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

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

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, $\ell = d$. $\square$

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 $\gcd(a,b)$. $\square$

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 $p|b$. $\square$

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 $b = r$. $\square$

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

   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 $m \leq ab/d$. $\square$

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,

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

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,

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

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

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

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 $0 \le r < n$. 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

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

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 $A_1 A_2 \cdots A_n$ 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

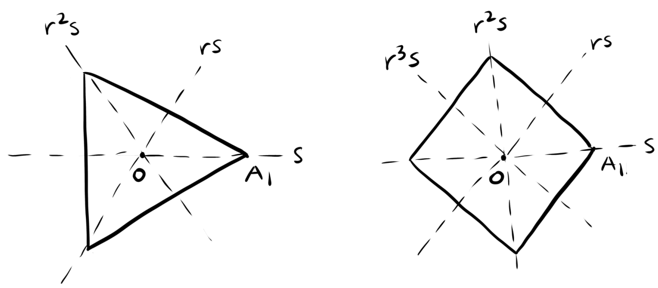
$$|D_n| = 2n.$$

- 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.

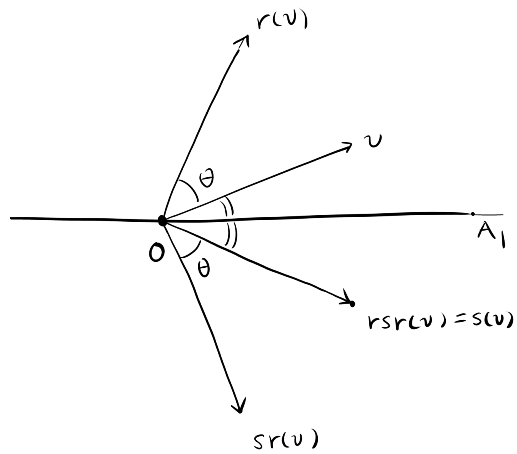
  Let s denote reflection across OA_1. It satisfies

  $$s^2 = 1.$$

  The other reflections are

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

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



The dihedral group has the presentation

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, rsr = s \rangle.$$

The third relation can equivalently be written

$$rsr = s, \quad sr = r^{n-1}s.$$

We also have $r^k s r^k = s$ and $sr^k = r^{n-k}s$.

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 $1 \leq i \leq n$, 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

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

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 $x, y \in \mathrm{im}(\varphi)$. Then $x = \varphi(a)$, $y = \varphi(b)$ for some $a, b \in G$. So $xy = \varphi(ab)$ is also in $\mathrm{im}(\varphi)$.

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

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

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. $\square$

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 $\mathbb{Z}/p\mathbb{Z}$. $\square$

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. $\square$

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. $\square$

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. $\square$

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, $Hg \subseteq gH$. $\square$

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.

5 Jan 26: Quotients and correspondence theorem

5.1 Quotients [2.12]

In this subsection, we define, for a **normal** subgroup N of G, the *quotient group* G/N. Note that the quotient group construction only applies when N is normal.

Recall that we had an equivalence relation on G given by

$$a \sim b \text{ if } b = an \text{ for some } n \in N.$$

The equivalence classes are the left cosets of N.

Definition 5.1. The elements of G/N are the left cosets aN. The group operation $\cdot$ on these elements is given by

$$(aN) \cdot (bN) = (ab)N.$$

Example 5.2. For $G = \mathbb{Z}$ and $H = n\mathbb{Z}$, the cosets are $\overline{a} = a + n\mathbb{Z}$, the congruence classes modulo n. The quotient group given by the above definition is the same as the group which we have already been denoting $\mathbb{Z}/n\mathbb{Z}$.

Before we go on, we need to check that the group operation in Definition 5.1 is actually well-defined, since a coset can be written as aN for different choices of a. In fact, recall that

$$aN = a'N \iff a' \in aN.$$

Lemma 5.3. *If $aN = a'N$ and $bN = b'N$ for $a, b, a', b' \in G$, then*

$$(ab)N = (a'b')N.$$

Proof. The assumptions tell us that $a' = an_1$ and $b' = bn_2$ for some $n_1, n_2 \in N$. Then

$$a'b' = an_1bn_2 = ab(b^{-1}n_1b)n_2 \in abN,$$

where we have used the fact that $b^{-1}n_1b \in N$ since N is normal. Thus, $(a'b')N = (ab)N$. $\square$

Thus, we have shown that the group operation defined on G/N actually makes sense. The group axioms can easily be checked. The identity of G/N is the coset $1 \cdot N = N$.

Remark 5.4.

1. Note that if G is a finite group, then by the counting formula,

$$|G/N| = |G|/|N|.$$

2. The group operation on G/N can equivalently be defined by

$$(aN) \cdot (bN) = \{xy : x \in aN, y \in bN\},$$

i.e., the product of cosets is the literal set of products of the elements in the cosets. This is the same as our previous definition by the same kind of calculation as in the proof of Lemma 5.3: if $x = an_1$ and $y = bn_2$, then

$$xy = an_1bn_2 = ab(b^{-1}n_1b)n_2 \in abN.$$

Example 5.5. Let $G = \mathbb{Z}/6\mathbb{Z}$, and let $N = \{0, 3\}$. Then G/N consists of the cosets

$$N = \{0, 3\} = 3 + N, \quad 1 + N = \{1, 4\} = 4 + N, \quad 2 + N = \{2, 5\} = 5 + N.$$

The coset $\{0, 3\}$ is the identity, and the group operation is commutative and given by

$$\{1, 4\} + \{1, 4\} = \{2, 5\}, \quad \{1, 4\} + \{2, 5\} = \{0, 3\}, \quad \{2, 5\} + \{2, 5\} = \{1, 4\}.$$

The quotient group G/N is isomophic to $\mathbb{Z}/3\mathbb{Z}$.

Example 5.6. Let G and H be groups, and let N be the subgroup of $G \times H$ given by

$$N = \{(g, 1_H) : g \in G\} \simeq G.$$

Then

$$G \times H/N \simeq H,$$

via the isomorphism $(g, h)N = (1_G, h)N \mapsto h$.

Example 5.7. Let $G = \mathbb{Z}/4\mathbb{Z}$, and let $N = \{0, 2\}$, which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Then G/N also has two elements so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. In this case,

$$G \ncong N \times G/N$$

since $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5.2 First isomorphism theorem [2.12]

Theorem 5.8 (First isomorphism theorem)**.** *Let $\varphi\colon G \to G'$ be a homomorphism of groups with kernel K. Then G/K is isomorphic to* $\mathrm{im}(\varphi)$.

