1. Well-ordering principle

We write $\mathbb{Z}$ for the set of integers, and $\mathbb{N} = \{1, 2, 3, \ldots\}$ for the set of natural numbers. I’ll use the convention where natural numbers are assumed to be positive.

I may also write $\mathbb{Z}_>^0$ for $\mathbb{N}$. We also use the notation $\mathbb{Z}_{\geq}^0 = \{0, 1, 2, \ldots\}$ for the set of non-negative integers.

**Well-ordering principle (WOP).** Every non-empty subset of $\mathbb{N}$ contains a smallest element.

Explicitly: if $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then there exists $a \in S$ such that for all $s \in S$ we have $a \leq s$.

Note: if $S = \emptyset$, there is no smallest element of $S$, since there are no elements in $S$ at all (no way to have $s \in S$).

Note: If we replace $\mathbb{N}$ with $\mathbb{Z}$, $\mathbb{R}$, or $[0, 1]$, none of these satisfy the well-ordering property.

The well-ordering principle is equivalent to mathematical induction.

**Mathematical induction (MI).** Let $S \subseteq \mathbb{N}$ be a subset such that (i) $1 \in S$, and (ii) for all $k \in \mathbb{N}$, if $k \in S$ then also $k + 1 \in S$. Then $S = \mathbb{N}$.

This is often phrased in terms of a sequence of propositions as follows:

Let $P_1, P_2, \ldots$ be a sequence of statements such that (i) $P_1$ is true, and (ii) for all $k \in \mathbb{N}$, if $P_k$ is true then $P_{k+1}$ is true. Then $P_n$ is true for all $\mathbb{N}$.

To see that this is really the same as mathematical induction, consider the set $S := \{ n \in \mathbb{N} \mid P_n \text{ is true} \}$.

**Proof that the well-ordering principle is equivalent to mathematical induction.**

WOP $\implies$ MI. Let $S \subseteq \mathbb{N}$ be such that (i) $1 \in S$ and (ii) $k \in S$ implies $k + 1 \in S$. Let $T := \mathbb{N} \setminus S = \{ k \in \mathbb{N} \mid k \notin S \}$, the complement of $S$. If $T = \emptyset$, then $S = \mathbb{N}$ and we are done, so suppose $T \neq \emptyset$ and derive a contradiction. Then by WOP there is a smallest element $t \in T$. By (i) we have $t \neq 1$, so $t > 1$ and thus $t - 1$ is a natural number. Since $t$ is smallest in $T$, we must have $t - 1 \in S$. But (ii) implies that $t \in S$, a contradiction.

MI $\implies$ WOP. (Skipped in class.) Let $T \subseteq \mathbb{N}$ be a non-empty subset. Let’s suppose $T$ has no smallest element and derive a contradiction. Let 

$$S := \{ n \in \mathbb{N} \mid T \cap \{1, \ldots, n\} = \emptyset \},$$

the set of $n$ such that all elements of $T$ are greater than $n$. Since $T$ has no smallest element, then $1 \notin T$, and therefore $1 \in S$. Now suppose $k \in S$, i.e., $\{1, \ldots, k\} \cap T = \emptyset$. We cannot have $k + 1 \in T$ (since then it would be the smallest element), so $\{1, \ldots, k + 1\} \cap T = \emptyset$, i.e., $k + 1 \in S$. We have shown that $S$ satisfies the hypotheses for mathematical induction, so $S = \mathbb{N}$ which implies $T = \emptyset$, a contradiction.

□

**Variant of WOP.** Every non-empty subset of $\mathbb{Z}_{\geq}^0$ contains a smallest element.

Date: October 20, 2017.
2. Division algorithm

(A reference for this and the following few sections is Goodman I.6.)

2.1. Theorem. For integers \(a, b \in \mathbb{Z}\) with \(b > 0\), there exist unique \(q, r \in \mathbb{Z}\) such that 
\[
a = qb + r.
\]

You can read this as 
\[
\frac{a}{b} = q + \frac{r}{b}.
\]

Here \(r\) is the “remainder” of \(a\) divided by \(b\).

Proof. Let \(S = \{ a - xb \mid x \in \mathbb{Z}, a - xb \geq 0 \}\). This is a subset of \(\mathbb{Z}_{\geq 0}\). Note that \(S\) is non-empty (if \(a \geq 0\) then \(a - 0b \in S\); if \(a < 0\) then \(a - ab = a(1 - b) > 0\) is in \(S\)).

By the WOP, there is a least element \(r\) of \(S\), and we can write \(r = a - qb\) with \(q \in \mathbb{Z}\). We know that \(r \geq 0\). If \(r \geq b\), then
\[
r - b = a - (q + 1)b
\]
is also non-negative and so an element of \(S\), contradicting minimality. Thus we must have \(r < b\) as desired.

For uniqueness, suppose \(a = qb + r = q'b + r'\). By relabelling, we can assume \(r' - r \geq 0\). The identity gives

\[
r' - r = (q - q')b.
\]

If \(0 \leq r \leq r' < b\) then \(0 \leq r' - r < b\). The only way \((q - q')b\) can be non-negative and less than \(b\) is if \(q - q' = 0\). So \(q = q'\) and therefore \(r = r'\).

\(\Box\)

3. Divisibility

Given \(a, b \in \mathbb{Z}\), we say that \(b\) divides \(a\) if there exists \(m \in \mathbb{Z}\) such that 
\[
a = bm.
\]

We write “\(b|a\)” for “\(b\) divides \(a\)”.

Note: we can equivalently say “\(a\) is an (integer) multiple of \(b\)”. I find this point of view easier to think about. Alternately, “\(b\) is a factor of \(a\)”.

Note: if \(b \neq 0\), then \(b|a\) if and only if the rational number \(\frac{a}{b}\) is in fact an integer.

Note: if \(b = 0\), then \(0|a\) if and only if \(a = 0\).

Note: for a non-zero integer \(a\), the set \(\{b \in \mathbb{Z} \mid b \text{ is a factor of } a\}\) is finite. This is because \(|bm| = |b||m| \leq |b|\) if \(m \neq 0\). E.g., the factors of 6 are \(\{\pm1, \pm2, \pm3, \pm6\}\). On the other hand, all integers are factors of 0.

3.1. Proposition. Let \(a, b, c, x, y \in \mathbb{Z}\).

(1) If \(a|b\) and \(b|c\) then \(a|c\).
(2) If \(a|n\) and \(a|m\) then \(a|(xn + yn)\).
(3) We have \(a|b\) and \(b|a\) if and only if \(a = \pm b\).

It is handy to convert statements about divisibility into ones about “sets of multiples”. Given \(a \in \mathbb{Z}\), let 
\[
Za = \{ na \mid n \in \mathbb{Z} \},
\]
the set of all integer multiples of \(a\). Then 
\[
a | b \iff b \in Za \iff Zb \subseteq Za,
\]
i.e., “\(a\) divides \(b\)” means “every multiple of \(b\) is also a multiple of \(a\)”. (Example: \(a = 3\) and \(b = 12\).)

