1 Group Theory

1.1 Groups

To learn more about algebraic geometry, we will now study group theory, a formalization of algebra which modern mathematics is built upon.

Definition 1.1.1. A *group* $(G, \star)$ is a set G, together with a law of composition $\star : G \times G \to G$ which satisfies the following conditions:

- Associativity: $(a \star b) \star c = a \star (b \star c)$ for every $a, b, c \in G$.
- Existence of identity: there exists some $e \in G$ such that $e \star g = g \star e = g$ for every $g \in G$.
- Existence of inverses: for every $g \in G$, there exists $h \in G$ such that $h \star g = g \star h = e$.

We denote the inverse of g as g^{-1}.

Example: The integers $\mathbb{Z}$ form a group under addition, since all group conditions are satisfied:

- Associativity: $(x + y) + z = x + (y + z)$ for every $x, y, z \in \mathbb{Z}$.
- Existence of identity: the integer 0 is the identity element, since $n + 0 = 0 + n = n$ for any integer n.
- Existsnce of inverses: if n is an integer, then $-n$ is the inverse of n, because $n + (-n) = (-n) + n = 0$.

We denote this group $(\mathbb{Z}, +)$.

Example: The natural numbers $\mathbb{N}$ do not form a group under addition, because

- The natural numbers do not contain the additive identity 0
- If n is a natural number, its additive inverse $-n$ is not a natural number

Example: The symmetries of a square form a group. There are 8 different ways to transform a square without changing the order of its vertices. These transformations are associative; if f, g, h are three of transformations of the square, then $(f \circ g) \circ h$ and $f \circ (g \circ h)$ yield the same transformation, where $\circ$ denotes composition.

All of these transformations are equal to a composition of 90° rotations and horizontal flips. Let us denote a 90° clockwise rotation by r, and a horizontal flip by s. Taking the group law as the composition of these two transformations (for example, $r \circ s$ is a flip followed by a 90° rotation), we can turn the set of symmetries of a square into a group.

For example, $r^2 = r \circ r$ is a 180° rotation, since it is a 90° clockwise rotation followed by another 90° clockwise rotation. The transformation s^2 does not change the state of the square, since flipping the square twice returns the square to its original position. In other words, $s^2 = e$, where e is the identity element of this group (which corresponds to 'do nothing'.) Similarly, $r^4 = e$.

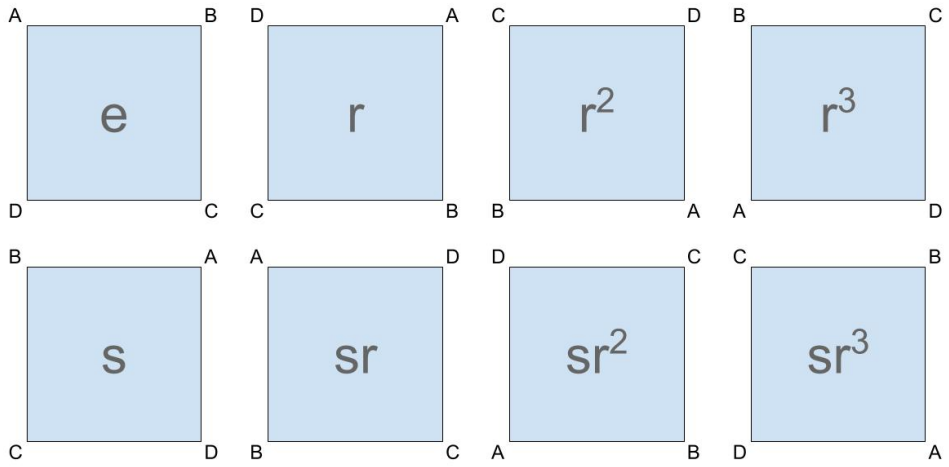

Figure 1: 8 Symmetries of a square

a \ b	e	r	r^2	r^3	s	sr	sr^2	sr^3
e	e	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	e	sr^3	s	sr	sr^2
r^2	r^2	r^3	e	r	sr^2	sr^3	s	sr
r^3	r^3	e	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	e	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	e	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	e	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	e

Figure 2: Multiplication table of D_8

This group is called the dihedral group of order 8, or D_8. In general, when we have a regular n-gon, its symmetries form the dihedral group of order $2n$, denoted D_{2n}.

