1 Jan 7: Elementary number theory

The goal of this lecture is to prove Fermat's little theorem.

Theorem 1.1. *Let p be a prime, and let a be any integer. Then $a^p - a$ is divisible by p.*

1.1 Modular arithmetic [2.7, 2.9]

An *equivalence relation* on a set S is a relation $\sim$ between certain pairs of elements of S. We write $a \sim b$ if a and b are *equivalent*. An equivalence relation is required to be

- *transitive*: if $a \sim b$ and $b \sim c$, then $a \sim c$.
- *symmetric*: if $a \sim b$, then $b \sim a$.
- *reflexive*: for all a, $a \sim a$.

An equivalence relation $\sim$ partitions S into *equivalence classes*.

Definition 1.2. Let n be a positive integer. For integers a, b, we write

$$a \equiv b \pmod{n}$$

if $a - b$ is divisible by n, i.e., $a - b = nk$ for some integer k.

Lemma 1.3 (Addition and multiplication modulo n)**.** *If $a' \equiv a \pmod{n}$ and $b' \equiv b \pmod{n}$, then $a' + b' \equiv a + b \pmod{n}$ and $a'b' \equiv ab \pmod{n}$.*

Proof. Suppose $a' = a + nk$ and $b' = b + n\ell$. Then

$$a' + b' = (a + b) + n(k + \ell),$$

and

$$a'b' = ab + n(a\ell + bk + k\ell).$$ □

Definition 1.4. Let $\mathbb{Z}/n\mathbb{Z}$ denote the set of equivalence classes of $\mathbb{Z}$ with respect to the equivalence relation $\equiv$. These equivalence classes are also referred to as *congruence classes* modulo n.

By the lemma above, addition and multiplication of congruence classes modulo n is well-defined. If we write $\overline{a}$ to denote the congruence class of a, then

$$\overline{a} + \overline{b} = \overline{a + b},$$

and similarly

$$\overline{a}\overline{b} = \overline{ab}.$$

The associative, commutative, and distributive laws carry over for addition and multiplication of elements of $\mathbb{Z}/n\mathbb{Z}$.

Example 1.5. $\mathbb{Z}/6\mathbb{Z}$ has 6 elements. The elements $\overline{2}$ and $\overline{8}$ are the same element since $2 \equiv 8 \pmod{6}$.

We have $\overline{2} \cdot \overline{5} = \overline{10}$, and $\overline{8} \cdot \overline{5} = \overline{40}$. Fortunately, $\overline{10} = \overline{40}$ since $10 \equiv 40 \pmod{6}$. We usually take the remainder when divided by 6 and say $\overline{2} \cdot \overline{5} = \overline{4}$.

1.2 Bezout's lemma [2.3]

We recall division with remainder: let n be an integer, and let a be a positive integer. Then there exists an integer q and an integer $0 \leq r < a$ such that

$$n = aq + r.$$

Definition 1.6. Let a and b be integers, not both zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the largest integer which divides both a and b. If $\gcd(a, b) = 1$, we say that a and b are *coprime* or *relatively prime*.

The GCD satisfies the property that

$$\gcd(a, b) = \gcd(a + bk, b)$$

for any integer k. Indeed, if d divides both a and b, then d divides both $a + bk$ and b, and conversely.

As such, we can compute GCD's using the *Euclidean algorithm*, which works by repeated division with remainder.

Example 1.7. For example, for $a = 314$, $b = 136$, since

$$314 = 2 \cdot 136 + 42, \quad 136 = 3 \cdot 42 + 10, \quad 42 = 4 \cdot 10 + 2,$$

we have

$$\gcd(314, 136) = \gcd(42, 136) = \gcd(42, 10) = \gcd(2, 10) = 2.$$

Proposition 1.8 (Bezout's lemma)**.** *For any integers a and b, not both zero, there exist integers r and s such that*

$$\gcd(a, b) = ra + sb.$$

Proof. Let $d = \gcd(a, b)$ Let ℓ be the smallest positive integer that can be expressed as

$$\ell = ra + sb$$

for some r and s.