3.2. Exercise (On PS 1).

(1) If \(Zb \subseteq Za\) and \(Zc \subseteq Zb\), then \(Zc \subseteq Za\).
(2) If \( n, m \in \mathbb{Z} \) then \( xm + yn \in \mathbb{Z} \).
(3) We have \( \mathbb{Z}a = \mathbb{Z}b \) if and only if \( a = \pm b \).

4. Greatest common divisor

Let \( a, b \) be a pair of integers. A **greatest common divisor (GCD)** of \( a \) and \( b \) is a \( d \in \mathbb{Z}_{\geq 0} \) such that

1. \( d \mid a \) and \( d \mid b \) (“common divisor”) and
2. if \( m \mid a \) and \( m \mid b \) then \( m \mid d \) (“greatest”, in the sense of “most divisible”).

E.g., 4 is a GCD of 12 and 20.

4.1. Example. If \( a = b = 0 \), then \( d = 0 \) is a GCD. (Because every integer divides 0.) Note that 0 is not really the “greatest” common divisor, in the sense of size.

Note: many definitions of GCD require \( d > 0 \), in which case GCD would be undefined in this case.

4.2. Lemma. If a GCD exists, it is unique.

**Proof.** Let \( d \) and \( d' \) be GCDs of \( a \) and \( b \). The properties imply that \( d \mid d' \) and \( d' \mid d \), whence \( d = \pm d' \), and therefore \( d = d' \) since GCDs are assumed to be positive. \( \square \)

We write \( \gcd(a, b) \) for the (unique) GCD of \( a \) and \( b \) if one exists.

We are going to show that GCDs exist (if at least one of the numbers is nonzero). We do this using the following concept of a **subgroup** of \( \mathbb{Z} \).

Say that a subset \( S \subseteq \mathbb{Z} \) is a **subgroup** if (i) \( 0 \in S \), (ii) if \( x \in S \) then \( -x \in S \), and (iii) if \( x, y \in S \), then \( x + y \in S \). I.e., it is a subset containing 0 and “closed” under addition and negation. (The terminology **subgroup** will be explained later when we talk about groups.)

4.3. Lemma. If \( S \) is a subgroup and \( a \in S \), then \( \mathbb{Z}a \subseteq S \).

**Proof.** Show \( na \in S \) for \( n \geq 1 \) by induction on \( n \). Similarly for \( (-n)a \in S \). \( \square \)

4.4. Exercise. \( \mathbb{Z}a \) is a subgroup of \( \mathbb{Z} \) for any integer \( a \).

4.5. Exercise. If \( a, b \in S \), then \( xa + yb \in S \) for any \( x, y \in \mathbb{Z} \).

**Integer combinations.** Given \( a, b \in \mathbb{Z} \), an **integer combination** is any integer of the form \( ma + nb \), for some \( m, n \in \mathbb{Z} \). Write

\[
I(a, b) := \{ ma + nb \mid m, n \in \mathbb{Z} \}
\]

for the set of integer combinations of \( a \) and \( b \).

4.6. Exercise (On PS 1). Check that \( I(a, b) \) is a subgroup.

4.7. Exercise. If \( S \) is a subgroup and \( a, b \in S \), then \( I(a, b) \subseteq S \).

In fact, \( I(a, b) \) is not a new example of a subgroup.

4.8. Proposition. Every subgroup \( S \subseteq \mathbb{Z} \) has the form \( S = \mathbb{Z}d \) for a unique \( d \geq 0 \).

**Proof.** Let \( S \) be a subgroup. We know that \( 0 \in S \). If \( S = \{0\} \), then \( S = \mathbb{Z}0 \). So suppose there exists a non-zero element \( x \) of \( S \). Then \(-x \in S \) also, and therefore \( S \) contains at least one positive element.

Let \( T := S \cap \mathbb{Z}_{>0} \), the set of positive elements of \( S \). Since \( T \) is non-empty, the WOP applies, and \( T \) has a smallest element \( d \).

**Easy observation.** \( \mathbb{Z}d \subseteq S \).
Harder observation. \( S \subseteq \mathbb{Z}d \). To show this, let \( s \in S \) be any element, and apply the division algorithm for \( "s/d" \). We get integers \( q, r \in \mathbb{Z} \) such that
\[
s = qd + r, \quad 0 \leq r < d.
\]
Then \( r = s - qd \in S \). Since \( d \) is the minimal positive element of \( S \), and \( 0 \leq r < d \), we must have \( r = 0 \). That is, we have proved that for any \( s \in S \) we can write \( s = qd \), so \( S \subseteq \mathbb{Z}d \).

Uniqueness. We just have to show that if \( \mathbb{Z}d = \mathbb{Z}e \), then \( d = \pm e \). Note that this is the same as saying \( d \mid e \) and \( e \mid d \). \( \square \)

In particular, for any \( a, b \in \mathbb{Z} \) there is a unique non-negative \( d \) such that
\[
I(a, b) = \mathbb{Z}d.
\]
This integer \( d \geq 0 \) has the properties that:
- \( d \mid a \) and \( d \mid b \)
- \( d = xa + yb \) for some \( x, y \in \mathbb{Z} \).

Guess what: this \( d \) is the GCD.

4.9. Theorem. If \( a, b \in \mathbb{Z} \), with \( a, b \) not both 0, and let \( d \geq 0 \) be such that \( I(a, b) = \mathbb{Z}d \). Then \( \gcd(a, b) = d \); in particular, a GCD exists.

Proof. Because \( I(a, b) = \mathbb{Z}d \) we have that \( a, b \in \mathbb{Z}d \), so \( d \mid a \) and \( d \mid b \), i.e., \( d \) is a common divisor.

Suppose \( c \) is also a common divisor, with \( c \mid a \) and \( c \mid b \). Then any integer combination of \( a \) and \( b \) is also a multiple of \( c \), i.e., \( I(a, b) \subseteq \mathbb{Z}c \). Since \( I(a, b) = \mathbb{Z}d \) we have that \( \mathbb{Z}d \subseteq \mathbb{Z}c \), i.e., \( c \mid d \). \( \square \)

5. Euclidean algorithm

5.1. Lemma. \( \gcd(a, b) = \gcd(b, a - kb) \).

Proof. Show that \( I(a, b) = I(b, a - kb) \):
\[
ma + nb = (n + mk)b + m(a - kb), \quad mb + n(a - kb) = na + (m - nk)b.
\]
\( \square \)

In particular
\[
\gcd(a, b) = \gcd(b, r) \quad \text{where } r = \text{remainder of } a \div b,
\]
since \( r = a - kb \) for some \( k \). This gives the Euclidean algorithm for computing \( \gcd(a, b) \) (assume \( b \geq 0 \)).

