the product of two real numbers. It makes no difference whether we first multiply in $GL_n(\mathbb{R})$ and then apply det, or whether we first apply det and then multiply in $\mathbb{R}$.

Abstracting, we have the following definition:

5.10.1 Definition Let $(G, *)$ and $(H, \circ)$ be two groups. A *(group) homomorphism* from G to H is a function $f\colon G \to H$ satisfying

$$f(x * y) = f(x) \circ f(y) \qquad \text{for all } x,\, y \in G.$$

Here x and y are in G, so we can form $x * y$, which is again in G. Then we can apply f to end with an element in H. Or, we can first apply f to x and y. Now we have two elements $f(x)$, $f(y) \in H$, so we can form $f(x) \circ f(y)$. The defining property of a homomorphism is that we must get the same result either way.

$$\begin{tikzcd}
G & x,\ y \arrow[rr, "*"] \arrow[d, "f"'] & & x * y \arrow[d, "f"] \\
H & f(x),\ f(y) \arrow[r, "\circ"] & f(x) \circ f(y) \arrow[r, equal] & f(x * y)
\end{tikzcd}$$

5.10.2 Example

★ Consider the groups $GL_n(\mathbb{R})$ and $\mathbb{R}\setminus\{0\}$ under multiplication. The determinant function $\det\colon M_n(\mathbb{R}) \to \mathbb{R}$ is a homomorphism.

★ Consider the groups $(\mathbb{R},+)$ (real numbers under addition) and $(\mathbb{R}\setminus\{0\},\cdot)$ (non-zero reals under multiplication). Let $f\colon \mathbb{R}\to\mathbb{R}\setminus\{0\}$ be the exponential function. Then

$$f(x+y)=e^{x+y}=e^x\cdot e^y=f(x)\cdot f(y)$$

so f is a homomorphism.

★ Recall the reduction mod n map $\pi\colon \mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$, example 2.1.13 defined by $\pi(n)=[n]$. Then $\pi(a+b)=[a+b]=[a]\oplus[b]=\pi(a)+\pi(b)$. So π is a homomorphism from the group $(\mathbb{Z},+)$ to $(\mathbb{Z}/n\mathbb{Z},\oplus)$.

★ The map $f\colon \mathbb{Z}/3\mathbb{Z}\to\mathbb{Z}$ given by $f([0])=0$, $f([1])=1$, $f([2])=2$ is not a homomorphism. $f([2+1])=f([3])=f([0])=0$, but $f([2])+f([1])=2+1=3$ because the $+$ here is in $\mathbb{Z}$.

64 Exercise Consider $\mathbb{R}^+$ under multiplication, and the group $\mathbb{R}$ under addition. Check that the natural logarithm map $\log\colon (0,\infty)\to\mathbb{R}$ is a homomorphism. This follows from the identity $\log(xy)=\log(x)+\log(y)$.

65 Exercise

(a) Suppose $f\colon G\to H$ is a homomorphism, and $a\in G$ has order n. Show that the order of $f(a)$ must divide n.

(b) Let G be any finite group. Find all homomorphisms $f\colon G\to\mathbb{Z}$.

Group homomorphisms are required to respect the group operation, but in fact they also respect the identity element and inverses:

5.10.3 Theorem Let $(G,*)$ and $(H,\circ)$ be groups, and let $f\colon G\to H$ be a homomorphism. Then:

(a) $f(1_G)=1_H$ (homomorphisms preserve the identity)

(b) $f(x^{-1})=f(x)^{-1}$ (homomorphisms preserve inverses).

Proof

(a) $f(1_G)=f(1_G*1_G)=f(1_G)\circ f(1_G)$, and the result follows by cancelling (theorem 5.3.1).

(b) By (a), $1_H=f(1_G)=f(x*x^{-1})=f(x)\circ f(x^{-1})$ and similarly $f(x^{-1})\circ f(x)=1_H$ so $f(x^{-1})$ is the inverse of $f(x)$. □

5.10.4 Definition Let $f\colon G\to H$ be a homomorphism. The *kernel* of f is the set

$$\ker f=\{g\in G\mid f(g)=1_H\}.$$

If H is abelian, $\ker f=\{g\in G\mid f(g)=0_H\}$.

5.10.5 Theorem Let $f\colon G\to H$ be a homomorphism.

(a) $\ker f$ is a subgroup of G.

(b) $\ker f=\{1_G\}$ iff f is injective.

Proof

(a) $1_G\in\ker f$ by theorem 5.10.3, so $\ker f$ is non-empty. If x, $y\in\ker f$ then $f(x)=f(y)=1_H$. So

$$\begin{aligned} f(xy^{-1}) &= f(x)f(y^{-1}) && f \text{ is a homomorphism}\\ &= f(x)f(y)^{-1} && \text{By theorem 5.10.3}\\ &= 1_H1_H^{-1} && \text{Since } x,\ y\in\ker f\\ &= 1_H. \end{aligned}$$

So $\ker f$ is a subgroup of G, by theorem 5.5.6.

(b) $\Longrightarrow$ Suppose $\ker f = \{1_G\}$. If $f(x) = f(y)$ then $f(x)f(y)^{-1} = 1_H$ so $f(x)f(y^{-1}) = 1_H$ by theorem 5.10.3. Since f is a homomorphism, $f(x)f(y^{-1}) = f(xy^{-1})$ so $f(xy^{-1}) = 1_H$, so $xy^{-1} \in \ker f$. Thus $xy^{-1} = 1_G$, so $x = y$. Hence f is injective.

$\Longleftarrow$ Suppose f is injective. We know $1_G \in \ker f$. Suppose $x \in \ker f$. Then $f(x) = 1_H = f(1_G)$ by theorem 5.10.3. Since f is injective $x = 1_G$. Thus $\ker f = \{1_G\}$. □

5.10.6 Example Consider the reduction mod n homomorphism $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. The kernel of π is the set of all integers a with $[a] = 0$, that is, all a with $a \equiv 0 \pmod{n}$. Thus $\ker \pi = \{nx \mid x \in \mathbb{Z}\} = n\mathbb{Z}$.

