1 Binary operations (09/20)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

which shows that this commutative binary operation is not associative.

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

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

1.1 Exercises

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

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

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

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

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

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

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

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

2 Groups (09/22)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.1 Exercises

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

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

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

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

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

3 Symmetric groups (09/25)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.1 Exercises

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

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

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

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

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

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

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

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

4 Cycle decomposition in cyclic groups (09/27)

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

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

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

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

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

Recall the following definition from last time.

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

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

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

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

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

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

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

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

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

can be written efficiently as

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

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

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

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

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

4.1 Exercises

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

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

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

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

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

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

and

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

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

5 Group homomorphisms (09/29)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1 Exercises

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

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

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

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

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

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

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

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

6 Subgroups (10/02)

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

(i) X is nonempty,

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

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

These conditions imply

(iv) $e \in X$,

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

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

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

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

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

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

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

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

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

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

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

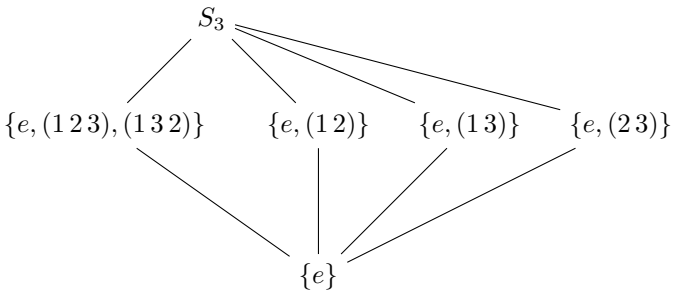

Figure 1: Subgroups of S_3.

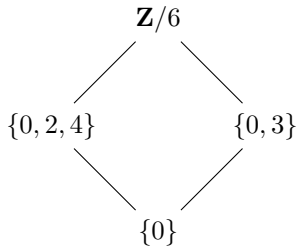

Figure 2: Subgroups of $\mathbf{Z}/6$.

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

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

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

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

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

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

6.1 Exercises

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

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

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

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