- We have \( \gcd(a, b) = \gcd(b, r) \) where \( r \) is the remainder. Iterate this.
- Since \( 0 \leq r < b \), the second input decreases at each step until it reaches 0, so the process terminates.
- We have \( \gcd(a, 0) = a \).

Example. Compute \( \gcd(52, 20) \):
\[
\begin{align*}
54 &= (2)20 + 14, & \gcd(54, 20) &= \gcd(20, 14) \\
20 &= (1)14 + 6, & \gcd(20, 14) &= \gcd(14, 6) \\
14 &= (2)6 + 2, & \gcd(14, 6) &= \gcd(6, 2) \\
6 &= (3)2 + 0, & \gcd(6, 2) &= \gcd(2, 0) = 2.
\end{align*}
\]
6. Relative primeness

We say that $a, b$ are relatively prime if $\gcd(a, b) = 1$. That is, if the only common factors of $a$ and $b$ are $\pm 1$. (Another term used is coprime.)

6.1. Proposition. $a$ and $b$ are relatively prime if and only if $1 = ma + nb$ for some $m, n \in \mathbb{Z}$.

This fact is magical. Basically, every interesting fact about relatively prime integers uses this observation.

6.2. Exercise (Important. On PS 1). Let $a, b$ be relatively prime integers. Show that if $a | bc$ then $a | c$.

(Hint: use the magic fact.)

Show that this is the same as: if $a, b$ are relatively prime and $a | n$ and $b | n$, then $ab | n$.

Note: Don’t try to use prime factorization to prove this: I will need the above fact as part of the proof of prime factorization.

6.3. Exercise (On PS 1). Let $a_1, \ldots, a_k$ be integers that are pairwise relatively prime, i.e., $\gcd(a_i, a_j) = 1$ for all $i \neq j$. Show that if $a_i | n$ for all $i = 1, \ldots, n$, then $a_1 \cdots a_k | n$. (Hint: use induction on $k$ and the previous exercise.)

7. Prime numbers

A positive integer $p$ is prime if exactly two positive integers divide $p$ (namely 1 and $p$).

Note: this excludes 1.

Warning: Do not confuse “prime” with “relatively prime”. Prime is a property of a positive integer: 2, 3, 5, etc. are, while 1, 4, 6, 8, 9, etc. aren’t.

The following lemma is the key fact about prime numbers.

7.1. Lemma. If $p$ prime and $p | ab$, then either $p | a$ or $p | b$.

Proof. The observation is that for $p$ prime and $m \neq 0$, $\gcd(p, m) \in \{1, m\}$, depending on whether $p$ divides $m$ or not.

We will show that $p | ab$ and $p \nmid a$ imply $p | b$. Since $p \nmid a$, then $xp + ya = 1$ for some $x, y$. Multiply by $b$ to get

$$xp + yab = b,$$

i.e., $b \in I(p, ab)$. Since $p | ab$ by hypothesis and $p | p$, we get $p | b$ as desired.

7.2. Exercise (On PS 1). Prove the converse of the above lemma. That is, if $p \in \mathbb{N}$ with $p > 1$ has the property that $p | ab$ implies $p | a$ or $p | b$, then $p$ must be prime.

7.3. Corollary. If $p | a_1 \cdots a_k$ then $p | a_i$ for some $i$.

Proof. Induction on $k$.

7.4. Proposition. Every $n \geq 2$ is prime or is a product of primes.

Proof. Induction on $n$. Note that 2 is prime (base case). For a given $n$, either it is prime, or it has a divisor $a$ such that $1 < a < n$, and $n = ab$ with $1 < b < n$. In this case we have that $a$ and $b$ have prime factorizations by induction, and the result follows.

So every $n \geq 2$ has a prime factorization: $n = p_1 \cdots p_k$, where each $p_i$ is prime. These are unique.

7.5. Proposition. If $n \geq 2$ is such that $n = p_1 \cdots p_k = q_1 \cdots q_\ell$ where the $p_i$ and $q_j$ are primes, then $k = \ell$ and the lists $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$ are the same up to reordering.

Proof. Induction on $n$. If $n$ is prime then it is clear the factorization is unique. If not then consider $m = n/p_k$. By a previous result, $p_k$ must divide some $q_j$, whence $p_k = q_j$ since both are prime, and we get $m = p_1 \cdots p_{k-1} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_\ell$. By induction, $k - 1 = \ell - 1$ and the lists $p_1, \ldots, p_{k-1}$ and $q_1, \ldots, q_{j-1}, q_{j+1}, \ldots, q_\ell$ are the same up to reordering.
7.6. **Theorem** (Euclid). There are infinitely many primes.

*Proof.* If there are finitely many distinct primes $p_1, \ldots, p_k$, let $n = 1 + p_1 \cdots p_k$. Then no $p_i$ divides $n$, since only 1 divides 1. Clearly $n > p_i$ for all $i$, so if $n$ is prime, it is not in the original list. If $n$ is not prime it is composite, and so has a prime factor $q$, which is not in the original list. □

8. **Equivalence relations and equivalence classes**

Equivalence relations are a way to parcel up sets into non-intersecting pieces.

A relation on a set $S$ is a subset $R \subseteq S \times S$ of the set of ordered pairs $(a, b)$ of elements of $S$. We often use notation:

$$a \sim_R b \iff (a, b) \in R,$$

and say “$a$ is related to $b$ by $R$”. (Often just write “$a \sim b$”, or use some other specific notation.)

Familiar examples of relations on $S = \mathbb{R}$:

- equality $=$,
- $<$,
- $\leq$.

8.1. **Example.** The divisibility relation $a \mid b$ is a relation on $\mathbb{Z}$. Another relation is “relative primeness”.

Say that a relation $\sim$ on $S$ is an **equivalence relation** if

1. (reflexive) $x \sim x$ for all $x \in S$,
2. (symmetric) $x \sim y$ implies $y \sim x$ for all $x, y \in S$,
3. (transitive) $x \sim y$ and $y \sim z$ imply $x \sim z$ for all $x, y, z \in S$.

Example: equality is an equivalence relation on any set.

Non-examples: $<$ and $\leq$ are not equivalence relations on $\mathbb{R}$. The divisibility relation “$a$” is not an equivalence relation.

8.2. **Exercise** (On PS 2). Let $\sim$ be the relation on $\mathbb{Z}$ defined by: $a \sim b$ if $\gcd(a, b) = 1$. Determine which of the properties of equivalence relation are satisfied by $\sim$.