5.10.7 Example Define a map $f\colon \mu_n \to \mathbb{Z}/n\mathbb{Z}$ by $f(\zeta^r) = [r]$ for $0 \leq r < n$. Then $f(\zeta^k) = [k]$ for any $k \geq 0$.

Proof Write $k = qn + r$ with $0 \leq r < n$. Then $\zeta^k = \zeta^{qn} \cdot \zeta^r = 1 \cdot \zeta^r = \zeta^r$ so $f(\zeta^k) = [r]$. But $k \equiv r \pmod{n}$ so $[r] = [k]$.
qed

Hence for any r, $s \geq 0$

$$f(\zeta^r \cdot \zeta^s) = f(\zeta^{r+s}) = [r+s] = [r] \oplus [s] = f(\zeta^r) \oplus f(\zeta^s).$$

Thus f is a homomorphism.

The kernel of f is the set of elements mapped to the identity. The identity in $\mathbb{Z}/n\mathbb{Z}$ is $[0]$ (additive notation). So

$$\begin{aligned} \ker f &= \{\zeta^r \mid 0 \leq r < n, \quad f(\zeta^r) = 0\} \\ &= \{\zeta^r \mid 0 \leq r < n, \quad [r] = [0]\} \\ &= \{1\}. \end{aligned}$$

By theorem 5.10.5 f is injective. f is also surjective since for any $[r] \in \mathbb{Z}/n\mathbb{Z}$, $f(\zeta^r) = [r]$. So f is a bijective homomorphism.

5.10.8 Example Let $\mathscr{F}$ be the group of all functions $\mathbb{R} \to \mathbb{R}$ under addition (example 4.1.3). Let $\mathscr{D}$ be the subset of all differentiable functions $\mathbb{R} \to \mathbb{R}$. This is a subgroup by theorem 5.5.6: if f and g are differentiable so is $f - g$.

Define a function $D\colon \mathscr{D} \to \mathscr{F}$ by $D(f) = f'$ (the derivative). (So D is the derivative operator.) Then

$$D(f+g) = (f+g)' = f' + g' = D(f) + D(g)$$

so D is a homomorphism. The kernel of D is the set of all functions whose derivative is the 0 function. This is the set of all constant functions.

5.10.9 Example Let G, H and K be groups. Suppose $f\colon G \to H$ and $g\colon H \to K$ are homomorphisms. Prove that $f \circ g\colon G \to K$ is a homomorphism.

Proof Exercise.

66 Exercise Prove this.

67 Exercise For each of the following, determine if the function given is a homomorphism of groups. If it is, describe the kernel.

(a) Let $n \in \mathbb{Z}$. Let $f\colon \mathbb{Z} \to \mathbb{Z}$ be given by $f(x) = nx$ for all x.
(b) Let $f\colon \mathbb{R} \to \mathbb{R} \setminus \{0\}$ be given by $f(x) = 2^x$ for all x. Here $\mathbb{R}$ is a group under addition and $\mathbb{R} \setminus \{0\}$ is a group under multiplication.
(c) Let G be any group, and let $f\colon G \to G$ be given by $f(x) = x^{-1}$ for all x.
(d) Consider the groups $M_n(\mathbb{R})$ and $\mathbb{R}$, both under addition. Let $f\colon M_n(\mathbb{R}) \to \mathbb{R}$ be given by $f(A) = \operatorname{tr}(A)$, the trace of A.

68 Exercise Describe all homomorphisms $f\colon \mathbb{Z} \to \mathbb{Z}$, where $\mathbb{Z}$ is a group under addition.

69 Exercise Let G and H be groups. Let $\pi\colon G\times H \to G$ be projection onto the first coordinate, $\pi(x,y) = x$. Prove that π is a surjective homomorphism. Describe $\ker\pi$.

5.11. Group Isomorphisms

We would like to understand when two groups are "the same". Equality is too stringent a requirement, since two groups may be structurally identical without actually being equal as setsİnstead we introduce a notion of structural equivalence, called *isomorphism.*

Consider the two groups $\mu_2 = \{1, -1\}$ and $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. Each group has two elements. Thus each group contains its identity and one further element. In μ_2 the non-identity element is -1, which is of order 2. In $\mathbb{Z}/2\mathbb{Z}$ the non-identity element is 1, also of order 2. Indeed, the two Cayley tables are identical, except that the elements have different names:

μ_2	1	-1
1	1	-1
-1	-1	1

$\mathbb{Z}/2\mathbb{Z}$	0	1
0	0	1
1	1	0

We see that we can exactly match these Cayley tables if we match the identity $1 \in \mu_2$ with the identity $0 \in \mathbb{Z}/2\mathbb{Z}$, and match $-1 \in \mu_2$ with $1 \in \mathbb{Z}/2\mathbb{Z}$. An exact matching of elements between two sets is a bijection, so we have constructed a bijection $\mu_2 \to \mathbb{Z}/2\mathbb{Z}$. But not only that, the bijection carries one Cayley table onto the other, so it preserves the group operation.

5.11.1 Definition An *isomorphism* is a bijective group homomorphism. If there exists an isomorphism $f\colon G \to H$ we say that G is *isomorphic* to H, and write $G \simeq H$.

5.11.2 Example

★ $\mu_2 \simeq \mathbb{Z}/2\mathbb{Z}$. The isomorphism is constructed above.

★ More generally $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$. The isomorphism is constructed in example 5.10.7. In other words, *μ_n and $\mathbb{Z}/n\mathbb{Z}$ are really "the same" group.* The only difference is in the naming of elements. In μ_n the elements are labelled $\{1, \zeta, \zeta^2, \ldots\}$ and the group operation is written multiplicatively. In $\mathbb{Z}/n\mathbb{Z}$ the elements are labelled $\{0, 1, 2, \ldots\}$ and the group operation is written additively.

If $G \simeq H$ then any theorem we can prove about G is true for H, because we can just relabel all the elements, using our isomorphism.