Proof. The isomorphism is given by

$$\overline{\varphi}(aK) = \varphi(a).$$

This is well-defined and injective because K is the kernel. It is surjective by definition of the image of φ. It is a group homomorphism because

$$\overline{\varphi}((aK) \cdot (bK)) = \overline{\varphi}((ab)K) = \varphi(a)\varphi(b) = \overline{\varphi}(aK)\overline{\varphi}(bK). \qquad \square$$

Example 5.9. The kernel of the homomorphism $\varphi\colon \mathbb{R}^\times \to \mathbb{R}^\times$ given by

$$\varphi(x) = x^2$$

is $\{\pm 1\}$, and the image is $\mathbb{R}_{>0}$, the subgroup of positive real numbers. Thus,

$$\mathbb{R}^\times/\{\pm 1\} \simeq \mathbb{R}_{>0}.$$

Example 5.10. Consider the homomorphism $\varphi\colon D_4 \to \mathbb{Z}/4\mathbb{Z}$ given by

g	1	r	r^2	r^3	s	rs	r^2s	r^3s
$\varphi(g)$	0	2	0	2	2	0	2	0

.

We see that $\ker(\varphi) = \{1, r^2, rs, r^3s\}$. The two cosets of $\ker(\varphi)$ are

$$\{1, r^2, rs, r^3s\} \quad \text{and} \quad \{r, r^3, s, r^2s\}.$$

The quotient $D_4/\ker(\varphi)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is also isomorphic to the image $\{0, 2\} \subseteq \mathbb{Z}/4\mathbb{Z}$.

Example 5.11. (Artin, Exercise 2.8.6) Suppose $\varphi\colon G \to G'$ is a nontrivial homomorphism of groups with $|G| = 18$ and $|G'| = 15$. What is the order of its kernel?

Solution. We have $G/\ker(\varphi) \simeq \operatorname{im}(\varphi)$, so

$$18/|\ker(\varphi)| = |\operatorname{im}(\varphi)|.$$

Since $\operatorname{im}(\varphi)$ is a subgroup of G', the order of $\operatorname{im}(\varphi)$ is a divisor of $|G'| = 15$. From the above displayed equation, $|\operatorname{im}(\varphi)|$ also divides 18.

Thus, $|\operatorname{im}(\varphi)|$ divides $\gcd(15, 18) = 3$, and by assumption $|\operatorname{im}(\varphi)| \neq 1$, so $|\operatorname{im}(\varphi) = 3|$. This gives us $|\ker(\varphi)| = 6$.

5.3 Quotient map [2.12]

Proposition 5.12. *Let N be a normal subgroup of G. There is a canonical surjective homomorphism*

$$\pi\colon G \to G/N$$

given by $\pi(g) = gN$. The kernel of π is N.

5.4 Correspondence theorem [2.10]

Let $\varphi\colon G \to G'$ be a homomorphism of groups. We study the relationship between

$$\{\text{subgroups of } G\} \quad \text{and} \quad \{\text{subgroups of } G'\}.$$

We first observe the following way to go between them.

Proposition 5.13. *Let $\varphi\colon G \to G'$ be a homomorphism with kernel K.*

1. *If H is a subgroup of G, then $\varphi(H) = \{\varphi(h) : h \in H\}$ is a subgroup of G'.*

2. *If H' is a subgroup of G', then*

$$\varphi^{-1}(H') \coloneqq \{h \in G : \varphi(h) \in H'\}$$

is a subgroup of G which contains K.

Proof. The first statement is the fact that the image of a homomorphism is a subgroup, which we have seen before.

For the second part, we check closure, and the other group axioms are similar. Suppose $h_1, h_2 \in \varphi^{-1}(H)$. Then

$$\varphi(h_1 h_2) = \varphi(h_1)\varphi(h_2) \in H',$$

where we have used $\varphi(h_1), \varphi(h_2) \in H'$ and the closure condition for H'.

In addition, we see that

$$K \subseteq \varphi^{-1}(H')$$

because $\varphi(a) = 1_{G'} \in H'$ for all $a \in K$. □

Remark 5.14.

1. Note that the method in 2. above only lets us obtain subgroups of G containing K.

2. The method in 1. does not in general give us all subgroups of G' either.

   For example, if $\varphi\colon \mathbb{R}^\times \to \mathbb{R}^\times$ is given by

$$\varphi(x) = x^2,$$

   the entire group $\mathbb{R}^\times$ is not equal to $\varphi(H)$ for any subgroup H of $\mathbb{R}^\times$, since the image of φ consists of positive real numbers.

   However, if φ is *surjective*, then we have the following theorem.

Theorem 5.15 (Correspondence theorem)**.** *If $\varphi\colon G \to G'$ is a surjective homomorphism with kernel K, then the map*

$$\begin{aligned} \{\text{subgroups of } G \text{ containing } K\} &\to \{\text{subgroups of } G'\} \\ H &\mapsto \varphi(H) \end{aligned}$$

is a bijection with inverse

$$\varphi^{-1}(H') \leftarrow\!\shortmid H'.$$

Example 5.16. Consider the homomorphism $\varphi\colon \mathbb{C}^\times \to \mathbb{C}^\times$ given by

$$\varphi(z) = z^2.$$

Here $K = \{\pm 1\}$. The subgroup $\mathbb{R}^\times$ of $\mathbb{C}^\times$ contains K, and it corresponds to the subgroup $\mathbb{R}_{>0}$ of $\mathbb{C}^\times$ consisting of positive real numbers.

Corollary 5.17. *For a normal subgroup N of G, the subgroups of G/N correspond to the subgroups of G which contain N.*

Proof of correspondence theorem.

1. For H' a subgroup of G, we show that $\varphi(\varphi^{-1}(H')) = H'$. By definition of $\varphi^{-1}(H')$, we have
$$\varphi(\varphi^{-1}(H)) \subseteq H'.$$
Since φ is surjective, for each $h' \in H'$, there exists $h \in G$ such that $\varphi(h) = h'$. By definition again, $h \in \varphi^{-1}(H)$. Thus,
$$h' = \varphi(h) \in \varphi(\varphi^{-1}(H)),$$
so $H' \subseteq \varphi(\varphi^{-1}(H))$.