8.3. **Example.** Say that $\alpha, \beta \in \mathbb{R}$ determine the **same angle** if $\alpha - \beta = 2\pi n$ for some integer $n$. This implicitly defines an equivalence relation on $\mathbb{R}$:

$$\alpha \sim \beta \iff \alpha - \beta \in 2\pi \mathbb{Z}.$$

An **equivalence class** of an equivalence relation $(S, \sim)$ is a subset $C \subseteq S$ such that

1. $C$ is non-empty, and
2. if $x \in C$ and $s \in S$, then $s \in C$ if and only if $x \sim s$.

8.4. **Example.** For the equality relation on any set, the equivalence classes are the singleton sets $\{a\}$.

8.5. **Example.** For the “same angle” relation on $\mathbb{R}$, a typical equivalence class looks like

$$C = \{ \theta + 2\pi n \mid n \in \mathbb{Z} \} = \{ \ldots, \theta - 4\pi, \theta - 2\pi, \theta, \theta + 2\pi, \theta + 4\pi, \ldots \}.$$

Given $s \in S$, let $[s] = \{ x \in S \mid x \sim s \}$.

8.6. **Lemma.** $[s]$ is an equivalence class, and $s \in [s]$.

Thus, $[s]$ is “the equivalence class of $s$”.

We can restate everything about equivalence relations in terms of the “[s]” notation for equivalence classes: $x \sim y$ iff $[x] = [y]$.

8.7. **Exercise.** Let $\sim$ be an equivalence relation on $S$, and $x, y \in S$. The following are equivalent.

1. $x \sim y$.
2. $x \in [y]$.
3. $y \in [x]$.
4. $[x] = [y]$.
5. $[x] \cap [y] \neq \emptyset$. 
8.8. **Proposition.** For an equivalence relation \((S, \sim)\), every element of \(S\) is contained in exactly one equivalence class.

**Proof.** Exercise. □

A **partition** of a set \(S\) is a collection \(\{C_\alpha\}\) of subsets such that

1. each \(C_\alpha\) is non-empty,
2. \(C_\alpha \cap C_\beta = \emptyset\) unless \(C_\alpha = C_\beta\),
3. \(\bigcup C_\alpha = S\).

8.9. **Proposition.** The equivalence classes of an equivalence relation form a partition, and every partition comes from an equivalence class in this way.

**Proof.** Exercise. □

Given an equivalence relation \((S, \sim)\), we write \(S/\sim\) for the set of equivalence classes.

Equivalence classes give us a (surprising) way to create new mathematical objects. For instance, we can define an **angle** to be an equivalence class of the “same angle” relation on real numbers. Thus, we abstractly identify an angle \(\alpha\) with the set of all real numbers which represent it (in radians). For instance, the angle \(\alpha = \{\ldots, -11\pi/4, -7\pi/4, \pi/4, 9\pi/4, \ldots\}\) is the one at slope = 1. This equivalence class comes with many names: \(\alpha = [\pi/4] = [9\pi/4] = \ldots\).

In practice, we often make a choice of “canonical representative” for each equivalence class. For an equivalence relation \((S, \sim)\), a set of **representatives** is a subset \(R \subseteq S\) such that for each equivalence class \(C\), the intersection \(C \cap R\) contains exactly one element \(x\).

8.10. **Example.** For an equivalence class \(\alpha\) of the angle relation, there is a unique element \(\theta\) in \(\alpha \cap [0, 2\pi)\), and we can use this \(\theta\) as the canonical representative of \(\alpha\).

This is not the only choice, or even the only obvious choice. For instance, we could instead use the unique element \(\psi\) in \(\alpha \cap (-\pi, \pi]\). You have probably seen examples of both of these choices. There are infinitely other ways to make such a choice.

8.11. **Exercise** (On PS 2). Let \(S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\}\). Say \((a, b) \sim (c, d)\) iff \(ad = bc\).

1. Using only properties of the integers, show that \(\sim\) is an equivalence relation.
2. Show that every equivalence class \(C\) contains a unique element \((u, v)\) with the properties that (i) \(v > 0\), and (ii) \(\gcd(u, v) = 1\).

Part (2) gives us a standard way to choose a canonical representative.

(This exercise is basically having you prove that: fractions make sense, and can be written uniquely in lowest terms.)

Note: for (1), you’ll need to use the fact that if \(x, y \in \mathbb{Z}\) and \(xy \neq 0\) then \(x \neq 0\) and \(y \neq 0\). For (2), you’ll need the fact we proved: if \(\gcd(a, b) = 1\), then \(a|bc\) implies \(a|c\).

In these examples, there is a reasonably good choice of canonical representatives. However, in practice there may not be. (Or at least, finding a “good choice of representative” itself turns out to be a difficult problem to solve.)

8.12. **Example.** (It turns out nobody does Jordan Canonical Form in 416, so this example wasn’t very helpful.) Let \(M_{n \times n}(F)\) be the set of \(n \times n\) matrices over a field \(F\), e.g., \(\mathbb{R}\) or \(\mathbb{C}\). We say that \(A, B \in M_{n \times n}(F)\) are **similar** and write \(A \sim B\) if there exists an invertible matrix \(P\) such that \(B = PAP^{-1}\). Exercise: similarity is an equivalence relation on \(M_{n \times n}(F)\).

Is there a canonical form for similarity classes? When \(F = \mathbb{C}\) you may have learned the answer in your linear algebra class: they are the Jordan canonical forms. (Actually, even this is not quite right: Jordan forms are matrices built out of Jordan blocks along the diagonal, but the Jordan blocks can
be reordered without changing the equivalence class. So there is still a little bit of arbitrary choice involved.) (Give examples.)

When \( F = \mathbb{R} \) (or any other field), there is a more sophisticated version of the theorem. (Called “rational canonical form”, which is probably in your linear algebra text somewhere, but probably wasn’t covered in class.)

8.13. Example. Let \( S \subseteq M_{n \times n}(\mathbb{R}) \) be the set of real symmetric matrices: \( A = A^\top \). A famous theorem says these are diagonalizable with all real eigenvalues. Thus, each similarity class of elements of \( S \) contains a unique diagonal matrix where the diagonal entries are in monotonic order: \( \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n \).

9. Modular arithmetic

We fix a positive integer \( n \geq 1 \), called the modulus. Define an equivalence relation \( \sim \) on \( \mathbb{Z} \) by

\[
x \sim y \iff x - y = kn \text{ for some } k \in \mathbb{Z}.
\]

Typically, we write “\( x \equiv y \mod n \)” for this relation, or even sometimes \( x \equiv_n y \), and say that \( x \) and \( y \) are congruent modulo \( n \). Thus, \( x \equiv_n y \) iff \( x - y \in \mathbb{Z}n \).

9.1. Proposition. This is an equivalence relation on \( \mathbb{Z} \).

The equivalence classes have the form \( [x]_n = \{ x + kn \mid k \in \mathbb{Z} \} \), and are called congruence classes.