5.11.3 Theorem Let G, H, K be groups.

(a) $G \simeq G$.
(b) If $G \simeq H$ then $H \simeq G$.
(c) If $G \simeq H$ and $H \simeq K$ then $G \simeq K$.

Proof (a) The identity function $1_G\colon G \to G$ defined by $1_G(x) = x$ for all x is clearly a bijection. It is also a homomorphism, since $1_G(xy) = xy = 1_G(x)1_G(y)$.

(b) Let $f\colon G \to H$ be an isomorphism. We need an isomorphism $H \to G$. Since f is a bijection, $f^{-1}\colon G \to H$ is also a bijection. We check that f^{-1} is also a homomorphism. So let h_1, $h_2 \in H$. Since f is surjective, $h_1 = f(g_1)$ and $h_2 = f(g_2)$ for some g_1, $g_2 \in G$. This says that $g_1 = f^{-1}(h_1)$ and $g_2 = f^{-1}(h_2)$. Thus

$$\begin{aligned} f^{-1}(h_1h_2) &= f^{-1}(f(g_1)f(g_2)) \\ &= f^{-1}(f(g_1g_2)) \\ &= g_1g_2 \\ &= f^{-1}(h_1)f^{-1}(h_2). \end{aligned}$$

Hence $f^{-1}\colon H \to G$ is an isomorphism.

(c) Let $f\colon G \to H$ and $g\colon H \to K$ be isomorphisms. Then $g \circ f\colon G \to K$ is bijective, and is a homomorphism by Exercise 5.10.9. □

The next result is a generalization of example 5.10.7. For example, there is (up to isomorphism) only one group of order 2011 (prime), namely $\mathbb{Z}/2011\mathbb{Z}$. However there are many different relabellings of this group such as μ_{2011}.

5.11.4 Theorem Every cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Proof Let $\langle a\rangle$ and $\langle b\rangle$ be cyclic groups of order n. Define $f\colon \langle a\rangle \to \langle b\rangle$ by $f(a^r) = b^r$, $0 \le r < n$. Note that if $m = qn + r$ then $f(a^m) = f(a^{qn} \cdot a^r) = f(1 \cdot a^r) = f(a^r) = b^r = b^{qn} \cdot b^r = b^m$ so $f(a^m) = b^m$ for every $m \ge 0$.

Now f is a well defined surjective map between two finite sets with the same cardinality, hence is a bijection (theorem 3.3.7). And

$$f(a^r \cdot a^s) = f(a^{r+s}) = b^{r+s} = b^r \cdot b^s = f(a^r) \cdot f(a^s).$$

So f is a homomorphism. Thus any two cyclic groups of the same order are isomorphic. □

In particular: *any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

How to show two groups are isomorphic

Given G and H we must:

(a) Construct a function $f\colon G \to H$,
(b) Prove that f is a homomorphism,
(c) Prove that f is injective. Theorem 5.10.5 may be useful here.
(d) Prove that f is surjective.

An alternative to steps (c) and (d) is to show that f has an inverse, by constructing a function $g\colon H \to G$ and showing that $f \circ g$ and $g \circ f$ are identity functions.

5.11.5 Example We prove that $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Proof Let us denote the elements of $\mathbb{Z}/6\mathbb{Z}$ by $[n]_6$ to distinguish them from elements $[n]_2 \in \mathbb{Z}/2\mathbb{Z}$ and $[n]_3 \in \mathbb{Z}/3\mathbb{Z}$, and the addition in $\mathbb{Z}/6\mathbb{Z}$ by $\oplus_6$ etc. We need to construct a function $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. If this is going to be an isomorphism it should map the element $[1]_6 \in \mathbb{Z}/6\mathbb{Z}$ to an element of order 6 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. After a bit of searching we find that $([1]_2, [1]_3)$ has order 6. (See example 5.7.2). So we define

$$f([n]_6) = ([n]_2, [n]_3).$$

We must check that this function is well defined. As it stands, the rule for f appears to depend on the representative of $[n]_6$ chosenḂut if $[n]_6 = [m]_6$ in $\mathbb{Z}/6\mathbb{Z}$ then $n \equiv m \pmod 6$ so $n \equiv m \pmod 2$ and $n \equiv m \pmod 3$. This means $[n]_2 = [m]_2$ in $\mathbb{Z}/2\mathbb{Z}$ and $[n]_3 = [m]_3$ in $\mathbb{Z}/3\mathbb{Z}$. (Check that you understand this argument.)

Next we check that f is a homomorphism. But

$$\begin{aligned} f([n]_6 \oplus_6 [m]_6) &= f([n+m]_6) \\ &= ([n+m]_2, [n+m]_3) \\ &= ([n]_2 \oplus_2 [m]_2, [n]_3 \oplus_3 [m]_3) \\ &= ([n]_2, [n]_3) \oplus ([m]_2, [m]_3) \\ &= f([n]_6) \oplus f([m]_6). \end{aligned}$$

Finally, we have to show that f is a bijection. According to theorem 3.3.7, it is enough to prove that f is injective. The kernel of f is the set of $[n]_6$ mapping to $([0]_2, [0]_3)$. For such $[n]_6$, $n \equiv 0 \pmod 2$ and $n \equiv 0 \pmod 3$ so $n \equiv 0 \pmod 6$, so $[n]_6 = [0]_6$. Thus $\ker f = \{[0]_6\}$ and f is injective. □

There is nothing special about 2 and 3 in this proof. The generalization is:

5.11.6 Theorem Let m, $n \in \mathbb{N}$ with $\gcd(m,n) = 1$. Then

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Proof Define a map $f\colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f([a]_{mn}) = ([a]_m, [a]_n)$. If $[a]_{mn} = [b]_{mn}$ then $mn \mid (a-b)$ so $a \equiv b \pmod m$ and $a \equiv b \pmod n$. Hence $([a]_m, [a]_n) = ([b]_m, [b]_n)$. Thus f is well defined.

