1 Basic group theory definitions

1.1 Groups, subgroups, and product groups [2.1–2.3, 2.11]

Definition 1.1 (Law of composition)**.** A *law of composition* on a set S is a map

$$S \times S \to S.$$

For example, addition and multiplication of integers.

Example 1.2. Let T be a set, and let S denote the set of all functions $g\colon T \to T$. Function composition

$$(g, f) \mapsto g \circ f$$

is a law of composition on S, where

$$g \circ f\colon T \xrightarrow{f} T \xrightarrow{g} T,$$

i.e., $g \circ f$ is the function $t \mapsto g(f(t))$.

Definition 1.3 (Group axioms)**.** A *group* is a set G with a law of composition such that

1. the law of composition is **associative**: $a(bc) = (ab)c$ for all $a, b, c \in G$.
2. G contains an **identity** element $e \in G$ such that $ea = ae = a$ for all $a \in G$.
3. every element $a \in G$ has an **inverse**, an element b such that $ab = ba = e$.

Proposition 1.4. *In a group,*

1. *the identity is unique. We often denote it by* 1 *or* 0.
2. *the inverse of an element* a *is unique. We usually denote it by* a^{-1}.
3. $(ab)^{-1} = b^{-1}a^{-1}$.
4. *the* ***cancellation law*** *holds: if* $ab = ac$*, then* $b = c$.

Proof.

1. If e and e' are both identities, then

$$e = ee' = e'.$$

4. Multiplying both sides of $ab = ac$ by a^{-1} on the left gives $b = c$.

$\square$

Example 1.5.

1. The set $\mathbb{Z}/n\mathbb{Z}$ equipped with addition is a group. The identity is the congruence class $\overline{0}$.

2. For $n > 1$, the set $\mathbb{Z}/n\mathbb{Z}$ equipped with multiplication is *not* a group. The identity would have to be $\overline{1}$, but $\overline{0}$ does not have a multiplicative inverse.

3. Let p be a prime. Recall that $(\mathbb{Z}/p\mathbb{Z})^\times$ denote the set of *nonzero* elements of $\mathbb{Z}/p\mathbb{Z}$. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group under multiplication.

4. In general, $(\mathbb{Z}/n\mathbb{Z})^\times$ is also a group under multiplication. Recall that this is the set of congruence classes $\overline{a}$ where a is relatively prime to n.

Definition 1.6. A group G is called *commutative* or *abelian* if $ab = ba$ for all $a, b \in G$.

Example 1.7. The examples above are abelian. An example of a nonabelian group is

$$\mathrm{GL}_n(\mathbb{R}) \coloneqq \{n \times n \text{ real matrices with nonzero determinant}\}.$$

The *order* of a group G is the number of elements of G, and denoted $|G|$. It could be infinite.

Definition 1.8. A *subgroup* of a group G is a subset H satisfying

1. the identity is contained in H.

2. if $a, b \in H$, then $ab \in H$. This property is referred to as *closure*.

3. if $a \in H$, then $a^{-1} \in H$.

The subgroup is called *proper* if it is not equal to G or $\{1\}$.

Example 1.9. The special linear group

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

is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Definition 1.10. Let G and G' be groups. The *product group* consists of the set of pairs

$$G \times G' = \{(a, a') : a \in G, a \in G'\},$$

and the law of composition is given by

$$(a, a') \cdot (b, b') = (ab, a'b').$$

The identity of $G \times G'$ is $(1_G, 1_{G'})$.

1.2 Permutations [1.5]

Definition 1.11. A *permutation* (of length n) is a bijective map $\sigma\colon \{1,2,\dots,n\} \to \{1,2,\dots,n\}$.

Here is an example of a permutation of length 6.

n	1	2	3	4	5	6
$\sigma(n)$	3	5	4	1	2	6

We express permutations using *cycle notation* which works like this.

- Pick an arbitrary index, for example 1.
- We see where σ sends 1. In this example, $\sigma(1) = 3$.
- We see where σ sends 3. In this example, $\sigma(3) = 4$.
- We see where σ sends 4. In this example, $\sigma(4) = 1$.
- We are back where we started. We indicate the cycle $\sigma\colon 1 \to 3 \to 4 \to 1$ using the notation
$$(134).$$
- We collect all cycles, and usually ignore 1-cycles, The σ above is
$$(134)(25)(6), \text{ or } (134)(25).$$

Note: the cycle notation is not unique. We can also express (134) as

$$(341) \text{ or } (413)$$

by choosing a different starting index.

Example 1.12. In cycle notation,

$$(1452) \circ (134)(25) = (135).$$

In general, *bijective* functions from a set T to itself form a group under composition. The identity is the function $\mathrm{id}(t) = t$, and inverses exist by the requirement that the functions are bijective.

Definition 1.13. The group of permutations of the set $\{1,2,\dots,n\}$ is called the *symmetric group* and denoted S_n. It has order $n!$

Example 1.14. The group S_3 has 6 elements. Let $x = (123)$ and $y = (12)$. Since x is a 3-cycle and y is a 2-cycle,

$$x^3 = 1, \quad y^2 = 1. \tag{$\heartsuit$}$$

One can verify without computation that the six elements

$$1, x, x^2, y, xy, x^2y$$

are distinct, using the cancellation law.