The 8 elements of D_8 are $e, r, r^2, r^3, s, sr, sr^2, sr^3$. Any sequence of flips and rotations can be written as one of these eight elements, using the associativity and the relations $s^2 = e, r^4 = e$, and $rs = sr^3$. For example,

$$srs = s(rs) = s(sr^3) = (ss)r^3 = r^3.$$

We can summarize the group law on D_8 by creating a table that lists all possible products $a \circ b$ of two elements $a, b \in D_8$. This table is called the *multiplication table* of D_8

By observing the multiplication table, we observe that every element has an inverse, because every row contains the element e. For example, the inverse of sr is itself. Thus D_8 is indeed a group.

Definition 1.1.2. An *abelian group* is a group $(G, \star)$ which satisfies the following additional condition:

- Commutativity: $a \star b = b \star a$ for every $a, b \in G$.

The group of integers $(\mathbb{Z}, +)$ is an abelian group, but D_8 is not abelian; for example, $sr \neq rs$.

Example: Let n be a positive integer, and let $\mathbb{Z}/n\mathbb{Z}$ denote the set $\{0, 1, 2, \ldots, n-1\}$. We can form $\mathbb{Z}/n\mathbb{Z}$ into an abelian group using addition mod n:

$$a \star b = \big((a+b) \bmod n\big).$$

For example, if $n = 4$ then $2 \star 3 = (5 \bmod 4) = 1$.

The pair $(\mathbb{Z}/n\mathbb{Z}, \star)$ satisfies all conditions for an abelian group:

- Associativity: $(a+b)+c = a+(b+c)$ for any $a, b, c \in \mathbb{Z}$, so the remainder mod n of the left and right hand sides are equal.
- Existence of identity: the integer 0 is the identity element, since $0 \star m = m \star 0 = m$ for any $m \in \mathbb{Z}/n\mathbb{Z}$.
- Existence of inverses: if $m \in \mathbb{Z}/n\mathbb{Z}$, let $p = n - m$, where $-$ denotes subtraction of integers. Then $m \star p = m \star (n-m) = (n \bmod n) = 0$, and similarly $p \star m = 0$.
- Commutativity: $a \star b = (a+b) \bmod n = (b+a) \bmod n = b \star a$ for any $a, b \in \mathbb{Z}/n\mathbb{Z}$.

This group is called the *cyclic group of order n*. When there is no confusion, we denote this group as $(\mathbb{Z}/n\mathbb{Z}, +)$ instead of $(\mathbb{Z}/n\mathbb{Z}, \star)$.

Exercises:

1. Is $(\mathbb{Q}, +)$ a group?
2. Is $(\mathbb{Z}, \times)$ a group? (that is, the set of integers with multiplication as the group law).
3. Is $(\mathbb{Q}, \times)$ a group?

1.2 Basic Properties

To understand more about groups, we will prove some basic properties of them. Our first property comes from the observation that all groups we've seen so far have a unique identity element; this is in fact the case for any group.

Proposition 1.2.1. *A group $(G, \star)$ has a unique identity element.*

Proof. Suppose $e_1, e_2 \in G$ are both identity elements. Since e_1 is an identity, we get $e_1 \star e_2 = e_2$. But since e_2 is an identity, we also get $e_1 \star e_2 = e_1$. Thus $e_1 = e_2$. □

Another useful fact is the uniqueness of inverses.

Proposition 1.2.2. *Every group element $g \in (G, \star)$ has a unique inverse.*

Proof. Exercise. □

The next property is called the cancellation law.