$f([a]_{mn} \oplus_{mn} [b]_{mn}) = f([a+b]_{mn}) = ([a+b]_m, [a+b]_n) = ([a]_m \oplus_m [b]_m, [a]_n \oplus_n [b]_n) = ([a]_m, [a]_n) \oplus_{mn} ([b]_m, [b]_n) = f([a]_{mn}) \oplus_{mn} f([b]_{mn})$ so f is a homomorphism.

If $f([a]_{mn}) = ([0]_m, [0]_n)$ then $[a]_m = 0$ so $m \mid a$ and similarly $n \mid a$. Since $\gcd(m,n) = 1$, $mn \mid a$ by corollary 1.7.6. So $[a]_{mn} = 0$. Hence the kernel of f is $\{0\}$, so f is injective.

Finally given any $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ and $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ there is an $[x] \in \mathbb{Z}/mn\mathbb{Z}$ with $[x]_m = [a]_m$ and $[x]_n = [b]_n$ that is, with $x \equiv a \pmod m$ and $x \equiv b \pmod n$, by the Chinese remainder theorem. (This again uses $\gcd(m,n) = 1$.) □

More generally still,

5.11.7 Theorem Let $m_1, \ldots, m_r \in \mathbb{N}$ with all the all m_i pairwise relatively prime. Then

$$\mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}.$$

Proof Exercise. □

This result is also called the *Chinese remainder theorem.* It is an algebraic formulation of the number theoretical Chinese remainder theorem we formulated earlier.[4]

How to show two groups are not isomorphic

There is a very easy way: if G and H are finite groups with a different number of elements then there cannot be a bijection $G \to H$. Or if one of G, H is infinite and the other is finite.

However two groups G and H with the same number of elements need not be isomorphic. It is difficult to prove that *no possible* function $G \to H$ is a group isomorphism. But isomorphisms preserve group properties. That is, if G has some property and $G \simeq H$ then H will also have the property (see below). Thus if G has a group property but H does not then G and H cannot be isomorphic.

The type of properties to look for are:

- G is cyclic but H is not (or vice versa),
- G is abelian,
- G has exactly one element of order 2, etc.

For example:

5.11.8 Example If G contains an element of order n and $G \simeq H$ then H contains an element of order n.

Proof Let $f\colon G \to H$ be a group isomorphism and let $b = f(a) \in H$. Let the order of a be n and the order of b be m. Then $a^n = 1$, so applying f, $f(a^n) = 1$, so $f(a)^n = 1$ so $b^n = 1$. This says that m, the order of b, divides n, the order of a (theorem 5.7.4). Apply the same argument with f^{-1}: $b^m = 1$ so $1 = f^{-1}(b^m) = f^{-1}(b)^m = a^m$ so $n \mid m$. Hence $n = m$. □

The fact that isomorphisms preserve the other properties can be proved similarly.

70 Exercise Suppose G is a finite cyclic group. Show that if $G \simeq H$ then H is a finite cyclic group. (The contrapositive is: if H is not a finite cyclic group then H cannot be isomorphic to G).

71 Exercise Show that if $G \simeq H$ and G is abelian, then so is H.

[4] Actually the result is still true if the LHS and RHS are viewed as rings (see later) and the isomorphism as a ring isomorphism. It is this ring result that is usually called the CRT.

Warning: properties that depend on the *names* of elements cannot be used, since names can change under isomorphisms. (If G has an element called a and $G \simeq H$, H need not have an element called a). The following types of properties can *not* be used:

- G contains the number 2,
- The elements of G are permutations,
- G is a subgroup of $\mathbb{Z}$ etc.

These properties have nothing to do with the *structure* of G. They merely reflect the particular *names* of elements in G.

5.11.9 Example Let $3\mathbb{Z} = \{3n \mid n \in \mathbb{Z}\}$. Check that $3\mathbb{Z}$ is a group under addition.

We cannot say $\mathbb{Z}$ is not isomorphic to $3\mathbb{Z}$ because $5 \in \mathbb{Z}$ and $5 \notin 3\mathbb{Z}$. In fact $\mathbb{Z}$ *is* isomorphic to $3\mathbb{Z}$. Let $f\colon \mathbb{Z} \to 3\mathbb{Z}$ be multiplication by 3, so $f(n) = 3n$ for all n.

f is injective: if $f(n) = f(m)$ then $3n = 3m$ so $n = m$. f is surjective by definition of $3\mathbb{Z}$. Also $f(n+m) = 3(n+m) = 3n + 3m = f(n) + f(m)$. □

5.11.10 Example $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof $\mathbb{Z}/4\mathbb{Z}$ has an element of order 4, namely 1. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ does not: its elements are $(0,0)$ of order 1, $(1,0)$ of order 2, $(0,1)$ of order 2 and $(1,1)$ of order 2. □

This means there are (at least) 2 different groups of order 4. It also shows that the hypothesis of relatively prime in the CRT (theorem 5.11.7) is necessary.

72 Exercise Show that no two of $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are isomorphic.

The above exercise gives 3 abelian groups of order 8. There are also 2 non-abelian groups of order 8: the dihedral group D_4 and the quaternion group Q_8 (example 54). These cannot be isomorphic to any of the 3 groups above, since an abelian group is never isomorphic to a non-abelian group.

73 Exercise Show that the dihedral group D_4 and the quaternion group Q_8 (example 54) are not isomorphic. Hint: count the number of elements of each order.

So there are at least 5 different groups of order 8. (In fact these are all the groups of order 8 up to isomorphism, although we shall not prove this.)

74 Exercise Let $S^1 = \{\cos\theta + i\sin\theta \mid 0 \leq \theta < 2\pi\}$. Show that S^1 is a group under multiplication. Is is isomorphic to $(\mathbb{R}, +)$? Explain.

5.12. Cosets. Lagrange's Theorem

As far as possible we would like to understand all groups. A great deal of progress has been made towards this goal. For example, there are known to be precisely two different groups of order 2005, one abelian ($\mathbb{Z}/2005\mathbb{Z}$) and one non-abelian.