We claim that $\ell | a$. Use division with remainder to write

$$a = \ell q + m$$

for $0 \leq m < \ell$. Then m can also be expressed in the form $ra + sb$:

$$m = a - \ell q = a - q(ra + sb) = (1 - qr)a - (qs)b.$$

Since ℓ was assumed to be minimal, $m = 0$, so $\ell | a$.

Similarly, $\ell | b$, so ℓ divides both a and b. Since d is the greatest common divisor,

$$\ell \leq d.$$

On the other hand, d divides both ra and sb, so d also divides ℓ, so

$$d \leq \ell.$$

Thus, $\ell = d$. □

Corollary 1.9. *Let e be an integer which divides both a and b. Then e divides* $\gcd(a, b)$.

Proof. Let

$$\gcd(a, b) = ra + sb.$$

Since e divides both terms on the right hand side, it also divides $\gcd(a, b)$. □

Corollary 1.10. *Let p be a prime, and let a and b be integers. If $p|ab$, then $p|a$ or $p|b$.*

Proof. Suppose that p divides ab, but p does not divide a.

Since p is prime, $\gcd(a, p) = 1$, so by Bezout's lemma there exist $r, s \in \mathbb{Z}$ such that

$$1 = ra + sp.$$

Multiplying both sides by b,

$$b = rab + spb.$$

Both terms on the right are multiples of p by the assumption $p|ab$, so $p|b$. □

Corollary 1.11 ($\mathbb{Z}/p\mathbb{Z}$ has inverses)**.** *Let p be a prime, and let a be an integer which is not divisible by p. There exists an integer b such that $ab \equiv 1 \pmod{p}$.*

Proof. As in the proof above, there exist $r, s \in \mathbb{Z}$ such that

$$1 = ra + sp.$$

So $ra \equiv 1 \pmod{p}$. Clearly, we can take $b = r$. □

1.3 Proof of Fermat's little theorem

Proof. If a is divisible by p, then it is apparent that $a^p - a$ is divisible by p. Assume $p \nmid a$.

1. Consider the set
$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$
of nonzero congruence classes modulo p. Then consider the set
$$\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$$
of congruence classes modulo p.

2. We claim that they're the same set. Indeed, since both sets have $p - 1$ elements, we just need to show that $\overline{j}$ appears in the second set for every $j \in \{1, \ldots, p-1\}$.

   In other words, we want $ka \equiv j \pmod{p}$ for some $k \not\equiv 0 \pmod{p}$. Let b be such that $ab \equiv 1 \pmod{p}$, and let $k = jb$. Then
   $$ka \equiv jba \equiv j \pmod{p}.$$
   Obviously $k \not\equiv 0 \pmod{p}$ since $j \not\equiv 0 \pmod{p}$.

3. Then

$$\begin{aligned} 1 \cdot 2 \cdots (p-1) &\equiv a \cdot (2a) \cdots (p-1)a \\ &\equiv 1 \cdot 2 \cdots (p-1) \cdot a^{p-1} \pmod{p}. \end{aligned}$$

Multiplying both sides by an inverse of $(p-1)!$ gives

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

1.4 $(\mathbb{Z}/n\mathbb{Z})^\times$

Corollaries 1.10 and 1.11 are not true if p is not prime. For example, $4|2 \cdot 2$ but 4 does not divide 2, and there is no integer b such that $2b \equiv 1 \pmod 4$, because $2b$ cannot be odd.

Here are some generalizations of them to general n.

Lemma 1.12. *Suppose n be a positive integer. If $n|ab$, then b is a multiple of $n/\gcd(a,n)$.*

Proof. Let $d = \gcd(a,n)$. Suppose

$$d = ra + sn.$$

Then $db = rab + snb$ is a multiple of n, so b is a multiple of n/d. □

Lemma 1.13. *Let n be a positive integer, and a be an integer such that $\gcd(a,n) = 1$. There exists an integer b such that $ab \equiv 1 \pmod n$.*

Proof. Since $\gcd(a,n) = 1$, there exist $r, s \in \mathbb{Z}$ such that

$$1 = ra + sn.$$

So $ra \equiv 1 \pmod p$, and we can take $b = r$. □

Definition 1.14. Let $(\mathbb{Z}/n\mathbb{Z})^\times$ denote the set of congruence classes $\overline{a}$ modulo n such that $\gcd(a,n) = 1$. Note that this does not depend on the choice of a, only on $a \pmod n$, since $\gcd(a + nk, n) = \gcd(a,n)$ as mentioned previously.