Proposition 1.2.3. *Let $a, b, c \in (G, \star)$ such that $a \star c = b \star c$. Then $a = b$.*

Proof. By the associative property,

$$\begin{aligned} a \star c &= b \star c \\ a \star (c \star c^{-1}) &= b \star (c \star c^{-1}) \\ a &= b. \end{aligned}$$

□

Definition 1.2.4. The *order* of a group $(G, \star)$ is the size of the group, $|G|$.

The order of D_{2n} is $2n$. The order of $\mathbb{Z}/n\mathbb{Z}$ is n. The order of $\mathbb{Z}$ is infinite.

For an element g of a group $(G, \star)$, we will denote g^n as the n-fold power $g \star \cdots \star g$. We have seen this notation when discussing the dihedral group.

Definition 1.2.5. Let $(G, \star)$ be a group with identity e. The *order* of an element $g \in G$ is the smallest integer n such that $g^n = e$. If no such integer exists, then g has infinite order.

The element $r \in D_8$ has order 4, because $r^4 = e$ but none of r, r^2, r^3 is the identity. The element $s \in D_8$ has order 2.

The element $[1] \in \mathbb{Z}/n\mathbb{Z}$ always has order n. The element $[2] \in \mathbb{Z}/3\mathbb{Z}$ has order 3, because $[2] + [2] + [2] = [0]$, but $[2] \neq [0]$ and $[2] + [2] = [1] \neq [0]$.

The element $0 \in \mathbb{Z}$ has order 1. All other elements of $\mathbb{Z}$ have infinite order.

Since the identity of a group is unique, every group has a unique element of order 1.

Exercises:

1. Prove proposition 1.2.2.
2. What are the elements of order 2 in D_8?

1.3 Subgroups

Definition 1.3.1. Let $(G, \star)$ be a group. A subset $H \subseteq G$ is a *subgroup* of G if H satisfies the following conditions:

- Closure under group law: if $a, b \in H$, then $a \star b \in H$.
- Contains identity: if e is the identity of G, then $e \in H$.
- Contains all inverses: if $h \in H$, then $h^{-1} \in H$.

We will write $H \leq G$ to denote that H is a subgroup of G.

Example: Consider the group $(\mathbb{Z}, +)$. The subset of even integers $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ is a subgroup of $\mathbb{Z}$, because it satisfies all subgroup conditions:

- Closure under group law: if $a, b \in 2\mathbb{Z}$ are both even, then their sum $a + b$ is also even, so $a + b \in 2\mathbb{Z}$.

- Contatins identity: 0 is an even integer.
- Constains all inverses: if $n \in 2\mathbb{Z}$, then its inverse $-n$ is also an even integer, so $-n \in 2\mathbb{Z}$.

In notation, $2\mathbb{Z} \leq \mathbb{Z}$.

The subset $\{-1, 0, 1\}$ is not a subgroup of $\mathbb{Z}$, even though it contains the identity and is closed under inverses, because it is not closed under addition: $1 + 1 = 2$ is not in the set.

The subset $\mathbb{N}$ is not a subgroup of $\mathbb{Z}$, since $\mathbb{N}$ does not contain all inverses. Indeed for $H \subseteq G$ to be a subgroup, H must be a group on its own.

In fact, the only subgroups of $\mathbb{Z}$ are $\{0\}$ and $n\mathbb{Z}$ for positive integers n, where $n\mathbb{Z}$ denotes multiples of n.

Example: The group D_8 has a total of subgroups, which are

- 1 subgroup of order 1: $\{e\}$
- 5 subgroups of order 2: $\{e, r^2\}, \{e, sr\}, \{e, sr^2\}, \{e, sr^3\}$
- 3 subgroups of order 4: $\{e, r, r^2, r^3\}, \{e, s, r^2, sr^2\}, \{e, sr, r^2, sr^3\}$
- 1 subgroup of order 8: D_8.