9.2. Proposition. Congruence modulo \( n \) has exactly \( n \) distinct equivalence classes. Each equivalence class \( C \) contains exactly one element from the set \( \{0, 1, \ldots, n - 1\} \).

Proof. The first statement follows from the second, which is a consequence of the division algorithm. If \( C = [x] \), we have \( x = qn + r \) for unique \( q, r \) with \( 0 \leq r < n \), so \( r \) is the only integer in the range \( [0, n) \) such that \( [x] = [r] \).

9.3. Remark. There are other convenient ways to choose canonical representatives:

- If \( n = 2k + 1 \) is odd, then every congruence class contains exactly one element from \( \{-k, -k + 1, \ldots, k - 1, k\} \). (E.g., \( n = 5 \), \( \{-2, -1, 0, 1, 2\} \).
- If \( n = 2k \) is even, then every congruence class contains exactly one element from \( \{-k + 1, -k + 2, \ldots, k - 1, k\} \). (E.g., \( n = 6 \), \( \{-2, -1, 0, 1, 2, 3\} \).

We write \( \mathbb{Z}/n \) for the set of congruence classes modulo \( n \). (Many notations are used; most textbooks use \( \mathbb{Z}_n \), although this notation is not used as much nowadays by mathematicians.)

We can define addition and multiplication of elements in \( \mathbb{Z}/n \):

\[
[a] + [b] := [a + b], \quad [a][b] := [ab].
\]

There is a major issue here, namely to show that these operations are well-defined. The problem is that the definitions are only given in terms of “names” of the equivalence classes, and an equivalence class has many different names. That they are well-defined comes from the following.

9.4. Proposition. If \( a \equiv_n a' \) and \( b \equiv_n b' \), then \( a + b \equiv_n a' + b' \) and \( ab \equiv_n a'b' \).

Example: For \( n = 5 \), we have \([17] + [9] = [26] \), but we know \([17] = [2] \) and \([9] = [4] \), and \([2] + [4] = [6] \). This is ok because \([26] = [6] \).

9.5. Proposition. For a positive integer \( m \), \( 9 | m \) if and only if 9 divides the sum of the digits of \( m \).

Proof. If \( m \) has base 10 representation \( a_k \cdots a_1 a_0 \) with \( a_i \in \{0, 1, \ldots, 9\} \), then \( m = \sum_i a_i(10)^i \). In \( \mathbb{Z}/9 \) we have

\[
[10] = [1], \quad \implies \quad [(10)^j] = [10]^j = [10] \cdots [10] = [1] \cdots [1] = [1],
\]
and so
\[ [a_k(10)^k + \cdots + a_1(10) + a_0] = [a_k][10^k] + \cdots + [a_1][10] + [a_0] = [a_k] + \cdots + [a_1] + [a_0]. \]
In other words,
\[ m \equiv a_k + \cdots + a_0 \mod 9. \]

10. Groups

A binary operation on a set \( S \) is a function \( S \times S \to S \), which is written using “infix notation”, e.g.,
\[ (a, b) \mapsto a \cdot b. \]
There are many symbols we might use here: +, −, ×, ÷, ⊕, ⊗, ·, ◦, or nothing at all (which is how we ordinarily write multiplication). Much of the time will use \( ab \), but will allow \( a \cdot b \) as an alternate form.

We can chain binary operations to get more complicated operations. For instance, the formulas
\[(x * y) * z \quad \text{and} \quad x * (y * z) \]
define three-fold operations on a set.

Note: a binary operation is just a function which is written with a funny notation. There is no requirement that it satisfy any particular rules: i.e., you don’t necessarily have \( a * b = b * a \) or any other such rule.

10.1. Example. Let \( S = \mathbb{R}^3 \), the set of 3d vectors. The operation vector cross product is a binary operation on \( \mathbb{R}^3 \):
\[ u, v \mapsto u \times v. \]

A group \((G, \cdot)\) consists of a set \( G \) together with a binary operation \( \cdot : G \times G \to G \) satisfying the following rules.

1. (Associativity) We have \((xy)z = x(yz)\) for all \( x, y, z \in G \).
2. (Identity) There exists an element \( e \in G \) such that \( xe = x = ex \) for all \( x \in G \).
3. (Inverse) For each \( x \in G \), there exists an element \( y \in G \) such that \( xy = e = yx \), where \( e \) is an element as in (2).

Note that a group consists of both a set and an operation. Just giving a set does not tell you what the group structure is. However, by abuse of notation we often just write the name of the set \( G \) for the whole group (hoping that the operation is understood). This is usually ok, but sometimes you need to be careful.

First, some basic facts.

- The element \( e \) of (2) is actually unique. That is, if \( e, f \in G \) are both such that \( xe = x = ex \) and \( xf = x = fx \) for all \( x \in G \), then we must have \( e = f \). Proof: Take \( x = e \) or \( f \).
\[ ef = e \quad \text{and} \quad ef = f. \]
We call \( e \) the identity element. Another common notation for it is 1.
- For a given \( x \), the element \( y \) of (3) is actually unique. That is, if \( y, z \in G \) such that \( xy = e = yx \) and \( xz = e = zx \), then \( x = z \). Proof:
\[ (yx)z = ez = z, \quad y(xz) = ye = y, \]
and these are same since associativity says \((yx)z = y(xz)\).
We call \( y \) the inverse of \( x \), and write \( y = x^{-1} \).

Variants:

- If \((G, \cdot)\) only satisfies (1) and (2), it is called a monoid.
- If \((G, \cdot)\) only satisfies (1), it is called a semi-group. (We will never talk about these.)
- If \((G, \cdot)\) satisfies the additional property:
(4) We have $xy = yx$ for all $x, y \in G$.
then we say that $G$ is a **commutative group**, or an **abelian group** (named for Niels Henrik Abel). (We can also talk about commutative monoids or commutative semi-groups.)

10.2. *Example.* $(\mathbb{R}, +)$, the real numbers with addition, is a commutative group.

10.3. *Example.* $(\mathbb{R}, \cdot)$, the real numbers with multiplication, is a commutative monoid. It is not a group, since 0 does not have a multiplicative inverse.

$(\mathbb{R} \setminus \{0\}, \cdot)$ is a commutative group. (Because the product of non-zero numbers is non-zero, and all such have a multiplicative inverse.)

10.4. *Example.* $(M_{n \times n}(\mathbb{R}), \cdot)$, the $n \times n$ real matrices with multiplication is a monoid, but not a group, and is not commutative (when $n \geq 2$).

$GL_n(\mathbb{R}) = \{ A \in M_{n \times n}(\mathbb{R}) \mid \det A \neq 0 \}$ together with multiplication is a group, not-commutative if $n \geq 2$.

In the above examples, we can replace $\mathbb{R}$ with any field, e.g., $\mathbb{Q}$ or $\mathbb{C}$.