A fundamental tool in understanding group structure is Lagrange's theorem. It imposes great restraints on the possible subgroups of a given group.

5.12.1 Theorem [Lagrange] Let G be a finite group of order n. Then the order of any subgroup of G divides n.

The strategy of the proof is as follows. Let H be a subgroup of G. We shall show that we can divide G into disjoint subsets called *cosets,* each with the same cardinality as H.

5.12.2 Definition Let G be a group, H a subgroup of G and $a \in G$. The *left coset* aH is the following subset of G:

$$aH = \{ah \mid h \in H\}.$$

The collection of all left cosets of H is denoted G/H.

(The *right coset* Ha is the set

$$Ha = \{ha \mid h \in H\}.$$

However we shall not use right cosets in this course.)

A special case occurs when $a = 1$. Then

$$1H = \{1h \mid h \in H\} = \{h \mid h \in H\} = H.$$

So $1H = H$.

If we are using additive notation cosets have the following appearance:

5.12.3 Definition Let G be an abelian group written additively. Suppose G has subgroup H. Let

$$a + H = \{a + h \mid h \in H\}$$

The importance of cosets is hinted at in the next example.

5.12.4 Example

$G = \mathbb{Z}$. Let $H = 3\mathbb{Z}$. Then H is a subgroup of G. The cosets of H are

$$\begin{aligned} 0 + H = H &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ 1 + H &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ 2 + H &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{aligned}$$

Note that these are exactly the congruence classes mod 3. The set of left cosets $G/H = \mathbb{Z}/3\mathbb{Z}$ is exactly what we called $\mathbb{Z}/3\mathbb{Z}$ earlier in the course.

5.12.5 Example Let $G = S_3$. Let σ and τ be the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Then $G = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. Recall that we have group table

S_3	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
1	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	1	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	1	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	1	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	1	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	1

Let $K = \langle\tau\rangle = \{1, \tau\}$. Then

$$\begin{aligned} 1K &= \{1, \tau\} \\ \sigma K &= \{\sigma, \sigma\tau\} \\ \sigma^2 K &= \{\sigma^2, \sigma^2\tau\} \\ \tau K &= \{1, \tau\} = 1K \\ \sigma\tau K &= \{\sigma\tau, \sigma\} = \sigma K \\ \sigma^2\tau K &= \{\sigma^2\tau, \sigma^2\} = \sigma^2 K \end{aligned}$$

So G/K consists of 3 cosets, each with 2 elements: K, σK and $\sigma^2 K$.

Let $H = \langle \sigma \rangle = \{1, \sigma, \sigma^2\}$. Then

$$\begin{aligned}
1H &= H \\
\sigma H &= \{\sigma, \sigma^2, 1\} = H \\
\sigma^2 H &= \{\sigma^2, 1, \sigma\} = H \\
\tau H &= \{\tau, \tau\sigma, \tau\sigma^2\} = \{\tau, \sigma^2\tau, \sigma\tau\} \\
\sigma\tau H &= \{\sigma\tau\sigma, \sigma\tau\sigma^2, \sigma\tau\} = \{\tau, \sigma^2\tau, \sigma\tau\} = \tau H \\
\sigma^2\tau H &= \{\sigma^2\tau\sigma, \sigma^2\tau\sigma^2, \sigma^2\tau\} = \{\tau, \sigma^2\tau, \sigma\tau\} = \tau H.
\end{aligned}$$

We see that G/H consists of two cosets, each with 3 elements.

In each example, all the cosets we have seen have the same number of elements, and partition up the group G into disjoint blocks. This is true in general, and is a generalization of Corollary 2.1.10.

5.12.6 Theorem Let G be a group, H a subgroup of G.

(a) $aH = bH$ iff $a^{-1}b \in H$.
(b) Any two left cosets of H in G are either equal, or disjoint.
(c) G is the union of all the left cosets aH as a varies across G.
(d) If G is finite then any two left cosets have the same number of elements, equal to the number of elements in H: $|aH| = |H|$ for every a.

Proof

(a) $\Longrightarrow$ If $aH = bH$ then $b \in bH = aH$ so $b = ah$ for some $h \in H$, so $a^{-1}b = h \in H$.

$\Longleftarrow$ Suppose $a^{-1}b = h \in H$. Then

$$b = ah, \qquad a = bh^{-1}.$$

Consider any element $bh_1 \in bH$. Then $bh_1 = a(hh_1) \in aH$. Thus $bH \subseteq aH$. And if $ah_2 \in aH$, $ah_2 = b(h^{-1}h_2) \in bH$ so $aH \subseteq bH$.

(b) Compare theorem 2.1.10. Let aH and bH be left cosets. If they are disjoint there is nothing to prove. Thus suppose $x \in aH$ and $x \in bH$. Then $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Then $a^{-1}b = h_1 h_2^{-1} \in H$. Thus $aH = bH$ by (a).

(c) $a = a \cdot 1 \in aH$ for every a so each $a \in G$ occurs in one of the cosets, namely aH. Thus every element of G occurs somewhere in the union.

(d) We define a function $f\colon H \to aH$ by $f(h) = ah$. This has an inverse $g\colon aH \to H$ defined by $g(ah) = h$. So f is a bijection. By theorem 3.3.6, $|H| = |aH|$. □

5.12.7 Definition Let G be a group, H a subgroup. If the number of left cosets of H in G is a finite number n, we say that H has *index* n in G. We denote this by $[G\colon H] = n$.

Note: if G is finite it certainly only has a finite number of left cosets.