Definition 1.15. In the special case when $n = p$ is a prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ is just all of the elements of $\mathbb{Z}/p\mathbb{Z}$ other than $\overline{0}$.

1.5 Least common multiple

Definition 1.16. Let a and b be integers, both not zero. The *least common multiple* of a and b, denoted $\operatorname{lcm}(a,b)$ is the smallest positive integer which is a multiple of both a and b.

Proposition 1.17. *Let a and b be positive integers. If $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$, then $ab = dm$.*

Proof. Suppose $m = ak$. Since $b|m$, by Lemma 1.12, $k \geq b/d$, so $m \geq ab/d$. On the other hand, it is clear that ab/d is a multiple of both a and b, so $m \leq ab/d$. □

2 Jan 12: Basic group theory definitions

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

Definition 2.1 (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 2.2. 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 2.3 (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 2.4. *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 $b = c$.

□

Example 2.5.

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

Example 2.7. 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 2.8. 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 2.9. 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 2.10. 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 $(1_G, 1_{G'})$.

2.2 Permutations [1.5]

Definition 2.11. A *permutation* (of length n) is a bijective map $\sigma\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

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 2.12. 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 2.13. The group of permutations of the set $\{1, 2, \ldots, n\}$ is called the *symmetric group* and denoted S_n. It has order $n!$

Example 2.14. 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,

$$x^3 = 1, \quad y^2 = 1. \tag{♡}$$

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

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

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

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

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

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

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

2.3 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 2.15. 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 2.16. *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 2.17. 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 2.18 (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 2.19. *In a finite group G, the order of every element divides $|G|$.*

3 Jan 14: Homomorphisms and isomorphisms

3.1 Dihedral group

Let $A_1A_2\cdots A_n$ be a regular n-gon, with center O. The *dihedral group* D_n consists of the symmetries of the regular n-gon. It has order

$$|D_n| = 2n.$$

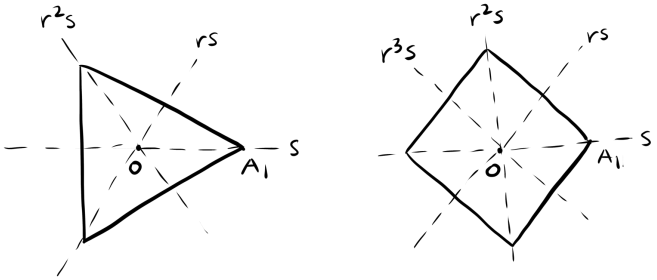
- There are n rotations in D_n. Let r denote rotation by $2\pi/n$ around O. It satisfies

  $$r^n = 1.$$

  The other rotations are

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

- There are n reflections in D_n.



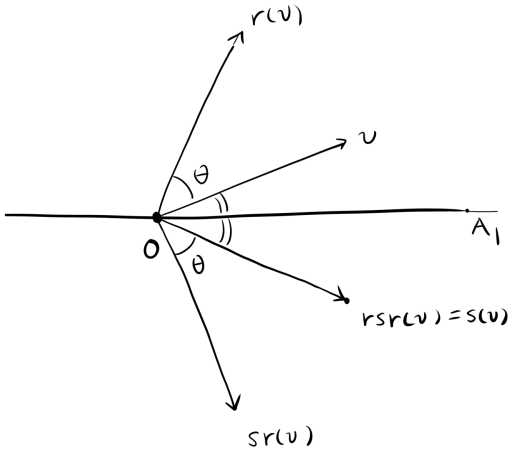
  Let s denote reflection across OA_1. It satisfies

  $$s^2 = 1.$$

  The other reflections are

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

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,

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

3.2 Definitions [2.5, 2.6]

Definition 3.1. Let G and G' be groups. A *homomorpmism* is a map $\varphi\colon G \to G'$ such that

$$\varphi(ab) = \varphi(a)\varphi(b)$$

for all $a, b \in G$. The product ab is taken in G, and the product $\varphi(a)\varphi(b)$ is taken in G'.