10.5. *Exercise.* Fix a positive real number $c$, and let $S = (-c, c) \subseteq \mathbb{R}$. Consider the formula

$$x \ast y := \frac{x + y}{1 + c^{-2}xy}.$$  

Show that this defines a binary operation on $S$, which makes $(S, \ast)$ into an abelian group. Explain why the formula does not define a group structure on $\mathbb{R}$.

*Bonus:* Where have you seen this operation before (perhaps in a physics class)?

By an **additive group**, we mean a group $(G, +)$ in which the operation is written using a “+” sign. By convention, additive groups are always abelian: we only use “+” for commutative operations. For additive groups, the identity element is denoted “0”, and the inverse of $x$ is denoted “$-x$”.

10.6. *Example.* The integers $(\mathbb{Z}, +)$ with addition are an additive group. (The non-negative integers $(\mathbb{Z}_{\geq 0}, +)$ are merely a monoid.)

10.7. *Example.* If $V$ is any vector space (over any field $F$), then $(V, +)$ is an additive group.

10.8. *Example.* For any $n$, $(\mathbb{Z}/n, +)$ is an additive group.

11. **Rings**

A **ring** is $(R, +, \cdot)$, consisting of a set $R$ and two binary operations on $R$ (called “addition” and “multiplication”) such that

- $(R, +)$ is an abelian group,
- $(R, \cdot)$ is a monoid, and
- (Distributive law) $a(b + c) = (ab) + (ac)$ and $(b + c)a = (ba) + (ca)$ for all $a, b, c \in R$.

Note that $(R, +)$ is an additive group, so 0 is the identity and $-x$ the inverse. Typically one writes 1 for the identity of multiplication.

A **commutative ring** is one in which multiplication is commutative: $ab = ba$.

A **field** is a commutative ring such that every non-zero element has a multiplicative inverse, and also $1 \neq 0$.

Examples: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $M_{n \times n}(R)$ where $R$ is a ring, $R[x]$ (polynomials in the variable $x$ with coefficients in a ring $R$).

We will study rings in more depth later in the course.

---

1This is just some set $R$, not necessarily the set of real numbers $\mathbb{R}$. 

12. Subgroups

Given a group $G$, a **subgroup** is a subset $H \subseteq G$ such that (i) the binary operation $\cdot : G \times G \to G$ restricts to an operation $H \times H \to H$, such that (ii) $(H, \cdot)$ is a group.

12.1. Example. The set of integers $\mathbb{Z}$ is subgroup of the additive group $(\mathbb{R}, +)$.

12.2. Example. The set $\{\pm 1\}$ is a subgroup of $\mathbb{R} \times = (\mathbb{R} \setminus \{0\}, \cdot)$.

12.3. Exercise (On PS 3?). Recall that a real matrix $A \in M_{n \times n}(\mathbb{R})$ is **orthogonal** if $A^\top A = I = AA^\top$.

Show that the set $O(n)$ of orthogonal $n \times n$ matrices is a subgroup of $GL_n(\mathbb{R})$.

12.4. Proposition. Let $(G, \cdot)$ be a group and $H \subseteq G$ a subset such that

1. if $x, y \in H$ then $xy \in H$, (“closed under multiplication”)
2. the identity element $e$ of $G$ is an element of $H$,
3. if $x \in H$, then the inverse $x^{-1}$ of $x$ in $G$ is an element of $H$.

Then $(H, \cdot)$ is a subgroup.

*Proof.* (1) tells us that $\cdot$ actually restricts to a function $\cdot : H \times H \to H$. (2) tells us that $H$ has an identity element (which is the same as the identity element of $G$). (3) tells us that any element of $H$ has an inverse (which is the same as the inverse in $G$). □

We have already introduced the notion of “subgroup” for the additive group $\mathbb{Z}$, and we proved that every subgroup of $\mathbb{Z}$ has the form $\mathbb{Z}d$ for a unique $d \geq 0$.

13. Multiplication tables

Let $G = \{e, a, b, c\}$ be a set with 4 elements, with multiplication defined by the following table.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>e</td>
</tr>
</tbody>
</table>

(Read this so that $xy$ is computed by looking up the spot at row $x$, column $y$.) This turns out to define an abelian group. (Associativity is not obvious.) This group is called the **Klein four-group**.

13.1. Exercise (On PS2). Consider the set $G$ consisting of the following matrices:

$$
e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Check that $G$ is a subgroup of $GL_2(\mathbb{R})$, and that its multiplication table is as given above.

13.2. Exercise (On PS2). Determine all the subgroups of the Klein four-group.

14. Direct products of groups

Given groups $G$ and $H$, we define the **product group** $G \times H$ as follows. The elements of $G \times H$ are ordered pairs $(g, h)$. The product is given by

$$(g, h) \cdot (g', h') := (gg', hh').$$

Exercise: show that this defines a group structure.

The multiplication on $G \times H$ is defined “componentwise”.

14.1. Exercise. Show that the subsets $G' := \{(g, e_H) \mid g \in G\}$ and $H' := \{(e_G, h) \mid h \in H\}$ are subgroups of the direct product $G \times H$. 
15. Inverses and Cancellation

Most of these should be exercises.

- If \( ab = e \), then \( ab = ba \), \( a = b^{-1} \), and \( a^{-1} = b \). (Prove in class.)
- We have that \( (a^{-1})^{-1} = a \). (Prove in class.)
- We have that \( (ab)^{-1} = b^{-1}a^{-1} \). (Exercise)
- If \( a_1 \cdots a_k = e \) then \( a_2 \cdots a_k a_1 = e \). (Exercise)
- (Cancellation) If \( ac = bc \) then \( a = b \); if \( ca = cb \), then \( a = b \).
- For any \( a, b \) there exist \( x \) and \( y \) such that \( ax = b \) and \( ya = b \).

Given a group \( G \) and element \( g \in G \), we get left multiplication and right multiplication by \( g \) functions

\[
L_g, R_g: G \to G, \quad L_g(x) := gx, \quad R_g(x) := xg.
\]

15.1. Corollary. Both \( L_g \) and \( R_g \) are bijections \( G \to G \).

For instance, if \( G \) has finitely many elements and we list them without repetition as: \( a_1, \ldots, a_n \), then the list \( ga_1, \ldots, ga_n \) is also all elements of \( G \) without repetition (but possibly in a different order). Likewise the list \( a_1g, \ldots, a_ng \).

These lists are the rows and columns of the multiplication table of \( G \).

16. General associative law

Associativity says \( (ab)c = a(bc) \), and we celebrate this by simply writing \( abc \) for this expression, since the parentheses don’t matter.

Given four elements, we see that there are five different products:

\[
((ab)c)d, \quad (a(bc))d, \quad a((bc)d), \quad a(b(cd)), \quad (ab)(cd)
\]

16.1. Remark. You can represent these by “binary trees” with four leaves.

These are all equal. (Proof: \( (a(bc))d = ((ab)c)d = (ab)(cd) = a(b(cd)) = a((bc)d) \).) If we remember 3-fold associativity, this is really just three different expressions:

\[
(abc)d = (ab)(cd) = a(bcd).
\]

We write \( abcd \) for any of these.