5.12.8 Theorem If G is finite then $|G| = [G\colon H] \cdot |H|$ for any subgroup H.

Proof This is a counting argument. G can be written as a disjoint union of left cosets by theorem 5.12.6. So

$$G = a_1H \cup a_2H \cup \cdots \cup a_nH.$$

The number n of these cosets is $[G\colon H]$, by definition. Moreover, each of these cosets has $|H|$ elements. The result follows. □

5.12.9 Corollary [Lagrange] Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.

Proof In theorem 5.12.8 $|G|$, $[G\colon H]$ and $|H|$ are all positive integers. □

5.12.10 Corollary Let $|G| = n$. Then the order of any element of G divides n.

Proof Let $a \in G$. The order of a is the order of the cyclic subgroup $\langle a\rangle$ generated by a. According to Lagrange's theorem, the size of this subgroup must divide n. □

5.12.11 Corollary If $|G| = p$ is prime, then $G \simeq \mathbb{Z}/p\mathbb{Z}$. That is, there is only one group of order p (up to isomorphism).

Proof Let $|G| = p$. Let $a \in G$ with $a \neq 1$. Then the order of a is not 1 and divides p, so must be p. Thus the cyclic subgroup $\langle a\rangle$ of G contains p elements, so is all of G. So G is a cyclic group with p elements, hence is $\simeq \mathbb{Z}/p\mathbb{Z}$ (theorem 5.11.4). □

We finally can prove Euler's theorem (theorem 2.11.1).

5.12.12 Corollary [Euler's Theorem] Let $n \in \mathbb{N}$. If $\gcd(a, n) = 1$ then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof Let $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$. The order of G is $\varphi(n)$, so the order of each $a \in G$ divides $\varphi(n)$. So $a^{\varphi(n)} \equiv 1 \pmod{n}$ (see theorem 5.7.4). □

75 Exercise True or false? If G is a group of order n and $a \in G$ then a has order n.

5.13. Normal Subgroups. Quotient Groups

Let G be a group, and let H be a subgroup. Then we can form the set of left cosets G/H. If we are lucky *this set of cosets will also form a group,* called the *quotient* of G by H. If we understand H and G/H then we have gone a long way towards understanding G.

As a set, G/H is the set of left cosets of H. We would like to define a group operation on G/H. How should we define the product of aH and bH? There is a natural choice:

$$(aH)(bH) = (ab)H. \tag{5.13.1}$$

But there is a major difficulty with this "definition". The cosets aH and bH have many different names. Do we get the same answer no matter which representative is chosen? If not, our multiplication rule will not make sense. (Compare the discussion for addition and multiplication of congruence classes mod n, § 2.2.)

5.13.1 Example Let $G = S_3$, $H = \langle\sigma\rangle$, $K = \langle\tau\rangle$. (Refer to example 5.12.5). $G/H = \{H, \tau H\}$. According to equation 5.13.1 the multiplication table in G/H should be

	H	τH
H	H	τH
τH	τH	H

(Recall $H = 1 \cdot H$ and $\tau^2 = 1$.) But $H = \sigma H$, and $\tau H = \sigma\tau H$. If we multiply these out, do we get the same answer? $(\sigma H)(\sigma\tau H) = \sigma^2\tau H = \tau H$, so yes. Testing the other possibilities, we find multiplication is well defined in this case.

Now consider G/K. We should define $(\sigma K)(\sigma K) = \sigma^2 K$. But $\sigma K = \sigma\tau K$. Now $(\sigma\tau K)(\sigma K) = (\sigma\tau\sigma)K = \tau K \neq \sigma^2 K$. So multiplication does not make sense in G/K.

We see that we can only sometimes define a multiplication of cosets. In order for multiplication to make sense, we shall show that H must have the following property:

5.13.2 Definition A subgroup H of G is said to be *normal* if for every g in G and $h \in H$, we have $g^{-1}hg \in H$. We write

$$H \trianglelefteq G$$

to mean H is a normal subgroup of G.

Note that g^{-1}, h and $g \in G$ so $g^{-1}hg \in G$ is certain. However g need not be in H, so $g^{-1}hg$ need not remain in H in general.

Obviously $G \trianglelefteq G$ for every G. Write[5]

$$H \triangleleft G$$

if $H \trianglelefteq G$ and $H \neq G$.

5.13.3 Example Let $G = S_3$ and let σ, τ be as above. Let $H = \langle\sigma\rangle$ and $K = \langle\tau\rangle$.

Claim: $H \trianglelefteq G$.

Proof Check using the group table that $\tau\sigma = \sigma^{-1}\tau$ and $\tau\sigma^2 = \sigma^{-2}\tau$ (note that $\sigma^2 = \sigma^{-1}$). So $\tau\sigma^r = \sigma^{-r}\tau$ for $r = 1$, 2. Also note that $\tau = \tau^{-1}$.

Let $h = \sigma^r \in H$ and $g \in G$. Consider $g^{-1}hg$. If $g \in H$ then this product is automatically in H, since H is a subgroup. So let $g = \sigma^s\tau$ for $s = 0$, 1 or 2. Then $g^{-1}hg = \tau\sigma^{-s}\sigma^r\sigma^s\tau \ = \tau\sigma^r\tau = \sigma^{-r} \in H$. □

Claim: K is not normal in G.

Proof Let $g = \sigma \in G$ and $h = \tau \in K$. Then $g^{-1}hg = \sigma^{-1}\tau\sigma \ = \sigma^{-1}\sigma^2\tau = \sigma\tau \notin K$.

This explains why G/H was a group above, but G/K was not. □

5.13.4 Example Any subgroup of an abelian group is normal.

Proof Let H be a subgroup of G. Let $g \in G$ and $h \in H$. In additive notation we must check that $-g + h + g \in H$. But $-g + h + g = h + (-g) + g = h \in H$. □

This is why we had no problem defining a group operation in $\mathbb{Z}/n\mathbb{Z}$.

We now prove the theorem motivating the definition of normal subgroup.

5.13.5 Theorem Let $H \trianglelefteq G$. Then G/H is itself a group, under the group operation defined by

$$(aH)(bH) = (ab)H.$$

If $[G\colon H]$ is finite, then G/H is a group with $[G\colon H]$ elements.

Proof We must show that this binary operation on G/H is well defined. The potential problem is that a single coset aH may have many different names: it is quite possible for $aH = a'H$ without $a = a'$. So a priori the definition of multiplication depends on the particular representative of the coset chosen.