2. For H a subgroup of G containing K, we show that $\varphi^{-1}(\varphi(H)) = H$. By definition, we have
$$H \subseteq \varphi^{-1}(\varphi(H)).$$
Now suppose $g \in \varphi^{-1}(\varphi(H))$. This means that $\varphi(g) \in \varphi(H)$, which by definition means that $\varphi(g) = \varphi(h)$ for some $h \in H$. This means that $g \in hK$, but since $K \subseteq H$, this implies
$$g \in hK \subseteq H.$$
Thus $\varphi^{-1}(\varphi(H)) \subseteq H$. $\square$

6 Jan 28: Group actions

6.1 Correspondence theorem [2.10]

The correspondence between subgroups also gives us some information about normal subgroups.

Theorem 6.1 (Correspondence theorem)**.** *If $\varphi\colon G \to G'$ is a surjective homomorphism with kernel K, then the map*

$$\begin{aligned}\{\text{subgroups of } G \text{ containing } K\} &\to \{\text{subgroups of } G'\}\\ H &\mapsto \varphi(H)\end{aligned}$$

is a bijection with inverse

$$\varphi^{-1}(H') \hookleftarrow H'.$$

Theorem 6.2 (Correspondence theorem, cont'd)**.** *If H and H' are corresponding subgroups, then H is normal if and only if H' is normal.*

Proof.

1. Suppose H' is normal. Then for any $h \in \varphi^{-1}(H')$ and $g \in G$, we have

   $$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in H',$$

   where we have used $\varphi(h) \in H'$ and the fact that H' is normal. (This implication does not require φ to be surjective.)

2. Suppose H is normal. Then for any $g' \in G'$ and $h \in H$, we have

   $$g'\varphi(h)g'^{-1} = \varphi(ghg^{-1}) \in \varphi(H),$$

   where $g \in G$ is some element such that $\varphi(g) = g'$. Here we have used surjectivity of φ. □

6.2 Symmetry

Example 6.3. Recall that S_n is the set of bijective maps from $\{1, 2, \ldots, n\}$ to itself.

Example 6.4. Recall that

$$\begin{aligned}\mathrm{GL}_n(\mathbb{R}) &= \{\text{invertible } n \times n \text{ matrices } A \text{ with real entries}\}\\ &= \{\text{bijective linear maps } f\colon \mathbb{R}^n \to \mathbb{R}^n\}.\end{aligned}$$

A linear map is a function which preserves the vector space structure on $\mathbb{R}^n$, i.e.,

$$f(au + bv) = af(u) + bf(v).$$

The matrix A corresponds to the linear map $f(v) = Av$.

Example 6.5. The dihedral group D_n is the group of symmetries of a regular n-gon $A_1A_2\cdots A_n$. What we really mean is

$$D_n = \{\text{isometries from } A_1A_2\ldots A_n \text{ to itself}\}.$$

Here, an *isometry* of the plane is a map $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ which preserves distance, i.e.,

$$\|f(u) - f(v)\| = \|u - v\|$$

for all $u, v \in \mathbb{R}^2$.

Not all isometries are linear maps (and not all linear maps are isometries), but all of the elements of the dihedral group are linear maps.

Here are the elements of D_n in matrix form. Suppose that $A_1A_2\ldots A_n$ is centered at $(0,0)$, and $A_1 = (1,0)$.

The element r^k is a rotation by $\theta = 2\pi k/n$ around the origin, so

$$r^k = \begin{bmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{bmatrix}.$$

The element s is reflection across the x-axis, so it sends (x,y) to $(x,-y)$, so

$$s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The other reflections are

$$r^k s = \begin{bmatrix} \cos(2\pi k/n) & \sin(2\pi k/n) \\ \sin(2\pi k/n) & -\cos(2\pi k/n) \end{bmatrix}.$$

6.3 Group actions [6.7]

In the previous subsection, we saw that many groups we've seen consist of bijective maps from some set to itself, which preserve some additional structure on the set.

Another example of this is the set of automorphisms of a group G, which are the bijective maps from G to itself which preserve the group structure.

Definition 6.6. Let S be a set and let G be a group. An action of G on S is a map $*\colon G \times S \to S$ satisfying

1. $1 * s = s$ for all $s \in S$.
2. (associativity) $(gh) * s = g * (h * s)$ for all $g, h \in G$ and $s \in S$.

Given an action of G ond S, every element $g \in G$ can be viewed as a bijective map

$$g\colon S \to S, \quad s \mapsto g * s.$$

It is bijective because the axioms imply that $g^{-1}\colon S \to S$ is its inverse:

$$g * (g^{-1} * s) = 1 * s = s \quad \forall s \in S.$$

Example 6.7. The map

$$*\colon G \times G \to G, \quad g * a = gag^{-1}$$

is an action of G on G itself. This is G acting on itself by conjugation. We check that it satisfies the group action axioms.

1. $1 * a = 1a1 = a$ for all $a \in G$.
2. $(gh) * a = (gh)a(gh)^{-1} = ghah^{-1}g^{-1} = g * (hah^{-1}) = g * (h * a)$.

In this case, every element g acts by an automorphism of G.

Example 6.8. The map

$$*\colon G \times G \to G, \quad g * a = ga$$

is also a group action. We check associativity:

$$(gh) * a = gha = g * (ha) = g * (h * a).$$

In this case, the elements g don't act by automorphisms, only bijections.

6.4 Orbits and stabilizers [6.7]

Let G be a group acting on a set S.

Definition 6.9. Let $s \in S$. The *orbit* of s is

$$O_s = \{s' \in S : s' = gs \text{ for some } g \in G\}.$$

We can define an equivalence relation on S by

$$s \sim s' \text{ if } s' = sg \text{ for some } g \in G.$$

Then the orbits O_s are the equivalence classes of S under this equivalence relation. The orbits of the action of G on S partition S.

Example 6.10.

1. Consider the action of $\mathbb{R}^\times$ on the set $\mathbb{R}$ given by $c * x = cx$. The orbit of $x = 0$ is $\{0\}$, and the orbit of any nonzero x is $\mathbb{R} - \{0\}$.
2. Consider the action of $\mathbb{R}^\times$ on $\mathbb{R}^2$ given by $c * (x, y) = (cx, c^{-1}y)$. The orbits are

   $$\{(0,0)\}, \quad \{(x,0) : x \neq 0\}, \quad \{(0,y) : y \neq 0\}, \quad \{(x,y) : xy = a\}$$

   for all nonzero real numbers a.