In other words, a homomorphism is a map which is compatible with the laws of composition on G and G'.

Proposition 3.2. *Let $\varphi\colon G \to G'$ be a homomorphism.*

1. *It maps the identity to the identity: $\varphi(1_G) = \varphi(1_{G'})$.*
2. *It maps inverses to inverses: $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

Proof. Since φ is a homomorphism,

$$\varphi(1_G)\varphi(1_G) = \varphi(1_G),$$

so $\varphi(1_G) = 1_{G'}$. In addition,

$$\varphi(a^{-1})\varphi(a) = \varphi(1_G) = 1_{G'},$$

so $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Definition 3.3. A homomorphism $\varphi\colon G \to G'$ is an *isomorphism* if it is bijective.

We say that two groups G and G' are *isomorphic* if there exists an isomorphism $\varphi\colon G \to G'$.

Example 3.4. The map $\varphi\colon \mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^\times$ given by

$\overline{a}$	0	1	2	3	4	5	(mod 6)
$\varphi(\overline{a})$	1	3	2	6	4	5	(mod 7)

is an isomorphism. It is bijective by the chart above. It is a homomorphism because it is actually given by

$$\varphi(\overline{a}) \equiv 3^a \pmod 7,$$

so

$$\varphi(\overline{a}+\overline{b}) = \overline{3^{a+b}} = \overline{3^a}\cdot\overline{3^b} = \varphi(\overline{a})\varphi(\overline{b}).$$

It is well defined by Fermat's little theorem, because

$$3^{a+6k} \equiv 3^a \pmod 7$$

since $3^6 \equiv 1 \pmod 7$, so $3^a \pmod 7$ only depends on $a \pmod 6$.

3.3 Sign of permutations [1.5]

A *permutation matrix* is an $n \times n$ matrix with entries in $\{0, 1\}$, which has exactly one 1 in each row and column. Every permutation matrix has determinant equal to ± 1.

Definition 3.5. Given a permutation σ, the associated permutation matrix is the matrix with

$$P_{\sigma(i),i} = 1$$

for $1 \le i \le n$, and 0 in all other entries. This is the unique matrix with the property

$$P\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{bmatrix}.$$

Example 3.6. If $\sigma = (123)$, then the associated permutation matrix P is below and satisfies

$$PX = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix}.$$

Definition 3.7. The *sign* of σ is the determinant $\det P = \pm 1$ of its permutation matrix.

Proposition 3.8. *If σ and τ are permutations with associated permutation matrices P and Q, then the permutation matrix of $\sigma\tau$ is PQ.*

Corollary 3.9. *The map* $\operatorname{sign}\colon S_n \to \{\pm 1\}$ *sending σ to its sign is a homomorphism of groups. (Here $\{\pm 1\}$ is a group under multiplication.)*

3.4 Kernel and image [2.5]

Definition 3.10. Let $\varphi\colon G \to G'$ be a homomorphism of groups. The *image* of φ is

$$\operatorname{im}(\varphi) = \{x \in G' : x = \varphi(a) \text{ for some } a \in G\}.$$

The *kernel* of φ is

$$\ker(\varphi) = \{a \in G : \varphi(a) = 1_{G'}\}.$$

Lemma 3.11. *The kernel and image of a homomorphism $\varphi\colon G \to G'$ are subgroups of G and G', respectively.*

Proof. We verify closure in each case and omit the verification of the other axioms.

1. Suppose $x, y \in \operatorname{im}(\varphi)$. Then $x = \varphi(a)$, $y = \varphi(b)$ for some $a, b \in G$. So $xy = \varphi(ab)$ is also in $\operatorname{im}(\varphi)$.
2. Suppose $a, b \in \ker(\varphi)$. Then $\varphi(ab) = \varphi(a)\varphi(b) = 1_{G'} \cdot 1_{G'} = 1_{G'}$, so $ab \in \ker(\varphi)$. □

Lemma 3.12. *A homomorphism $\varphi\colon G \to G'$ is injective if and only if* $\ker(\varphi)$ *is the trivial subgroup* $\{1_G\}$.