Given five elements, we have that

\[
a(bcd) = (ab)(cd) = (abc)(de) = (abcd)e.
\]

Each of these can be proved by using associativity to slide the rightmost element in the left bracket to be the leftmost element in the right bracket. E.g.,

\[
(abc)(de) = ((ab)c)(de) = (ab)(c(de)) = (ab)(cde).
\]

We can thus write \( abcd \) for any of these 5-fold products. Likewise there are 14 different ways to write 6-fold products, which turn out to all be the same.\(^2\) We can now state this in arbitrary generality.

16.2. Proposition. Let \( G \) be a group. There is a unique collection of functions \( G^n \to G \), defined for each \( n \geq 1 \), (which we write as \( "(a_1, \ldots, a_n) \mapsto a_1a_2 \cdots a_n" \)), such that

1. For \( n = 1 \), the function \( G \to G \) sends \( a \mapsto a \).
2. For \( n = 2 \), the function \( G \times G \to G \) is the product \( (a_1, a_2) \mapsto a_1a_2 \).
3. For all \( 1 \leq k < n \) and \( n \geq 3 \), we have \( a_1a_2 \cdots a_n = (a_1 \cdots a_k)(a_{k+1} \cdots a_n) \).

\(^2\)The numbers 1, 1, 2, 5, 14, 42, 132, 429, \ldots, \frac{1}{n+1} \binom{2n}{n}, \ldots \) are called the Catalan numbers.
Proof. Let’s define “\(a_1 \cdots a_n\)” inductively (on \(n\)) by

\[ a_1 \cdots a_n := (a_1 \cdots a_{n-1})a_n. \]

Thus,

\[ a_1a_2a_3 := (a_1a_2)a_3, \quad a_1a_2a_3a_4 := ((a_1a_2)a_3)a_4, \quad a_1a_2a_3a_4a_5 := (((a_1a_2)a_3)a_4)a_5, \quad \ldots \]

These formulas are forced on us by (3), using the case \(k = n - 1\). So if there is a solution, it must be these functions. We still need to check the other cases of (3) to know that it the function behaves the way we want.

We now show (3): that \((a_1 \cdots a_k)(a_{k+1} \cdots a_n) = a_1 \cdots a_n\) for all \(1 \leq k < n\) by induction on \(n\). If \(k = n - 1\), it’s just the definition, while if \(k < n - 1\) we have:

\[
\begin{align*}
(a_1 \cdots a_k)(a_{k+1} \cdots a_n) &= (a_1 \cdots a_k)((a_{k+1} \cdots a_{n-1})a_n) \quad \text{definition,}
&= ((a_1 \cdots a_k)(a_{k+1} \cdots a_{n-1}))a_n \quad \text{associativity,}
&= (a_1 \cdots a_{n-1})a_n \quad \text{induction,}
&= a_1 \cdots a_n \quad \text{definition.}
\end{align*}
\]

□

From now on, I will leave out parentheses when I can.

Note that the above proof did not use inverses or identity, so it is true in any semigroup. For instance, it applies to multiplication in a ring.

17. Powers of elements

Given an element \(a\) of a group, we define \(a^n\) for every \(n \in \mathbb{Z}\) as follows:

\[ a^n = \begin{cases} 
  a^{n-1}a & \text{if } n \geq 2, \\
  a & \text{if } n = 1, \\
  e & \text{if } n = 0, \\
  a^{-1} & \text{if } n = -1, \\
  a^{n+1}a^{-1} & \text{if } n \leq -2.
\end{cases} \]

Note that this is an inductive definition (in two places).

17.1. Lemma. For all \(n \in \mathbb{Z}\), \(a^{n+1} = a^na\).

Proof. Break into cases. (This is a little tedious.) □

17.2. Proposition. For all \(m, n \in \mathbb{Z}\) we have \(a^ma^n = a^{m+n}\).

Proof. Fix \(m \in \mathbb{Z}\) and suppose \(n \geq 0\). We first show that \(a^ma^n = a^{m+n}\) by induction on \(n\).

If \(n = 0\), then \(a^m a^0 = a^m e = a^m = a^{m+0}\).

For \(n \geq 0\), we have

\[
\begin{align*}
  a^m a^{n+1} &= a^m(a^n a) \quad \text{by lemma}
&= (a^m a^n) a \quad \text{associativity,}
&= a^{m+n}a \quad \text{by induction on } n
&= a^{m+n+1} \quad \text{by lemma.}
\end{align*}
\]

A similar proof (exercise) handles the case of \(n < 0\). □

17.3. Exercise. Show that \((a^m)^n = a^{mn}\). (Hint: break into cases \(n < 0, n = 0, n > 0\). For the \(n \neq 0\) cases, use induction on \(n\).)
In an additive group \((G, +)\) we write

“\(ka\)” instead of “\(a^k\),”

where \(a \in G\) and \(k \in \mathbb{Z}\). Thus in an additive group we have \(0a = 0\), \(1a = a\), \((-1)a = -a\), and we have the rules:

\[
ma + na = (m + n)a, \quad m(na) = (mn)a, \quad a \in G, \, m, n \in \mathbb{Z}.
\]

Note: the way we work with additive groups is a lot like the way we work with vector spaces. In particular, “\(ka\)” is a kind of “scalar multiplication”, where scalars are just integers.

18. ORDER OF ELEMENTS

Let \(a\) be an element of a group \(G\). We say that \(a\) has **order** \(n \in \mathbb{N}\) if \(n\) is the smallest positive integer such that \(a^n = e\), and we write order\((a) = n\). If no such smallest integer exists, we say that \(a\) has **infinite order**, and write order\((a) = \infty\).

**Easy fact:** the only element with order 1 is \(e\). (Exercise.)

**Remark:** if any positive power of \(a\) is the identity, then the WOP implies that \(a\) has a finite order. Thus, \(a\) has infinite order when all positive (in fact, non-zero) powers of \(a\) are not equal to \(e\).

18.1. **Example.** Consider \(R = \left( \begin{array}{cc} -\sqrt{3}/2 & -1/2 \\ 1/2 & -\sqrt{3}/2 \end{array} \right) \) in \(GL_2(\mathbb{R})\). Check that order\((R) = 3\). This is clear when you realize that \(v \mapsto Rv\) gives rotation of the plane through a 120° angle.

Likewise, let \(A = \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \), and note that order\((A) = 2\).