Definition 6.11. A group action is *transitive* if there is only one orbit, i.e., for any two elements $s, s' \in S$, there exists $g \in G$ such that $s' = gs$.

Example 6.12. The action of S_n on $\{1, 2, \ldots, n\}$ is transitive.

Definition 6.13. Let $s \in S$. The *stabilizer* is

$$G_s = \{g \in G : gs = s\}.$$

It is the set of elements of G which fix s. The group action axioms imply that G_s is a actually a subgroup of G.

Example 6.14. Consider the action of the dihedral group $G = D_6$ acting on the set of vertices $S = \{A_1, A_2, \ldots, A_6\}$ of a regular hexagon. This action is transitive, so the orbit of A_1 is the entire set

$$O_{A_1} = \{A_1, A_2, \ldots, A_6\}.$$

The only elements of D_6 which fixes A_1 are the identity and reflection across OA_1. Thus

$$G_{A_1} = \{1, s\} = \langle s \rangle.$$

The stabilizers of the other vertices are also groups of order 2.

Lemma 6.15. *Let H be a subgroup of a group G. For any element $a \in G$, the subset*

$$aHa^{-1} = \{g \in G : g = aha^{-1} \text{ for some } h \in H\}$$

is also a subgroup of G.

Proposition 6.16. *Let G be a group acting on a set S, and let $s \in S$. Then for any $a \in G$, the stabilizer of $s' = as$ is the conjugate subgroup aG_sa^{-1}.*

Proof. Let $g \in G$. Note that

$$gs' = s' \iff gas = as \iff a^{-1}gas = s \iff a^{-1}ga \in G_s \iff g \in aG_sa^{-1}.$$

□

6.5 Operation on cosets [6.8]

Let G be a group, and let H by any subgroup of G. Let G/H denote the set of left cosets of H.

Following Artin, we write $[C]$ to denote a coset C when viewed as an element of the set G/H. We have an action of G on G/H defined by

$$g[C] = [gC]$$

where $gC = \{gc : c \in C\}$.

This action can equivalently be defined by $g[aH] = [gaH]$.

Proposition 6.17. *The action of G on G/H is transitive and the stabilizer of the coset $[H]$ is the subgroup H.*

Example 6.18. Let $G = S_3$, $H = \langle y \rangle = \{1, y\}$. Then

$$G/H = \{\{1, y\}, \{x, xy\}, \{x^2, x^2y\}\}.$$

The element x acts by a 3-cycle

$$[\{1, y\}] \to [\{x, xy\}] \to [\{x^2, x^2y\}] \to [\{1, y\}].$$

The element y fixes $[H] = [\{1, y\}]$, and swaps

$$[\{x, xy\}] \leftrightarrow [\{x^2, x^2y\}].$$

The stabilizer of the *element* $[\{1, y\}] \in G/H$ is the *subgroup* $H = \{1, y\} \subseteq G$.

Note that left multiplication by y does not fix the elements of $\{1, y\}$, rather, it fixes the entire coset $[\{1, y\}]$.

7 Feb 2: Orbit-stabilizer theorem, Burnside's lemma, permutation representations

7.1 Orbit-stabilizer theorem [6.8, 6.9]

Theorem 7.1. *Let S be a finite set on which a group G acts. Let $s \in S$. The elements of O_s are in bijection with the left cosets of G_s. In particular,*

$$|G| = |G_s| \cdot |O_s|.$$

Proof. Note that

$$O_s = \{gs : g \in G\}.$$

However, sometimes $gs = g's$ for different $g, g' \in G$. This happens exactly when $g^{-1}g's = s$, i.e.,

$$g^{-1}g' \in G_s,$$

or $g' \in gG_s$.

Thus, we have a bijection $G/G_s \to O_s$ given by $[gG_s] \mapsto gs$. This is well-defined by definition of G_s, surjective by definition of O_s, and injective by the discussion above.

Thus, $|O_s| = [G : G_s]$, the number of left cosets of G_s, and the formula in the theorem statement follows from the counting formula

$$|G| = |G_s|[G : G_s]. \qquad \square$$

7.2 Orbits partition S [6.9]

Note that if S is partitioned into k orbits $O_1, O_2, \dots, O_k$, then we also have the formula

$$|S| = |O_1| + \cdots + |O_k|.$$

7.3 Application of the orbit-stabilizer theorem

Definition 7.2 (Fixed points)**.** Let G be a group acting on a set S. For any $g \in G$, the set of *fixed points* of g is the set

$$S^g := \{s \in S : gs = s\}.$$

Theorem 7.3 (Burnside's lemma)**.** *Let G be a finite group acting on a finite set S. Then*

$$\text{number of orbits of } G \text{ acting on } S = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

Proof. Suppose S is partitioned into k orbits $O_1, \dots, O_k$.

1. Let $s \in S$. The orbit stabilizer theorem gives

$$\frac{1}{|O_s|} = \frac{|G_s|}{|G|}.$$

   We take the sum over $s \in S$ of both sides, to get

$$\sum_{s\in S} \frac{1}{|O_s|} = \frac{1}{|G|} \sum_{s\in S} |G_s|. \qquad (\heartsuit)$$

2. However note that the left hand side of $(\heartsuit)$ is equal to

$$\sum_{s\in S} \frac{1}{|O_s|} = \sum_{i=1}^{k} \sum_{s\in O_i} \frac{1}{|O_i|} = \sum_{i=1}^{k} 1 = k,$$

   the number of orbits! So in fact,

$$k = \frac{1}{|G|} \sum_{s\in S} |G_s|.$$

3. On the other hand,

$$\sum_{s\in S} |G_s| = \sum_{g\in G} |S^g|.$$

   This equation comes from counting the number of elements in the set

$$X = \{(g, s) \in G \times S : gs = s\}$$

   in two different ways: for fixed $s_0 \in S$, the number of pairs (g, s_0) in X is $|G_{s_0}|$. Then we sum over s_0. Alternatively, for each $g_0 \in G$, the number of pairs (g_0, s) in X is $|S^{g_0}|$, and we sum over g_0.

$\square$

Example 7.4. Let p be a prime. Find the number of different ways to color the edges of a regular p-gon using a colors, where two colorings are considered the same if one can be obtained from the other by rotating the p-gon.

