Elements of Group Theory

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Groups are ubiquitous in modern mathematics.

We will primarily be interested in applications of groups to the theory of congruences.

The classical results of Wilson, Fermat and Euler can all be recast as statements about the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$.

The theory of groups is extensive, and we will only develop those tools that will be useful in the context of elementary number theory.

Binary Operations

Definition

Let S be a set. A *binary operation on* S is a function $\cdot : S \times S \to S$.

Remarks. Given a binary operation $\cdot : S \times S \to S$ and $x, y \in S$:

- We usually use infix notation and write $x \cdot y$ rather than $\cdot(x, y)$.
- Depending on the operation, it is also common to abbreviate $x \cdot y$ as xy.

Examples. Addition and multiplication are binary operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

Groups

Definition

A *group* is a set G together with a binary operation which satisfies:

1. (Associativity) For all $a, b, c \in G$, $(ab)c = a(bc)$.
2. (Identity) There exists an $e \in G$ so that $ae = ea = a$ for all $a \in G$.
3. (Inverses) For each $a \in G$, there exists $b \in G$ so that $ab = ba = e$.

A group G is called *abelian* if it also satisfies:

4. (Commutativity) For all $a, b \in G$, $ab = ba$.

Examples

- $(\mathbb{Z}, +)$ is an abelian group. $(\mathbb{Z}, \times)$ is *not* a group.
- $(\mathbb{R} \setminus \{0\}, \times)$ and $(\mathbb{R}^+, \times)$ are abelian groups.
- For any $n \in \mathbb{N}$, $(\mathbb{Z}/n\mathbb{Z}, +)$ and $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ are (finite) abelian groups.
- The set

$$\mathrm{GL}_2)(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

  is a non-abelian group under matrix multiplication.
- For any nonempty set S, the set $\mathrm{Perm}(S)$ of bijections $S \to S$ is a group under function composition, non-abelian if $|S| \geq 3$.

Basic Properties of Groups

Let G be a group.

The identity element in G is unique. If $e, e' \in G$ are *both* identities, then

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

Note that we have used the "two-sided-ness" of the identity here.

Given $a \in G$, its inverse is also unique. If $b, c \in G$ are both inverses of a, then

$$b = be = b(ac) = (ba)c = ec = c.$$

Note that we have used associativity as well as the "two-sided-ness" of both inverses and the identity.

Let $a \in G$. We denote its inverse by a^{-1}.

We set $a^0 = e$ and for $n \in \mathbb{N}$ we define

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ times}},$$
$$a^{-n} = (a^{-1})^n.$$

With these definitions one can show that we have the familiar laws of exponents:

$$a^{m+n} = a^m a^n,$$
$$(a^m)^n = a^{mn},$$

for all $m, n \in \mathbb{Z}$.

Additive Groups

Sometimes it is convenient to describe a group using additive notation rather than multiplicative notation.

In this case we write $a + b$ for ab, 0 for e, and $-a$ for a^{-1}.

When using additive notation, we write

$$\underbrace{a + a + \cdots + a}_{n \text{ times}} = na$$

for $n \in \mathbb{N}$ and set $(-n)a = -(na)$. The laws of exponents become

$$(m + n)a = ma + na,$$
$$(mn)a = m(na),$$

for all $m, n \in \mathbb{Z}$.

Consider the additive group $\mathbb{Z}/n\mathbb{Z}$.

For any $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ we have

$$n(a + n\mathbb{Z}) = (na) + n\mathbb{Z} = 0 + n\mathbb{Z}.$$

Notice that $n = |\mathbb{Z}/n\mathbb{Z}|$.

This is no coincidence. It turns out that for any finite group G one has

$$a^{|G|} = e \quad \text{for all } a \in G.$$

The proof of this fact in general would take us too far afield.

However, when G is abelian we can give a very simple proof.

Translations

Let G be a group. For $a \in G$ define $L_a : G \to G$ by

$$L_a(x) = ax \quad \text{for all } x \in G.$$

L_a is called *left translation by* a.

Lemma 1

Let G be a group. For any $a \in G$, L_a is a bijection.

Proof. One can easily show that $(L_a)^{-1} = L_{a^{-1}}$ (HW). The result follows. □

Remark. The *right translation* $R_a(x) = xa$ also defines a bijection $G \to G$. However, if G is nonabelian, then $L_a \neq R_a$, in general.

Left translation will be the main tool in proving our main result.

Theorem 1

Let G be a finite abelian group. Then for any $a \in G$ one has

$$a^{|G|} = e.$$

Proof. Let

$$P = \prod_{x \in G} x,$$

the product of all of the elements in G.

Because G is abelian, the value of P is independent of how we choose to order the elements of G.

Let $a \in G$. Since $L_a : G \to G$ is a bijection,

$$P = \prod_{x \in G} x = \prod_{x \in G} L_a(x) = \prod_{x \in G} (ax).$$

Because G is abelian, in the final product we can factor out one copy of a for each $x \in G$. That is,

$$\prod_{x \in G} (ax) = a^{|G|} \prod_{x \in G} x = a^{|G|} P.$$

Hence, $P = a^{|G|} P$. Multiplication by P^{-1} on both sides finally yields

$$a^{|G|} = e.$$

Fermat's Little Theorem

Let $p \in \mathbb{N}$ be prime. Our first nontrivial application of Theorem 1 will be to the multiplicative group

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{a + p\mathbb{Z} : p \nmid a\} = \{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \ldots, (p-1) + p\mathbb{Z}\}.$$

Since $\left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p - 1$, it follows that if $p \nmid a$, then

$$(a + p\mathbb{Z})^{p-1} = a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z} \quad \Leftrightarrow \quad a^{p-1} \equiv 1 \pmod{p}.$$

This proves:

Theorem 2 (Fermat's Little Theorem)

Let $p \in \mathbb{N}$ be prime and $a \in \mathbb{Z}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

There is an equivalent formulation of Fermat's theorem that doesn't require an additional hypothesis on a.

Corollary 1

Let $p \in \mathbb{N}$ be prime. For any $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

Proof. If $p|a$, then $p|a^p$, and hence

$$a \equiv 0 \equiv a^p \pmod{p}.$$

If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem.

Multiplying both sides of this congruence by a we immediately obtain $a^p \equiv a \pmod{p}$. □

Examples

Example 1

Find the remainder when 3^{298} is divided by 7.

Solution. Since $7 \nmid 3$, Fermat's theorem tells us that

$$3^6 \equiv 1 \pmod{7}.$$

So we reduce the exponent 298 modulo 6:

$$298 = 49 \cdot 6 + 4.$$

Thus

$$3^{298} = 3^{49 \cdot 6 + 4} = (3^6)^{49} \cdot 3^4 \equiv 1^{49} \cdot 3^4 \equiv (3^2)^2 \equiv 4 \pmod{7}.$$

Hence the remainder is $\boxed{4}$. □

Example 2

Let $a \in \mathbb{Z}$. Show that if $(a, 35) = 1$, then $a^{12} \equiv 1 \pmod{35}$.

Solution. It suffices to show that

$$a^{12} \equiv 1 \pmod{5} \quad \text{and} \quad a^{12} \equiv 1 \pmod{7}.$$

(Why?)

If $(a, 35) = 1$, then $5 \nmid a$ and $7 \nmid a$. By Fermat:

$$a^{12} = (a^4)^3 \equiv 1^3 \equiv 1 \pmod{5},$$
$$a^{12} = (a^6)^2 \equiv 1^2 \equiv 1 \pmod{7},$$

which is what we needed to show. □