Suppose $a_1H = a_2H$ and $b_1H = b_2H$. We must show $(a_1H)(b_1H) = (a_2H)(b_2H)$. That is, we must show $(a_1b_1)H = (a_2b_2)H$. By theorem 5.12.6, it is enough to show $(a_1b_1)^{-1}a_2b_2 \in H$.

Now $a_1^{-1}a_2 = h_1$ and $b_1^{-1}b_2 = h_2$ for some $h_1, h_2 \in H$ (using theorem 5.12.6 applied to the hypotheses). So

$$\begin{aligned}(a_1b_1)^{-1}a_2b_2 &= b_1^{-1}(a_1^{-1}a_2)b_2 \\ &= (b_1^{-1}b_2)(b_2^{-1}a_1^{-1}a_2b_2) \quad \text{Inserting factor } b_2b_2^{-1} \\ &= h_2(b_2^{-1}h_1b_2).\end{aligned}$$

Since $H \trianglelefteq G$, $(b_2^{-1}h_1b_2) \in H$. So $(a_1b_1)^{-1}a_2b_2 \in H$. This proves multiplication is well defined in G/H.

The group axioms are easy to check:

Associativity: $(aH)\Big((bH)(cH)\Big) = (aH)(bcH) = a(bc)H = (ab)cH = \Big((aH)(bH)\Big)(cH)$.

Identity: $(aH)(1H) = (a \cdot 1)H = aH$ and $(1H)(aH) = (1 \cdot a)H = aH$ so G/H has an identity, H.

Inverses: $(aH)(a^{-1}H) = (aa^{-1})H = H$, $(a^{-1}H)(aH) = (a^{-1}a)H = H$. □

[5] Many authors use $\triangleleft$ for both $\trianglelefteq$ and $\triangleleft$.

76 Exercise Let N be a subgroup of G. Show that $N \trianglelefteq G$ iff $aN = Na$ for every $a \in G$. That is, if N is normal, left cosets are the same as right cosets (and are just called cosets). This is why we have only concentrated on left cosets in this course.

77 Exercise Suppose N is a subgroup of G with $[G\colon N] = 2$. Show that N must be normal.

Intuition about G/H

The elements of G/H are cosets of G. So an entire set of elements of G is merged together into a single object in G/H. For example, the entire subgroup H is merged into a single element, and becomes the identity in G/H.

Thus the quotient group "blurs" collections of elements into single elements. Elements a and $b \in G$ are equal when $a^{-1}b = 1$. In the quotient group $aH = bH$ whenever $a^{-1}b \in H$, a weaker condition. Altogether G/H is a sort of shrunken or blurred version of G, with H controlling the amount of blurring or merging that takes place.

These remarks are illustrated in our S_3 example. Here is the group table, one last time:

S_3	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
1	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	1	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	1	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	1	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	1	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	1

In the quotient group G/H, the elements $1H, \sigma H, \sigma^2 H$ are all the same, equal to the identity. So the top left and bottom right corners of the table above become the identity. The quotient group looks like

S_3/H	H	τH
H	H	τH
τH	τH	H

G has 6 elements, but H has 3, so G/H has just two elements (2 subsets of G with 3 elements). In fact from the group table we see that $G/H \simeq \mathbb{Z}/2\mathbb{Z}$ with isomorphism $H \mapsto 0$, $\tau H \mapsto 1$.

5.13.6 Example The abstract definition of $\mathbb{Z}/n\mathbb{Z}$. The set $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, it is a normal subgroup. Instead of writing $a + n\mathbb{Z}$ for the coset of a, we write $[a]$ or just a. The addition we defined on $\mathbb{Z}/n\mathbb{Z}$ is exactly addition of cosets.

5.13.7 Example If G is any group, $G \trianglelefteq G$. There is just one coset since $gG = G$ for every g (because $g^{-1} \cdot 1 \in G$). So G/G is the trivial group with one element. This represents the most drastic collapsing of G possible.

5.13.8 Example We also have $H = \{1\} \trianglelefteq G$. But in this case each coset consists of a single element, since $aH = bH$ implies $a^{-1}b \in H = \{1\}$, so $a = b$. Thus $G/H \simeq G$ (an isomorphism is $G \to G/H$ sending $a \mapsto aH$.) In this case we get no collapsing at all.

5.13.9 Example Consider $\mathbb{Z}$ and $\mathbb{Q}$ under addition. $(\mathbb{Q}, +)$ is an abelian group so $\mathbb{Z}$ is a normal subgroup. In $\mathbb{Q}/\mathbb{Z}$, $a + \mathbb{Z} = b + \mathbb{Z}$ iff $a - b \in \mathbb{Z}$. So we have one coset $q + \mathbb{Z}$ for each $q \in [0, 1) \cap \mathbb{Q}$.

$1/2 + \mathbb{Z}$ has order 2 in $\mathbb{Q}/\mathbb{Z}$ because $(1/2 + \mathbb{Z}) + (1/2 + \mathbb{Z}) = (1 + \mathbb{Z}) = 0 + \mathbb{Z}$. In general $m/n + \mathbb{Z}$ has order n (provided $\gcd(m, n) = 1$.) Thus $\mathbb{Q}/\mathbb{Z}$ is an infinite group, in which every element has finite order.

78 Exercise Consider the group $(\mathbb{R}, +)$. Let $r \in \mathbb{R}$. Describe the group $\mathbb{R}/r\mathbb{R}$.

79 Exercise Show that $\mathbb{R}/\mathbb{Z} \simeq S^1$. Recall that $S^1 = \{\cos\theta + i\sin\theta \mid \theta in\mathbb{R}\}$ under multiplication.