Solution. If we don't consider rotations, the number of colorings is clearly a^p; for each of the p edges, we choose one of the a colors. Let S be the set of these colorings.

Let $G = \{1, r, r^2, \ldots, r^{p-1}\}$ be the group of rotations of the regular p-gon. We have an action of G on S. Recall that for any group action, we have an equivalence relation on S defined by

$$s' \sim s \text{ if } s' = gs \text{ for some } g,$$

whose equivalence classes are the orbits of the action.

Thus, the problem is exactly asking for the number of orbits of G acting on the set S of size a^p. By Burnside's lemma, we just need to calculate

$$\frac{1}{p} \cdot \sum_{g \in G} |S^g|.$$

Note that G is naturally isomorphic to $\mathbb{Z}/p\mathbb{Z}$. It is easier to think about G this way. There are two cases.

1. $g = 1$. Every element of S is fixed by the identity so,

$$|S^g| = |S| = a^p. \tag{$\spadesuit$}$$

2. $g = r^j$ for $j = 1, \ldots, p-1$. Note that s is fixed by g if and only if s is fixed by the entire subgroup $\langle g \rangle$ generated by g. In this case, since p is prime, $\langle g \rangle$ is the entire group G.

   The only colorings which are fixed by any rotation are the ones where every edge is the same color. There are a of these, so $|S^g| = a$

Thus, the sum in ($\spadesuit$) has one term equal to a^p and $(p-1)$ terms equal to a, and the final answer is

$$\boxed{\frac{a^p + (p-1)a}{p}.}$$

Example 7.5. Do the same as above but for a regular 25-gon.

Solution. The setup is the same. The set S has size a^{25}, and the group G which is isomorphic to $\mathbb{Z}/25\mathbb{Z}$ acts on S. We want to find the number of orbits, which Burnside's lemma tells us is equal to the sum

$$\frac{1}{25} \sum_{g \in G} |S^g|.$$

Since 25 is not prime, there are three cases now. The cases correspond to subgroups of $\mathbb{Z}/25\mathbb{Z}$, which also correspond to the divisors of 25.

1. $g = \overline{0}$. As before, $|S^g| = |S| = a^{25}$.

2. $\langle g \rangle = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}\}$. If we label the edges of the 25-gon $e_1, e_2, \ldots, e_{25}$, the colorings which are fixed by r^5 are determined by the colors of any 5 consecutive edges, e.g., $e_1, e_2, \ldots, e_5$. Then e_6 has the same color as e_1 because $r^5(e_1) = e_6$, etc.

   Thus, there are a^5 colorings which are fixed by $\{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}\}$, so for any generator of this subgroup, $|S^g| = a^5$.

3. $\langle g \rangle = \mathbb{Z}/25\mathbb{Z}$. Same as before, the only colorings fixed by the entire group G are the ones where all edges are the same color. So $|S^g| = a$.

Now, there are four elements $g \in \mathbb{Z}/25\mathbb{Z}$ such that $\langle g \rangle = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}\}$. There are 20 elements such that $\langle g \rangle = \mathbb{Z}/25\mathbb{Z}$; they correspond to the integers from $1, 2, \ldots, 25$ which are coprime to 25. Thus in the sum we want to compute, there is one term equal to a^{25}, four terms equal to a^5, and 20 terms equal to a. The final answer is

$$\boxed{\frac{a^{25} + 4a^5 + 20a}{25}.}$$

7.4 Permutation repsentations [6.11]

If a group G acts on a finite set of n elements, this gives us a homomorphism $G \to S_n$.

Proposition 7.6. *Let G be a group. Let $S = \{1, 2, \ldots, n\}$. There is a bijection*

$$\{\text{actions of } G \text{ on } S\} \leftrightarrow \{\text{homomorphisms } G \to S_n\}.$$

Proof. The proof is trivial but this is how it works. Suppose we are given an action of G on S. We want to define a homomorphism $\varphi \colon G \to S_n$.

Recall that elements of S_n are bijective maps from S to itself, and the group operation is function composition. We simply define

$$\varphi(g) = m_g,$$

where $m_g \colon S \to S$ is the map $m_g(s) = g * s$. Note that $m_g \in S_n$.

We check it satisfies $\varphi(gh) = \varphi(g) \circ \varphi(h)$. This is equivalent to $m_{gh} = m_g \circ m_h$, which is true since

$$m_{gh}(s) = (gh) * s = g * (h * s) = m_g(m_h(s)).$$

The map in the other direction is defined the same way. Given φ, the action of G on S is defined by $g * s = \varphi(g)(s)$. □

Definition 7.7 (Faithful group action)**.** An action of G on S is *faithful* if the only element $g \in G$ which fixes every element of S is the identity element of G, i.e.,

$$gs = s \quad \forall s \in S \implies g = 1.$$

If $S = \{1, 2, \ldots, n\}$, the action of G on S being faithful is equivalent to the corresponding homomorphism $G \to S_n$ being injective.

Example 7.8.

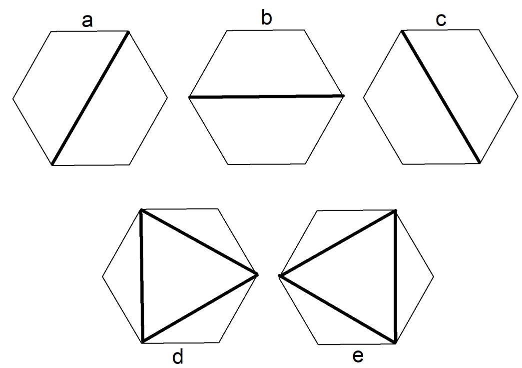
1. For any group G and any set S, there is an action of G on S defined by $gs = s$ for all $g \in G$ and $s \in S$.

   It is not faithful (unless G has only one element). If $S = \{1, 2, \ldots, n\}$, it corresponds to the trivial homomorphism $G \to S_n$.

2. We saw on problem set 2 that there's an injective homomorphim $D_5 \to S_5$, because D_5 acts faithfully on the vertices of a regular pentagon.

3. There is no injective homomorphism $D_5 \to S_4$, because $|D_5| = 10$ and $|S_4| = 24$. However, 10 does not divide 24, so S_4 does not have a subgroup isomorphic to D_5, by Lagrange's theorem.