Example: Consider the group $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. The even integers $\{0, 2\}$ forms a subgroup called $2\mathbb{Z}/4\mathbb{Z}$. But in $\mathbb{Z}/5\mathbb{Z}$, the even integers $\{0, 2, 4\}$ do not form a subgroup, as $2 + 4 = 1$ is not even.

In general, if m is an integer that divides n, then the multiples of m in $\mathbb{Z}/n\mathbb{Z}$ forms a subgroup (exercises). We usually denote this subgroup as $m\mathbb{Z}/n\mathbb{Z}$. In particular, if n is a prime number, then the only subgroups of $\mathbb{Z}/n\mathbb{Z}$ are $\{0\}$ and itself.

Definition 1.3.2. Let $g_1, \ldots, g_n$ be elements of an abelian group G. The *subgroup generated by* $g_1, \ldots, g_n$ is the set

$$\langle g_1, \ldots, g_n \rangle = \{g_1^{e_1} \cdots g_n^{e_n} : e_1, \ldots, e_n \in \mathbb{Z}\}.$$

When the exponent e_i is negative, we mean the $-e_i$-th power of the inverse of g_i, $g_i^{e_i} = (g_i^{-1})^{e_i}$. If $e_i = 0$, then $g_i^{e_i} = e$, where e is the identity of G.

The set $H = \langle g_1, \ldots, g_n \rangle$ is indeed a subgroup of G:

- Closure under group law: if $g_1^{e_1} \cdots g_n^{e_n}, g_1^{f_1} \cdots g_n^{f_n}$ are two elements of H, then

  $$(g_1^{e_1} \cdots g_n^{e_n})(g_1^{f_1} \cdots g_n^{f_n}) = g_1^{e_1+f_1} \cdots g_n^{e_n+f_n}$$

  because G is abelian.
- Contains identity: exercise.
- Contains all inverses: exercise.

Example: In the group of integers, $\langle 1 \rangle = \mathbb{Z}$, and $\langle 2 \rangle = 2\mathbb{Z}$. In general, $\langle n \rangle = n\mathbb{Z}$. The subgroup $\langle 2, 3 \rangle = \mathbb{Z}$, because $1 = 3 - 2 \in \langle 2, 3 \rangle$, and thus $\langle 1 \rangle \subseteq \langle 2, 3 \rangle$.

The subgroup $\langle g_1, \ldots, g_n \rangle \subseteq G$ is the smallest subgroup of G containing $g_1, \ldots, g_n$; if $H \leq G$ contains $g_1, \ldots, g_n$, then it must contain all $g_1^{e_1} \cdots g_n^{e_n}$ since H is closed under the group law.

Proposition 1.3.3. *Let $g \in G$ be an element of order r. Then $\langle g \rangle$ is a subgroup of order r.*

Proof. The elements of $\langle g \rangle$ are of form g^n, where n is an integer. The elements $g^0, g^1, \ldots, g^{r-1}$ are distinct; otherwise, if $g^a = g^b$ for some $0 \leq a < b < r$, then $g^{b-a} = e$, which contradicts that r is the order of g.

Now for any integer n, we can write $n = rq + d$, where q is an integer and $0 \leq d < r - 1$. Since g is order r, it follows that

$$g^n = g^{rq+d} = (g^r)^q g^d = g^d.$$

Thus g^n equals one of $g^0, \ldots, g^{n-1}$, and $\langle g \rangle = \{g^0, \ldots, g^{r-1}\}$. It follows that $|\langle g \rangle| = r$. □

Example: Consider the rotation $r \in D_8$. Then the order of r is 4, so $\langle r \rangle = \{e, r, r^2, r^3\}$, and the order of $\langle r \rangle$ is 4. Generally, $r \in D_{2n}$ generates the group $\langle r \rangle$ of order n.

A group generated by a single element is called a *cyclic group.*

Exercises:

1. Finish the proof that $\langle g_1, \ldots, g_n \rangle$ is a subgroup of G.
2. The set of integers $\mathbb{Z}$ is a subgroup of the set of rationals $\mathbb{Q}$ under addition. What is an example of a group $G \neq \mathbb{Z}, \mathbb{Q}$ such that $\mathbb{Z} \leq G \leq \mathbb{Q}$?