Proof. First suppose φ is injective. Since $\varphi(1_G) = 1_{G'}$, this means that if $\varphi(a) = 1_{G'}$, then $a = 1_G$, so $\ker(\varphi)$ is the trivial subgroup.

Now, suppose $\ker(\varphi) = \{1_G\}$. If $\varphi(a) = \varphi(b)$ for some $a, b \in G$, then

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1_{G'}.$$

Thus, $ab^{-1} = 1_G$, so $a = b$. □

Example 3.13. Consider the map

$$\varphi\colon \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},$$

which sends

$$\overline{a} \mapsto (\overline{a}, \overline{a}).$$

One can check that this is well-defined and a homomorphism.

The kernel of φ consists of all congruence classes $\overline{a}$ such that

$$a \equiv 0 \pmod 3 \text{ and } a \equiv 0 \pmod 5.$$

Since 3 and 5 are relatively prime, this implies that $a \equiv 0 \pmod{15}$, so $\ker(\varphi)$ is trivial.

The lemma then tells us that φ is injective. Both the target and the source have 15 elements, so φ is bijective, and thus it is an isomorphism.

3.5 Normal subgroups

However, not every subgroup of G can be the kernel of some homomorphism! The kernel always has the following property.

Definition 3.14. Let $a, g \in G$. The element gag^{-1} is called the *conjugate* of a by g. We say that two elements a and a' are *conjugate* if there exists $g \in G$ such that $a' = gag^{-1}$.

Definition 3.15 (Normal subgroup)**.** A subgroup N of G is *normal* if for all $a \in N$ and all $g \in G$, the conjugate gag^{-1} is also in N.

Proposition 3.16. *The kernel of a homomorphism $\varphi\colon G \to G'$ is normal.*

Proof. Suppose $a \in \ker(\varphi)$. For any $g \in G$, we have

$$\varphi(gag^{-1}) = \varphi(g) \cdot 1_{G'} \cdot \varphi(g)^{-1} = 1_{G'}. \qquad \square$$

Example 3.17.

1. If G is abelian, then every subgroup is normal, because $gag^{-1} = a$ for all a, g.
2. In general, the *center* of a group G is

   $$\{z \in G : zg = gz \quad \forall g \in G\}.$$

   It is always a normal subgroup of G.
3. $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$ since it is the kernel of the homomorphism $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$. (Here, $\mathbb{R}^\times$ denotes the group of nonzero real numbers under multiplication.)

Example 3.18. Recall our usual presentation

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

The cyclic subgroup generated by y, which consists of the elements $\{1, y\}$, is not normal. This is because

$$xyx^{-1} = xyx^2 = x(x^2y)x = xx^2(x^2y) = x^2y,$$

which is not in $\{1, y\}$.

3.6 Isomorphism classes [2.5]

Lemma 3.19. *If $\varphi\colon G \to G'$ is an isomorphism, then its inverse $\varphi^{-1}\colon G' \to G$ is also an isomorphism.*

As mentioned earlier, we say that G and G' are isomorphic if there exists an isomorphism $\varphi\colon G \to G'$. The *isomorphism class* of G consists of all groups isomorphic to G.

Example 3.20. Suppose $x \in G$ is an element of order n. The cyclic subgroup $\langle x \rangle$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. The map

$$\varphi(\overline{a}) = x^a$$

is an isomorphism $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \langle x \rangle$.

Example 3.21. The groups S_3 and D_3 are isomorphic since they both have the presentation

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

4 Jan 21: Cosets

4.1 Cosets [2.6, 2.8]

Definition 4.1 (Left cosets)**.** Let H be a subgroup of a group G. Let a be any element of G. We denote by aH the set

$$aH \coloneqq \{g \in G : g = ah \text{ for some } h \in H\}.$$

In other words, $aH = \{ah : h \in H\}$. This set is called a *left coset* of H.