Example 7.9. Let S be set consisting of the five objects shown below.



Then D_6 acts on S via its usual action on the regular hexagon. For example,

$$ra = c, \quad r^2a = b, \quad rd = e, \quad sa = c, \quad sb = b, \quad se = e.$$

This action is faithful, so it gives us an injective homomorphisms $D_6 \to S_5$.

8 Feb 4: Class equation

8.1 Cayley's theorem [7.1]

Recall that we have an action of G on itself by left multiplication

$$G \times G \to G, \quad (g, x) \mapsto gx.$$

For each $g \in G$, the (left) multiplication-by-g map m_g is bijective, and moreover, it does not fix all (or any) $x \in G$ unless $g = 1$. Thus this action is faithful.

Theorem 8.1. *A finite group G of order n is isomorphic to a subgroup of S_n.*

Proof. From last time, the above group action gives us a homomorphism φ from G to

$$\mathrm{Perm}(G) \coloneqq \text{ the group of permutations of the set of elements of } G,$$

which is isomorphic to S_n, since $|G| = n$. Specifically, the homomorphism is given by $\varphi(g) = m_g$.

Since the left multiplication action is faithful, φ is an injective homomorphism from $G \to S_n$, so G is isomorphic to the subgroup $\mathrm{im}(\varphi)$ of S_n. $\square$

8.2 Class equation [7.2]

Also recall that we have another action of G on itself by *conjugation*. It is the map

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1}.$$

Question 8.2. What are the orbits of the action of G on itself by left multiplication?

Definition 8.3. A *conjugacy class* in a group G is an orbit of the conjugation action of G on itself. The conjugacy class of an element $a \in G$ is

$$C(x) = \{gag^{-1} : g \in G\}.$$

Example 8.4. The conjugacy class of the identity element is always just

$$C(1) = \{1\}.$$

Example 8.5. In $\mathrm{GL}_n(\mathbb{R})$, two matrices A and B are conjugate if

$$B = XAX^{-1}$$

for some invertible $n \times n$ matrix X. So conjugate elements of $\mathrm{GL}_n(\mathbb{R})$ have the same characteristic polynomial.

The converse is not quite true. For example

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

both have characteristic polynomial $(t-1)^2$, but they are not conjugate.

Definition 8.6. For any $x \in G$, the *centralizer* of x in G is the stabilizer of x under the conjugation action. We denote it

$$Z(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}.$$

Definition 8.7. The *center* of a group G is the set

$$Z = \{z \in G : zg = gz \text{ for all } g \in G\}$$

of elements which commute with all elements of G.

Example 8.8.

1. The centralizer of the identity element is always the whole group.
2. If G is abelian, $Z(x) = Z = G$ for any $x \in G$.
3. The centralizer of the matrix $x = \begin{bmatrix} 2 & \\ & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$ consists of all matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that

$$\begin{bmatrix} 2a & b \\ 2c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 2 & \\ & 1 \end{bmatrix} = \begin{bmatrix} 2 & \\ & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2a & 2b \\ c & d \end{bmatrix}.$$

   Solving this equation gives $c = d = 0$, so

$$C(x) = \left\{ \begin{bmatrix} a & \\ & d \end{bmatrix} : a, d \in \mathbb{R}^\times \right\}.$$

4. The center of $\mathrm{GL}_n(\mathbb{R})$ consists of the scalar matrices $c \cdot I_n$ for $c \in \mathbb{R}^\times$.

Proposition 8.9. *Let G be a group and let $x \in G$.*

1. *The centralizer $Z(x)$ contains x, and it contains Z.*
2. *The following are equivalent.*
   (i) $Z(x) = G$. (ii) $x \in Z$. (iii) $C(x) = \{x\}$.

The *class equation* is the formula

$$|G| = \sum_{\substack{\text{conjugacy} \\ \text{classes } C}} |C|.$$

This equation is trivial, but it is useful because there are several restrictions on the numbers that appear on the right hand side.

- At least one of the terms in the sum on the right is equal to 1, it corresponds to the conjugacy class $C(1)$.

- Moreover, every 1 that appears on the right hand side corresponds to an element of the center Z.
- Every term on the right divides $|G|$, since by the orbit-stabilizer theorem,

$$|G| = |Z(x)| \cdot |C(x)|.$$

Example 8.10. We compute the class equation for S_3, by first determining the centralizers, and then using the orbit-stabilizer theorem.

1. The centralizer $Z(x)$ contains x, which has order 3, so $Z(x)$ is a subgroup of S_3 whose order is a multiple of 3, so $|Z(x)| = 3$ or 6.

   It is not the whole group because x is not in the center of S_3, since

$$yx = x^2 y \neq xy,$$

   so $|Z(x)| = 3$, and $|C(x)| = 2$.

2. The centralizer $Z(y)$ contains y, so $Z(y)$ is a subgroup of S_3 whose order is even, so $|Z(y)| = 2$ or 6.

   Again, y is not in the center of S_3, so $|Z(y)| = 2$, and $|C(y)| = 3$.

So we have found a conjugacy class of size 3 and a conjugacy class of size 2, and together with $\{1\}$, these partition S_3. Thus, the class equation is

$$6 = 1 + 2 + 3.$$

8.3 Application of class equation [7.3]

In this subsection, let p be a prime. We use the class equation to classify groups of order p^2.

Theorem 8.11. *Let G be a group of order p^2. Then G is isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Definition 8.12. A *p-group* is a group G whose order is a positive power of p.

Proposition 8.13. *The center of a p-group is not trivial.*

Proof. Suppose $|G| = p^e$, with $e \geq 1$. The class equation reads

$$p^e = \sum \text{divisor of } p^e,$$

and 1's on the right hand side correspond exactly to the elements of the center. All terms which are not equal to 1 are divisible by p, so the number of 1's in the sum is a multiple of p.

There is at least one 1 in the sum, corresponding to the identity, so there must actually be at least p 1's, so the center is not trivial. □

Proposition 8.14. *A group G of order p^2 is abelian.*

Proof. By the above proposition, Z has order either p or p^2. In fact, we show now that a group of order p^2 cannot have center of order p. This would imply $Z = G$, so G is abelian.