1.4 Maps between groups

Definition 1.4.1. Let $(G, \star), (H, *)$ be groups. A function $\varphi : G \to H$ is a *group homomorphism* if $\varphi(a \star b) = \varphi(a) * \varphi(b)$ for every $a, b \in G$.

Example: The function $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined $\varphi(n) = 2n$ is a group homomorphism. If a, b are integers, then $\varphi(a + b) = 2(a + b) = 2a + 2b = \varphi(a) + \varphi(b)$ by the distributive property.

The function $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined $\varphi(n) = n + 1$ is not a group homomorphism. For example, $\varphi(0 + 0) = 0 + 0 + 1 = 1$, but $\varphi(0) + \varphi(0) = (0 + 1) + (0 + 1) = 2$. Thus $\varphi(0 + 0) \neq \varphi(0) + \varphi(0)$.

Example: Let $(G, \star)$ and $(H, *)$ be any groups, and let 0_H denote the identity of H. The *zero map* $\varphi : G \to H$ defined $\varphi(g) = 0_H$ for every $g \in G$ is a group homomorphism. For any $g_1, g_2 \in G$, we have

$$\varphi(g_1 \star g_2) = 0_H = 0_H * 0_H = \varphi(g_1) * \varphi(g_2).$$

Only a few special functions are group homomorphisms; for example, we will show that a group homomorphism always maps the identity of the domain to the identity of the codomain.

Proposition 1.4.2. *Let $(G, \star)$ and $(H, *)$ be groups, with identity elements $0_G \in G$ and $0_H \in H$. If $\varphi : G \to H$ is a group homomorphism, then $\varphi(0_G) = 0_H$.*

Proof. Since φ is a group homomorphism, $\varphi(0_G \star 0_G) = \varphi(0_G) * \varphi(0_G)$. But $0_G \star 0_G = 0_G$, so

$$\varphi(0_G) = \varphi(0_G \star 0_G) = \varphi(0_G) * \varphi(0_G).$$

By the cancellation law, $\varphi(0_G) = 0_H$. □

Now we can show that the only group homomorphisms $\varphi : \mathbb{Z} \to \mathbb{Z}$ are of the form $\varphi(n) = rn$, where r is an integer. In other words, the only group homomorphisms from $\mathbb{Z}$ to itself are multiplication by integers. To see why this is true, suppose we have a group homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$. Let $r = \varphi(1)$. Since

$$r + \varphi(-1) = \varphi(1) + \varphi(-1) = \varphi(1 + (-1)) = \varphi(0) = 0,$$

subtraction gives $\varphi(-1) = -r$. Now for any positive integer n, we can write $n = 1 + \cdots + 1$, and thus

$$\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = r + \cdots + r = rn.$$

Similarly, $\varphi(-n) = r(-n)$. If $n = 0$, then $\varphi(0) = 0$.

Definition 1.4.3. A bijective group homomorphism $\varphi : G \to H$ is called an *isomorphism*. If there exists an isomorphism $\varphi : G \to H$, we say G and H are *isomorphic* and write $G \simeq H$.

Example: We saw that the map $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ defined $\varphi(n) = 2n$ is a group homomorphism. This map is injective; if $\varphi(a) = \varphi(b)$ for integers $a, b \in \mathbb{Z}$, then $2a = 2b$, so $a = b$. This map is also surjective, since the range of φ is the even integers, $2\mathbb{Z}$. Therefore, φ is a group isomorphism. The groups $\mathbb{Z}$ and $2\mathbb{Z}$ are isomorphic, that is, $\mathbb{Z} \simeq 2\mathbb{Z}$.

Two isomorphic groups have the "same" group structure. The example above shows that $\mathbb{Z}$ and $2\mathbb{Z}$ can be seen as the same group, by relabeling $n \mapsto 2n$.