Example 4.2. Let G be the additive group $\mathbb{Z}$, and let $H = 100\mathbb{Z}$ be the set of all multiples of 100, i.e.,

$$H = \{\dots, -200, -100, 0, 100, 200, \dots\}.$$

H is a subgroup of $\mathbb{Z}$.

Recall that elements of $\mathbb{Z}/100\mathbb{Z}$ are congruence classes modulo 100. The element we denote $\overline{a}$ is the set of all integers which are congruent to $a \pmod{100}$, so

$$\overline{3} = \{\dots, -197, -97, 3, 103, 203, \dots\} = \{3 + h : h \in 100\mathbb{Z}\}.$$

Thus $\overline{3} = 3 + 100\mathbb{Z}$ is a left coset of H. Note also that

$$3 + 100\mathbb{Z} = 103 + 100\mathbb{Z} = 12403 + 100\mathbb{Z},$$

etc.

Let $\varphi\colon G \to G'$ be a homomorphism. Let $K = \ker(\varphi)$. We know that K is the set of all elements of G which map to $1_{G'}$. In general, for $g' \in G$, the set of all elements of G which map to g' is called the *fiber* over g'.

Proposition 4.3. *Let $\varphi\colon G \to G'$ be a homomorphism. Let $a \in G$ be any element. The set of all elements $x \in G$ such that $\varphi(x) = \varphi(a)$ is the left coset aK.*

Proof. Suppose $\varphi(x) = \varphi(a)$. Then

$$\varphi(a^{-1}x) = \varphi(a)^{-1}\varphi(x) = 1_{G'},$$

so $a^{-1}x \in K$, which implies $x = a(a^{-1}x) \in aK$.

On the other hand, if $x \in aK$, then $x = ak$ for some $k \in K$, so

$$\varphi(x) = \varphi(a)\varphi(k) = \varphi(a). \qquad \square$$

4.2 Counting formula [2.8]

We can also view left cosets of H as equivalence classes for the following equivalence relation.

Let H be a subgroup of G. We define

$$a \sim b \text{ if } b = ah \text{ for some } h \in H.$$

We check that it is indeed an equivalence relation.

- (Transitivity) If $a \sim b$ and $b \sim c$, then $b = ah_1$ and $c = bh_2$, so $c = ah_1h_2$, so $a \sim c$.
- (Symmetry) If $a \sim b$, then $b = ah$ so $a = bh^{-1}$, so $b \sim a$.
- (Reflexivity) We have $a = a \cdot 1_G$, so $a \sim a$.

Corollary 4.4. *The left cosets of H partition G.*

Example 4.5. Recall again that

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

has the 6 elements

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

Let $H = \langle y \rangle$ be the subgroup generated by y. We calculate the 6 sets aH:

$$H = \{1, y\}, \quad xH = \{x, xy\}, \quad x^2H = \{x^2, x^2y\},$$

and

$$yH = \{y, 1\}, \quad xyH = \{xy, x\}, \quad x^2yH = \{x^2y, x^2\}.$$

Note that these are the same as the three above. So there are 3 distinct left cosets of H

$$H = \{1, y\} = yH, \quad xH = \{x, xy\} = xyH, \quad x^2H = \{x^2, x^2y\} = x^2yH,$$

and these three sets partition S_3.

Definition 4.6. The number of left cosets of H is called the *index* of H in G and denoted $[G : H]$. If $|G|$ is infinite, it could be infinite.