Suppose to the contrary that $|Z| = p$. Let $x \notin Z$. The fact we use is that the centralizer $Z(x)$ is a subgroup of G so its order divides p^2. It contains Z and x, so it has order greater than p, so $|Z(x)| = p^2$. Thus $Z(x) = G$, but $Z(x) = G$ is equivalent to $x \in Z$, a contradiction. $\square$

We want to prove that if G has order p^2, then it is either cyclic or the product of two copies of $\mathbb{Z}/p\mathbb{Z}$.

Proposition 8.15 (Artin Proposition 2.11.4)**.** *Let H and K be subgroups of a group G. Consider the function*

$$f\colon H \times K \to G, \quad f(h,k) = hk.$$

Note that its image is $HK := \{hk : h \in H,\ k \in K\}$. Then f defines an isomorphism from $H \times K$ to G if and only if all of the following are satisfied:

- $H \cap K = \{1\}$.
- $HK = G$.
- *H and K are normal.*

Proof of Theorem 8.11. If G has an element x of order p^2, then we are done, because then $G = \langle x \rangle \cong \mathbb{Z}/p^2\mathbb{Z}$.

Otherwise, every non-identity element of G has order p. We also know that G is abelian from the previous proposition. Thus, we can choose any element $x \in G$ of order p, and let $H = \langle x \rangle$. Then we can choose any element $y \notin H$ of order p, and let $K = \langle y \rangle$. Then both H and K are isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and

- $H \cap K = \{1\}$ since their intersection is isomorphic to a subgroup of $\mathbb{Z}/p\mathbb{Z}$ which is not the whole group.
- For any two distinct pairs (h,k), $(h',k') \in H \times K$, the products hk and $h'k'$ are distinct as well, since $H \cap K = \{1\}$. Thus HK has at least p^2 elements, but $|G| = p^2$, so $HK = G$.
- Since G is abelian, H and K are normal.

Thus, $G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. $\square$

9 Feb 11: Conjugation in S_n

9.1 Conjugation in the symmetric group [7.5]

The main observation here is that **conjugation in the symmetric group is basically renaming the indices**.

For example, let $p = (1\ 3\ 4)\ (2\ 5)$, and let $q = (1\ 4\ 5\ 2)$. We compute qpq^{-1}. We forget about the cycle decomposition for a second. The permutations p and q are the functions

i	1	2	3	4	5
$p(i)$	3	5	4	1	2

i	1	2	3	4	5
$q(i)$	4	1	3	5	2

Then

i	$q(1)$	$q(2)$	$q(3)$	$q(4)$	$q(5)$
$qpq^{-1}(i)$	$q(3)$	$q(5)$	$q(4)$	$q(1)$	$q(2)$

This is because $qpq^{-1}(q(i)) = q(p(i))$ for any i, so we just added a $q(\cdot)$ to every entry of the first table.

The function q tells us how to "rename" the indices. So in this case, the cycle decomposition of qpq^{-1} is

$$(q(1)\ q(3)\ q(4))\ (q(2)\ q(5)) = (4\ 3\ 5)\ (1\ 2).$$

If we the cycle decomposition for qpq^{-1} under p, then we can read off the table for q.

$$\frac{(1\ 3\ 4)\ (2\ 5)}{(4\ 3\ 5)\ (1\ 2)}$$

Theorem 9.1. *Two elements of S_n are in the same conjugacy class if and only if they have the same cycle type.*

A couple more: $(1\ 2)\ (3\ 4)$ is conjugate to $(1\ 3)\ (2\ 4)$, and $(1\ 2)\ (3\ 4\ 5)\ (6\ 7)$ is conjugate to $(1\ 5)\ (2\ 4)\ (3\ 7\ 6)$.

Thus, the conjugacy classes in S_n correspond to *partitions* of n.

9.2 Class equations of S_4 and S_5 [7.5]

Example 9.2. The partitions of 4 are

$$4 = 4, \quad 4 = 3 + 1, \quad 4 = 2 + 2, \quad 4 = 2 + 1 + 1, \quad 4 = 1 + 1 + 1 + 1.$$

The corresponding conjugacy classes of S_4 and their sizes are

partition	$4 = 4$	$4 = 3 + 1$	$4 = 2 + 2$	$4 = 2 + 1 + 1$
shape	$(-\ -\ -\ -)$	$(-\ -\ -)$	$(-\ -)\ (-\ -)$	$(-\ -)$
$\lvert C \rvert$	6	8	3	6

in addition to the conjugacy class of the identity. The class equation is

$$24 = 1 + 3 + 6 + 6 + 8.$$

Example 9.3. The partitions of 5 are

$$5,\ 4+1,\ 3+2,\ 3+1+1,\ 2+2+1,\ 2+1+1+1,\ 1+1+1+1+1.$$

There are 24 elements of the form $(- \ - \ - \ - \ -)$, 30 $(- \ - \ - \ -)$'s, 20 $(- \ - \ -)\ (- \ -)$'s, 20 $(- \ - \ -)$'s, 15 $(- \ -)\ (- \ -)$'s, 10 $(- \ -)$'s, and the identity. The class equation is

$$120 = 1 + 10 + 15 + 20 + 20 + 30 + 24.$$

9.3 Signs of permutations

Recall that we defined the sign homomorphism

$$\mathrm{sign}\colon S_n \to \{\pm 1\},$$

by $\mathrm{sign}(\sigma) = \det P_\sigma$, where P_σ is the permutation matrix associated to the permutation σ. Recall that this is a group homomorphism, meaning that we have

$$\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma)\,\mathrm{sign}(\tau).$$

Definition 9.4. A *transposition* is a permutation of the form $(i\ j)$, i.e., it is a permutation which just swaps two indices i and j.

Example 9.5. The permutation matrix associated to the transposition $(1\ 2)$ is

$$\begin{pmatrix} & 1 & & & \\ 1 & & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

which is one row-swap away from the identity matrix, so it has determinant 1. Thus the sign of $(1\ 2)$ is -1. A similar argument shows that $\mathrm{sign}(i\ j) = -1$ for any transposition $(i\ j)$.