From a more advanced viewpoint, normal subgroups are the same thing as kernels. First, kernels are always normal subgroups:

5.13.10 Theorem Let $f\colon G \to H$ be a group homomorphism. Then $\ker f \trianglelefteq G$.

Proof Let $g \in G$ and $h \in \ker f$. We must show $g^{-1}hg \in \ker f$. But $f(g^{-1}hg) = f(g)^{-1}f(h)f(g) = f(g)^{-1}f(g)$ since $f(h) = 1$, and $f(g)^{-1}f(g) = 1$, so $g^{-1}hg \in \ker f$ and we are done. □

On the other hand, every normal subgroup is the kernel of something:

5.13.11 Theorem Let $N \trianglelefteq G$. Then the map $F\colon G \to G/N$ given by $F(g) = gN$ is a surjective group homomorphism with kernel N.

Proof $F(g_1g_1) = (g_1g_2)N = (g_1N)(g_2N) = F(g_1)F(g_2)$. F is surjective by the definition of G/N. Finally

$$\begin{aligned}\ker F &= \{g \in G \mid 1N = gN\}\\ &= \{g \in G \mid 1^{-1}g \in N\}\\ &= \{g \in G \mid g \in N\} = N. \quad \square\end{aligned}$$

5.14. The First Isomorphism Theorem

In this section we give a hint of the more advanced theory.

5.14.1 Definition A group G is said to be *simple* if it has no normal subgroups except for G and $\{1\}$. (It is allowed to have other non-trivial subgroups, but no normal ones.)

Simple groups are rather like prime numbers. Much information about G can be obtained from knowledge of the simple subgroups of G. Simple groups are thus very important in more advanced group theory.

5.14.2 Example $\mathbb{Z}/p\mathbb{Z}$ is simple for every prime number p.

Proof By Lagrange's theorem, $\mathbb{Z}/p\mathbb{Z}$ has no subgroups except for $\{1\}$ and the whole group. □

There are many other simple groups. One of the great projects of twentieth century mathematics was to classify all of the finite simple groups. This was eventually achieved, although the proof is thousands of pages long.

There is a very important result that describes the image of a group under a homomorphism. This result is used often in advanced algebra.

5.14.3 Theorem [First Isomorphism Theorem] Let $f\colon G \to H$ be a group homomorphism. Then

$$G/\ker f \simeq \mathrm{Im} f.$$

Proof Let $K = \ker f$. We know that $K \trianglelefteq G$ by theorem 5.13.10, so $G/\ker f$ is a group.

Define a map $\overline{f}\colon G/K \to H$ by

$$\overline{f}(gK) = f(g).$$

As usual, we must check that this makes sense. Suppose $g_1K = g_2K$. Then $g_1^{-1}g_2 \in K$, so $f(g_1^{-1}g_2) = 1$. Since f is a homomorphism this means $f(g_1)^{-1}f(g_2) = 1$ so $f(g_1) = f(g_2)$. Thus $\overline{f}(g_1K) = \overline{f}(g_2K)$ and $\overline{f}$ is well defined.

Next check that $\overline{f}$ is a homomorphism: $\overline{f}(g_1K \cdot g_2K) = \overline{f}(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = \overline{f}(g_1K)\overline{f}(g_2K)$.

If $\overline{f}(gK) = 1$ then $f(g) = 1$ so $g \in \ker f = K$ so $gK = K$ the identity element in G/K. So the only element of the kernel of $\overline{f}$ is the identity. Hence f is injective.

Finally the image of $\overline{f}$ is the set of all possible $f(g)$, as g varies across G. This is exactly the image of f. So if we consider $\overline{f}$ as a map from G/K to Imf, it will be surjective, and hence an isomorphism. □

5.15. Table of Small Groups

We give a complete list of groups of small order, up to isomorphism. The proof that this lists is complete is beyond the scope of this course. (See Math 3303.)

It may seem that we have omitted some groups. For example $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a group of order 6. However by the CRT (theorem 5.11.7, example 5.11.5) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$, so we have listed a group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

n	Abelian Groups	Non-abelian Groups
1	$\{1\}$	
2	$\mathbb{Z}/2\mathbb{Z}$	
3	$\mathbb{Z}/3\mathbb{Z}$	
4	$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	
5	$\mathbb{Z}/5\mathbb{Z}$	
6	$\mathbb{Z}/6\mathbb{Z}$	$S_3 = D_3$
7	$\mathbb{Z}/7\mathbb{Z}$	
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	D_4, Q_8
9	$\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	
10	$\mathbb{Z}/10\mathbb{Z}$	D_5
11	$\mathbb{Z}/11\mathbb{Z}$	
12	$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	D_6, A_4, T
13	$\mathbb{Z}/13\mathbb{Z}$	
14	$\mathbb{Z}/14\mathbb{Z}$	D_7
15	$\mathbb{Z}/15\mathbb{Z}$	

Here A_4 is an index 2 subgroup of S_4, called the *alternating group* . T is the group

$$T = \langle a, b \mid a^6 = 1, a^3 = b^2, ba = a^{-1}b \rangle.$$

There are 14 groups of order 16, 51 of order 32 and 267 different groups of order 64 . . . .

5.16. Fundamental Theorem of Finite Abelian Groups

Examining the table in the previous section, the finite abelian groups that appear are all just products of $\mathbb{Z}/n\mathbb{Z}$ for various n. Remarkably, this is true for any finite abelian group.

5.16.1 Theorem [Fundamental Theorem of Finite Abelian Groups] Let A be a finite abelian group. Then

$$A \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

for some $m_1, \ldots, m_r \in \mathbb{Z}$.

Proof Omitted. □

There is no similar statement for non-abelian groups—these can be very complicated. It is known that every finite group is isomorphic to a subgroup of a symmetric group S_n for some n but it is not necessarily easy to extract usable information from this result.

80 Exercise Let X be a set, and let $\mathscr{P}(X)$ be the power set of X. Define a binary operation Δ on $\mathscr{P}(X)$ by $A\Delta B = (A \cup B) \setminus (A \cap B)$. This is called the *symmetric difference* of A and B.

Prove that $(\mathscr{P}(X), \Delta)$ is an abelian group. If X has n elements, which group is it?

Let S be the subset of $\mathscr{P}(X)$ consisting only of finite subsets of X with an even number of elements. Prove that S is a subgroup of $\mathscr{P}(X)$.