Lemma 4.7. *All left cosets aH of H have the same number of elements. (It could be infinite.)*

Proof. We have a bijection $H \to aH$ given by $h \mapsto ah$, with inverse $g \mapsto a^{-1}g$. Thus aH has $|H|$ elements. □

Theorem 4.8 (Counting formula)**.** *For any subgroup H of G,*

$$|G| = |H|[G : H].$$

Proof. This is because G is partitioned into $[G : H]$ equivalence classes, each of which has $|H|$ elements. □

4.3 Lagrange's theorem [2.8]

Theorem 4.9. *Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$.*

Proof. This follows directly from the above theorem. □

Remark 4.10. Let G be a finite group, and let $a \in G$ be any element Let n be the order of G. Then Lagrange's theorem tells us that n divides $|G|$ because the cyclic subgroup

$$H = \langle a \rangle = \{1, a, \ldots, a^{n-1}\}$$

satisfies $|H| = n$. From this we also get

$$a^{|G|} = 1.$$

Corollary 4.11. *Let p be a prime. Any group G of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Let a be any element of G other than the identity. Then a has order p, so the subgroup $\langle a \rangle$ has p elements. So $G = \langle a \rangle$, which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. □

Proposition 4.12 (Groups of order 4)**.** *Let G be a group of order 4. Then G is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

The dihedral group D_2 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is also called the Klein Four Group.

Proof. By the corollary of Lagrange's theorem mentioned last time, the order of every element divides $|G| = 4$.

Case 1: G has an element x of order 4. Then $G = \langle x \rangle$ so it's isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Case 2: Every element of G other than the identity has order 2. Then for any $x, y \in G$, we have

$$xyxy = 1,$$

which (using $x^2 = y^2 = 1$), implies $yx = xy$. So G is abelian.

We can check directly that the map

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$$

given by

$$(0,0) \mapsto 1_G, \quad (1,0) \mapsto x, \quad (0,1) \mapsto y, \quad (1,1) \mapsto xy$$

is an isomorphism. □

4.4 More on the counting formula [2.8]

Corollary 4.13. *For any homomorphism $\varphi\colon G \to G'$,*

$$|G| = |\ker(\varphi)||\operatorname{im}(\varphi)|.$$

Proof. By Proposition 4.3, the cosets of $\ker(\varphi)$ are the nonempty fibers of φ, which are in bijection with $\operatorname{im}(\varphi)$. Thus, G is partitioned into $|\operatorname{im}(\varphi)|$ cosets of $\ker(\varphi)$, from which the formula follows. □

Proposition 4.14. *If $G \supseteq H \supseteq K$ is a chain of subgroups of a group G, then*

$$[G : K] = [G : H][H : K].$$

Proof. Suppose $[G : H] = n$, and $[H : K] = m$. Then we have partitions

$$G = a_1H \cup \cdots \cup a_nH,$$

and

$$H = b_1K \cup \cdots \cup b_mK.$$

The second line lets us note that each a_jH, for $1 \le j \le n$, is partitioned into m cosets of K

$$a_jH = a_jb_1K \cup \cdots \cup a_jb_mK.$$

So G is partitioned into mn cosets of K, so $[G : K] = mn$.

The cases where one of $[G : H]$ or $[H : K]$ is infinite are similar. □

4.5 Right cosets [2.8]

Definition 4.15. Let H be a subgroup of G. A *right coset* of H is a set

$$Ha \coloneqq \{ha : h \in H\}.$$

Proposition 4.16. *If H is a normal subgroup of G, then $gH = Hg$ for all $g \in G$.*

Proof. For any $h \in H$, we have

$$gh = ghg^{-1}g \in Hg,$$

where we have used the assumption $ghg^{-1} \in H$ since H is normal. Thus, $gh \subseteq Hg$. Similarly, $Hg \subseteq gH$. □

Example 4.17. We return to the subgroup $H = \langle y \rangle$ of S_3, which is not normal. Earlier, we calculated the left cosets

$$\{1, y\}, \quad \{x, xy\}, \quad \{x^2, x^2y\}.$$

We similarly calculate the right cosets

$$H = \{1, y\}, \quad Hx = \{x, yx\} = \{x, x^2y\}, \quad Hx^2 = \{x^2, yx^2\} = \{x^2, xy\},$$

and

$$Hy = \{y, 1\}, \quad Hxy = \{xy, yxy\} = \{xy, x^2\}, \quad Hx^2y = \{x^2y, yx^2y\} = \{x^2y, x\}.$$

Thus, there are also three distinct right cosets

$$\{1, y\}, \quad \{x, x^2y\}, \quad \{x^2, xy\},$$

which also partition G, but they are different from the left cosets.