Proposition 9.6. *Every element of S_n can be expressed as a product of transpositions.*

Example 9.7. Let $\sigma \in S_5$ be the permutation

i	1	2	3	4	5
$\sigma(i)$	3	5	4	1	2

Working backwards,

i	1	2	3	4	5
$(1\ 3) \circ \sigma(i)$	1	5	4	3	2

i	1	2	3	4	5
$(2\ 5) \circ (3\ 4) \circ (1\ 3) \circ \sigma(i)$	1	2	3	4	5

Proof of Proposition 9.6. We note that

$$\begin{aligned}(i_1\ i_2\ \cdots\ i_k) &= (i_1\ i_k) \circ (i_1\ i_2\ \cdots\ i_{k-1}) \\ &= (i_1\ i_k) \circ (i_1\ i_{k-1}) \circ \cdots \circ (i_1\ i_2).\end{aligned}$$

Since every permutation can be decomposed into cycles, every permutation can be written as a product of transpositions. □

We call permutations with sign $+1$ *even*. Permutations with sign -1 are called *odd*.

Example 9.8. Transpositions are odd. By the decomposition in the proof of Proposition 9.6, a k-cycle is even if and only if k is odd. The permutation

$$(1\ 2)\ (3\ 4\ 5)\ (6\ 7\ 8\ 9)$$

has sign $(-1) \cdot 1 \cdot (-1) = 1$.

9.4 Alternating group [7.5]

Definition 9.9. The *alternating group* A_n is the kernel of the sign homomorphism, i.e., it is the subgroup of S_n of even permutations.

Example 9.10. The elements of S_3 are

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

The elements of A_3 are

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

Question 9.11. What is the order of A_5?

Note that conjugate permutations have the same sign. In S_5, the conjugacy classes which contain even permutations are the ones consisting of permutations with the cycle types, in addition to the identity.

shape	$(-\ -\ -\ -\ -)$	$(-\ -\ -)$	$(-\ -)\ (-\ -)$
number	24	20	15

However, the class equation of A_5 is **not** $60 = 1 + 15 + 20 + 24$.

- Two permutations p and p' may be conjugate in S_5 but not in A_5, i.e., there could exist $q \in S_5$ such that

$$p' = qpq^{-1},$$

  but there may not exist q in the smaller group A_5 which makes the same equation hold.

- If two elements are conjugate in A_5, then they are clearly also conjugate in S_5.
- Thus, some of the even conjugacy classes of S_5 remain a class in A_5, and some split up in A_5.

We will see shortly that the conjugacy class of 5-cycles splits into two conjugacy classes of size 12 in A_5, and the class equation of A_5 is

$$60 = 1 + 15 + 20 + 12 + 12.$$

9.5 Simple groups [7.4]

Definition 9.12. A group G is *simple* if it contains normal subgroup other than $\{1\}$ and G.

Theorem 9.13. *The alternating group A_5 is simple.*

Proof. Suppose N is a normal subgroup of A_5. By definition of normal, it must be a union of conjugacy classes, including the conjugacy class $\{1\}$. By Lagrange's theorem, the order of N must divide 60.

There is no divisor of 60 other than 1 and 60 which can be written as a sum of some of the terms 1, 15, 20, 12, 12, if the term 1 must be included. □

The group A_4 contains the proper normal subgroup

$$\{1, (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\},$$

so it is not simple.

Theorem 9.14. *The alternating group A_n is simple for $n \geq 5$*

9.6 Class equation of A_5

Lemma 9.15. *If p and p' are conjugate in S_n and the centralizer $Z(p)$ contains an odd permutation, then p and p' are also conjugate in A_n.*

Proof. Suppose σ has sign -1, and $\sigma p \sigma^{-1} = p$.

Since p and p' are conjugate, there exists $q \in S_n$ such that $qpq^{-1} = p'$. If q is even, then p and p' are conjugate in A_n.

If q is odd, note that

$$(q\sigma)p(q\sigma)^{-1} = q\sigma p \sigma^{-1} q^{-1} = p'$$

as well, and $q\sigma \in A_n$, so p and p' are conjugate in A_n. □

Lemma 9.16. *Let $p \in S_n$. If the centralizer $Z(p)$ contains only even permutations, then the conjugacy class $C(p)$ splits into two conjugacy classes (of equal size) in A_n.*

Proof. We temporarily denote by $Z_G(p)$ and $C_G(p)$ the centralizer and conjugacy class of p in the group G, respectively.

The assumption is that $Z_{S_n}(p) = Z_{A_n}(p)$. By the orbit-stabilizer theorem

$$|A_n| = |Z_{A_n}(p)| \cdot |C_{A_n}(p)|,$$

and

$$|S_n| = |Z_{S_n}(p)| \cdot |C_{S_n}(p)|.$$

Since $|S_n| = 2|A_n|$, and $|Z_{S_n}(p)| = |Z_{A_n}(p)|$, the above two equations give us

$$|C_{S_n}(p)| = 2 \cdot |C_{A_n}(p)|.$$

Thus, $C(p)$ splits into two conjugacy classes in A_n, with half the size. $\square$

In A_5, there are 3 cases:

1. The centralizer of the 3-cycle $(1\ 2\ 3) = (1\ 2\ 3)\ (4)\ (5)$ contains the odd permutation $(4\ 5)$. Thus, the set of all 3-cycles forms a conjugacy class in A_5. Recall that there are 20 of these.

2. The centralizer of $(1\ 2)\ (3\ 4)$ contains the odd permutation $(1\ 2)$. Thus, the set of all permutations with cycle type $(-\ -)\ (-\ -)$ forms a conjugacy class in A_5 as well as in S_5. There are 15 of these.

3. Let $p = (1\ 2\ 3\ 4\ 5)$. This is an even permutation. The permutations q such that $qpq^{-1} = p$ are (the identity or) given by the tables

$$\frac{(1\,2\,3\,4\,5)}{(2\,3\,4\,5\,1)}, \frac{(1\,2\,3\,4\,5)}{(3\,4\,5\,1\,2)}, \frac{(1\,2\,3\,4\,5)}{(4\,5\,1\,2\,3)}, \frac{(1\,2\,3\,4\,5)}{(5\,1\,2\,3\,4)},$$

   i.e., $(1\,2\,3\,4\,5)$, $(1\,3\,5\,2\,4)$, $(1\,4\,2\,5\,3)$, $(1\,5\,4\,3\,2)$, and the identity.

   These are the powers of p, so they are all even. Thus the set of 5-cycles forms two conjugacy classes in A_5, with 12 elements each.

   Indeed, the 5-cycles $(1\,2\,3\,4\,5)$ and $(1\,3\,5\,2\,4)$ are not conjugate in A_5.

Thus, the class equation of A_5 is

$$60 = 1 + 15 + 20 + 12 + 12.$$