Example: Let $r \in D_8$ be a 90° rotation, and consider the group $\langle r \rangle$. Since r is an element of order 4, the group $\langle r \rangle$ is a group of order 4, consisting of elements e, r, r^2, r^3.

The groups $\langle r \rangle$ and $\mathbb{Z}/4\mathbb{Z}$ are isomorphic. The isomorphism is given by the map $\varphi : \mathbb{Z}/4\mathbb{Z} \to \langle r \rangle$, defined

$$\varphi(n) = r^n.$$

This map is a group homomorphism, as

$$\varphi(a + b) = r^{a+b} = r^a r^b = \varphi(a)\varphi(b).$$

The map φ is injective; if $\varphi(a) = \varphi(b)$, then $r^a = r^b$, So $r^{a-b} = e$. Since r is an element of order 4, this means $a - b$ is a multiple of 4. Thus $a - b \equiv 0 \bmod 4$, and $a \equiv b \bmod 4$.

The map φ is also surjective, since $0, 1, 2, 3$ are mapped to e, r, r^2, r^3, respectively.

Alternatively, we observe that $\mathbb{Z}/4\mathbb{Z} = \langle 1 \rangle$, where 1 is an element of order 4 in $\mathbb{Z}/4\mathbb{Z}$. Thus $\mathbb{Z}/4\mathbb{Z}$ and $\langle r \rangle$ are both cyclic groups generated by an element of order 4.

Exercises:

1. Prove the following: if $\varphi : G \to H$ is a group homomorphism, then for every $g \in G$,

   $$\varphi(g^{-1}) = (\varphi(g))^{-1}.$$

   In the example $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ defined $\varphi(n) = 2n$, we indeed find $-(2n) = 2(-n)$.

2. Let $G = \{-1, 1\}$. The set G can be turned into a group under multiplication.
   Show that $(G, \times) \simeq (\mathbb{Z}/2\mathbb{Z}, +)$.

1.5 Kernel and Image

Two special subgroups associated with a group homomorphism is the kernel and image.

Definition 1.5.1. The *kernel* of a group homomorphism $\varphi : G \to H$ is the set

$$\ker G = \{g \in G : \varphi(g) = 0_H\}.$$

In other words, $\ker \varphi$ is the set of elements which get mapped to the identity under φ.

Example: Let $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be the homomorphism

$$\varphi(n) = (n \bmod 2).$$

The kernel of φ is the set of elements of $\mathbb{Z}$ mapped to $0 \in \mathbb{Z}/2\mathbb{Z}$, which are the even integers. Thus $\ker \varphi = 2\mathbb{Z}$.

Proposition 1.5.2. *The kernel of a homomorphism $\varphi : G \to H$ is a subgroup of G.*

Proof.

- Closure under group law: if g_1, g_2 are two elements of $\ker G$, then

  $$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = 0_H 0_H = 0_H.$$

  Thus $g_1 g_2 \in \ker G$.
- Contains identity: $\varphi(0_G) = 0_H$, so $0_G \in \ker G$.
- Contains all inverses: if $g \in \ker G$, then $\varphi(g^{-1}) = (\varphi(g))^{-1} = 0_H^{-1} = 0_H$.

□

Definition 1.5.3. The *image* of a group homomorphism $\varphi : G \to H$ is the set

$$\mathrm{im}(\varphi) = \{\varphi(g) : g \in G\}.$$

In other words, $\mathrm{im}(\varphi)$ is the set of elements of H that are mapped to from G.

Example: Let $\varphi : \mathbb{Z} \to \mathbb{Z}$ be the homomorphism $\varphi(n) = 2n$. Then the image of φ is

$$\{\varphi(n) : n \in \mathbb{Z}\} = \{2n : n \in \mathbb{Z}\} = 2\mathbb{Z}.$$

Proposition 1.5.4. *The image of a homomorphism $\varphi : G \to H$ is a subgroup of H.*

Proof. Exercise. □

The kernel controls the behavior of the homomorphism; in particular, it is a useful tool to determine if a function is injective.