So S_3 consists of these 6 elements. Observe that

$$yx = (12) \circ (123) = (23) = (132) \circ (12) = x^2 y. \qquad (\diamondsuit)$$

This rule lets us move all occurrences of y to the right. For example,

$$x^{-1} y^3 x^2 y = x^2 y x^2 y = x^2 (yx) xy = x^2 (x^2 y) xy = x(yx)y = x(x^2 y)y = 1.$$

The elements x and y and the equations ($\heartsuit$) and ($\diamondsuit$) are called a set of *generators and relations* for S_3, and we write

$$S_3 = \langle x, y \mid x^3 = 1, y^2 = 1, yx = x^2 y \rangle.$$

This is called a *presentation* of the group S_3.

1.3 Orders [2.4]

For any $x \in G$, the *cyclic subgroup* generated by x consists of the elements

$$\ldots, x^{-2}, x^{-1}, 1, x, x^2, \ldots$$

and is denoted $\langle x \rangle$.

Definition 1.15. Let x be an element of a group G. The *order* of x is the smallest positive integer n such that $x^n = 1$.

If no such integer exists, then x has *infinite order.*

Proposition 1.16. *Let x be an element of G of order n. Let k and j be integers.*

1. *If $x^k = 1$, then $k = nq$ for some integer q.*
2. *If $x^k = x^j$, then $k - j = nq$ for some integer q.*

Proof.

1. Let $k = nq + r$ for $0 \leq r < n$. Then if $x^k = 1$, since $x^n = 1$, we have

   $$1 = x^k = x^{nq+r} = (x^n)^q x^r = x^r.$$

   By minimality of n, we must have $r = 0$.
2. Follows from 1. □

Example 1.17. Some applications of the above properties of orders:

1. If x has order n, then $\langle x \rangle$ is a finite subgroup of order n, consisting of the elements

   $$1, x, x^2, \ldots, x^n.$$

2. Let $G = (\mathbb{Z}/p\mathbb{Z})^\times$. Fermat's little theorem is the statement that for any $a \in G$,
$$a^{p-1} = 1.$$
Thus, the order of every element of G divides $p-1$.

The formulation of Fermat's little theorem in 2. above generalizes to any finite group.

Theorem 1.18 (Lagrange's theorem)**.** *Let G be a finite group. Then for any $a \in G$,*
$$a^{|G|} = 1.$$

Proof for abelian groups. The proof is similar to the proof of Fermat's little theorem we saw in Lecture 1.

Let $G = \{g_1, \ldots, g_n\}$, where $n = |G|$. Then $G = \{ag_1, \ldots, ag_n\}$ is the same set because the (left) multiplication by a map $G \to G$ is bijective; it has inverse (left) multiplication by a^{-1}.

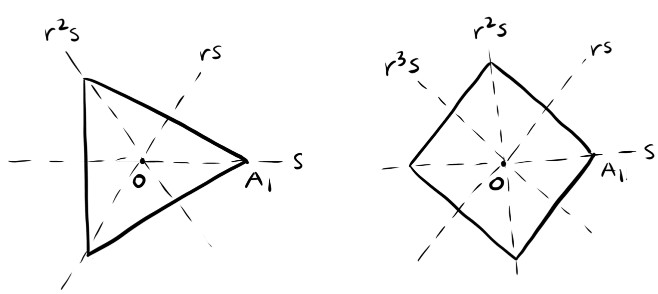
Taking the product of all elements in G,
$$g_1 \cdots g_n = a^n (g_1 \cdots g_n).$$
This calculation requires G to be abelian. By cancellation, $a^n = 1$. □

Corollary 1.19. *In a finite group G, the order of every element divides $|G|$.*

1.4 Dihedral group

Let $A_1 A_2 \cdots A_n$ be a regular n-gon, with center O. (In the case $n = 2$, it is a segment.) The *dihedral group* D_n consists of the symmetries of the regular n-gon. It has order
$$|D_n| = 2n.$$

- There are n rotations in D_n. Let r denote rotation by $2\pi/n$ around O. It satisfies
$$r^n = 1.$$
The other rotations are
$$1, r, r^2, \ldots, r^{n-1}.$$
- There are n reflections in D_n.



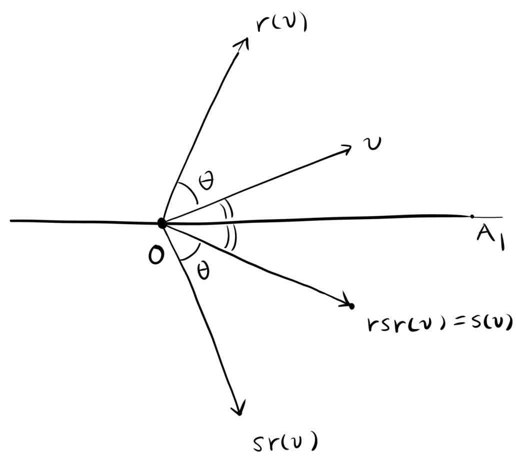
Let s denote reflection across OA_1. It satisfies

$$s^2 = 1.$$

The other reflections are

$$s, rs, r^2 s, \ldots, r^{n-1} s.$$

The transformations r and s satisfy $rsr = s$, since



which can be rewritten as

$$sr = r^{n-1} s.$$

The dihedral group has the presentation

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, sr = r^{n-1} s \rangle.$$

For example,

$$D_3 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^2 s \rangle.$$