Exercises:

1. Prove that the image of a group homomorphism $\varphi : G \to H$ is a subgroup of H.
2. (a) Let $\varphi : G \to H$ be a group homomorphism. Prove that if $\varphi(a) = \varphi(b)$ for some a and b in G, then ab^{-1} is in $\ker \varphi$.
   (b) Prove that if the kernel of a group homomorphism φ is the set $\{0\}$, then φ is injective.

1.6 Lagrange's Theorem

A very useful theorem that connects group theory with number theory is Lagrange's theorem; we will omit the proof of this result.

Theorem 1.6.1 (Lagrange)**.** *If G is a finite group, the order of every subgroup of G divides the order of G.*

That is, if H is a subgroup of G, then $|H|$ divides $|G|$.

We will prove the following theorem, commonly known as "Fermat's Little Theorem."

Theorem 1.6.2 (Fermat)**.** *Let p be a prime number. For any integer a, the number $a^p - a$ is a multiple of p.*

In other words, if p is prime and a is an integer, then $a^p \equiv a \bmod p$. The following is a useful lemma from number theory.

Proposition 1.6.3. *Let p be a prime number, and a an integer that is not a multiple of p. Then $a, 2a, 3a, \ldots, (p-1)a$ are distinct mod p.*

Proof. Exercises. □

For example, if $p = 5$ and $a = 2$, then

$$2 \equiv 2, 2 \times 2 \equiv 4, 3 \times 2 \equiv 1, 4 \times 2 \equiv 3.$$

Using this lemma, we can introduce a new group to our family of examples, the multiplicative group mod p.

Let $(\mathbb{Z}/p\mathbb{Z})^*$ be the set $\{1, 2, 3, \ldots, p-1\}$. In other words, $(\mathbb{Z}/p\mathbb{Z})^*$ is the set $\mathbb{Z}/p\mathbb{Z}$ without the element zero. Define a group operation on $(\mathbb{Z}/p\mathbb{Z})^*$ by multiplication, that is,

$$a \times b = (ab) \bmod p.$$

For example, in the group $(\mathbb{Z}/3\mathbb{Z})^* = \{1, 2\}$, we have $2 \times 2 = 4 \bmod 3 = 1$.

Proposition 1.6.4. *$(\mathbb{Z}/p\mathbb{Z})^*$ is a group under multiplication.*

Proof.

- Associativity: multiplication is associative in modular arithmetic.
- Existence of identity: 1 is the identity, since $1 \times n \equiv n \bmod p$ for any $n \in (\mathbb{Z}/p\mathbb{Z})^*$.
- Existence of inverses: Let $n \in (\mathbb{Z}/p\mathbb{Z})^*$. By our lemma, $n, 2n, 3n, \ldots, (p-1)n$ are each distinct modulo p. Since these $p-1$ values all lie in $\{1, 2, \ldots, p-1\}$ and are each distinct, exactly one value of k must yield $kn \equiv 1 \bmod p$. Thus k is the inverse of p.

□

In the example with $p = 5$ and $a = 2$, we find $3 \times 2 \equiv 1 \bmod 5$, so 3 is the inverse of 2.

The reason we remove 0 in $(\mathbb{Z}/p\mathbb{Z})^*$ is because 0 does not have an inverse under multiplication; there does not exist $n \in \mathbb{Z}/p\mathbb{Z}$ such that $0 \times n = 1$.

Now we are ready to prove Fermat's little theorem, in the exercises.

Exercises:

1. Prove proposition 1.6.3.
2. Let $a \in (\mathbb{Z}/p\mathbb{Z})^*$, and let $\langle a \rangle$ be the subgroup generated by a. If $|\langle a \rangle| = k$, why is $a^k \equiv 1 \bmod p$?
3. Prove Fermat's little theorem, using Lagrange's theorem with $G = (\mathbb{Z}/p\mathbb{Z})^*$ and its subgroup $\langle a \rangle$.