18.2. **Exercise (PS 3).** Show that the subset \(G := \{ R^i A^j \mid i, j \in \mathbb{Z}\} \subseteq GL_2(\mathbb{R})\) is a **subgroup**. Prove that \(|G| = 6\), and compute the orders of all six elements of \(G\). (Hint: to show it is a subgroup prove and make use of the identity \(AR = R^{-1}A\).)

18.3. **Lemma.** Given \(a \in G\), let

\[
S := \{ k \in \mathbb{Z} \mid a^k = e \}.
\]

Then \(S\) is a subgroup of \(\mathbb{Z}\), and we have \(S = \mathbb{Z}n\) for a unique \(n \geq 0\). If \(n = 0\) then order\((a) = \infty\), while if \(n > 0\) then order\((a) = n\).

**Proof.** First, it is straightforward to show that \(S\) is a subgroup of \(\mathbb{Z}\) using the criterion: (i) if \(i, j \in S\), then \(a^{i+j} = a^i a^j = ee = e\) so \(i + j \in S\); (ii) since \(a^0 = e\) we have \(0 \in S\); (iii) if \(i \in S\), then \(a^{-i} = (a^i)^{-1} = e^{-1} = e\) so \(-i \in S\).

Thus \(S = \mathbb{Z}n\) for a unique \(n \geq 0\). If \(n = 0\) then \(S\) contains no positive elements, so order\((a) = \infty\). If \(n > 0\), then \(n\) is the smallest positive element of \(S\), so order\((a) = n\).

As a consequence, we have that if \(a^d = e\) for \(d \neq 0\), then order\((a)|d\).

**Warning.** If someone says that \(a^d = e\), it does not imply that the order of \(a\) is \(d\), merely that the order **divides** \(d\). For instance, if I tell you that \(a^6 = e\), then all you know is that order\((a) \in \{1, 2, 3, 6\}\); it is even possible that \(a\) is the identity element.

18.4. **Lemma.** Let \(n = \text{order}(a)\).

(1) If \(n < \infty\), then \(a^s = a^t\) if and only if \(s \equiv t \mod n\).

(2) If \(n = \infty\), then \(a^s = a^t\) if and only if \(s = t\).

**Proof.** Let \(S = \{ k \in \mathbb{Z} \mid a^k = e \}\). Note that \(a^s = a^t\) if and only if \(a^{s-t} = e\) if and only if \(s - t \in S\).

For (1), we have \(S = \mathbb{Z}n\), so \(a^s = a^t\) if \(s - t \in \mathbb{Z}n\), i.e., if \(s \equiv t \mod n\).

For (2), we have \(S = \mathbb{Z}0 = \{0\}\), so \(a^s = a^t\) if \(s - t \in \mathbb{Z}0\), i.e., if \(s = t\). □
A consequence: if order\( (a) = n < \infty \), then every power of \( a \) can be written as \( a^k \) with exactly one \( k \) such that \( 0 \leq k < n \) (by the division algorithm).

The order (or size) of a group \( G \) is the number of elements in its set. We write \( |G| \) for the order of the group, which can be a positive number or infinite.

Warning: “order of a group” is not defined in the same way as “order of an element in the group”, but they are related in the following way.

18.5. Proposition. Given \( a \in G \), let \( H := \{ a^k \mid k \in \mathbb{Z} \} \) be the subset of \( G \) consisting of all powers of \( a \). Then \( H \) is a subgroup of \( G \), and \( |H| = \text{order}(a) \) as defined above.

Proof. To check that \( H \) is a subgroup is straightforward, using the criterion we established: (i) Given \( a^m, a^n \in H \), we certainly have \( a^m a^n = a^{m+n} \in H \); (ii) we have \( e = a^0 \in H \); (iii) If \( a^n \in H \), then \( (a^m)^{-1} = a^{-m} \in H \).

For the statement about size, we give a bijection between \( H \) and either \( \mathbb{Z}/n\mathbb{Z} \) or \( \mathbb{Z} \), depending on whether \( n = \text{order}(a) \) is finite or infinite. If \( n < \infty \), define \( \mathbb{Z}/n \to H \) by \( k \mapsto a^k \). By the previous lemma, this is well-defined and a bijection. Likewise, if \( n = \infty \), define \( \mathbb{Z} \to H \) by \( k \mapsto a^k \). \( \square \)

Note: we call \( H = \{ a^k \mid k \in \mathbb{Z} \} \) the cyclic subgroup generated by \( a \). (Soon we will talk about subgroups generated by more than one element.)

Examples.

18.6. Exercise (PS 3). Let \( a \in G \) be an element of order 6. Compute \( \text{order}(a^k) \) for every integer \( k \).

18.7. Proposition. Every element of a finite group has finite order.

Proof. Given \( a \in G \), let \( H = \{ a^k \mid k \in \mathbb{Z} \} \). Since \( G \) is finite and \( H \) is a subset of \( G \), we have \( \text{order}(a) = |H| \leq |G| < \infty \). \( \square \)

Remark. It is not true that every element of an infinite group has infinite order. Example is \( \mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot) \); \( \text{order}(-1) = 2 \).

19. Order Theorem

There is an important result about the order of elements in a finite group.

19.1. Theorem (Order theorem). If \( |G| = n < \infty \), then the order of every element of \( G \) divides \( n \).

19.2. Example. Consider the quaternion group \( Q = \{ \pm I, \pm A, \pm B, \pm C \} \subseteq GL_2(\mathbb{C}) \), with

\[
A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad C = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.
\]

Note that \( AB = C = -BA, BC = A = -CB, CA = B = -AC \), and \( A^2 = B^2 = C^2 = -I \). We have \( |Q| = 8 \). Thus the order of any element of \( Q \) must lie in \( \{1,2,4,8\} \). In fact, order\( (I) = 1 \), order\( (-I) = 2 \), while the order of the remaining 6 elements is 4.

There is a clever proof which works only for finite abelian groups, which I will leave as an exercise.

For the proof I give here, we will set up a new equivalence relation on \( G \). For a general group \( G \) and element \( a \in G \), define an equivalence relation \( \sim_a \) on the set \( G \) by

\[ x \sim_a y \iff \text{exists } k \in \mathbb{Z} \text{ such that } y = a^k x. \]

Exercise: this defines an equivalence relation. (Later the equivalence classes of this will be called “left \( (a)\)-cosets”.)

Example, with pictures. (E.g., \( G = \mathbb{Z}/12, a = [3]_{12} \). Second example: Klein 4-group or quaternion group.)

19.3. Lemma. Every equivalence class \( C \) of this relation has size = \( \text{order}(a) \).
Proof. Write \( d = \text{order}(a) \). Let \( H = \{ a^k \mid k \in \mathbb{Z} \} \), the cyclic subgroup generated by \( a \), so \(|H| = d\). Note that \( H \) is actually an equivalence class for \( \sim_a \).

Consider any other equivalence class \( C \), and choose an element \( g \in C \). Note that \( C = \{ a^kg \mid k \in \mathbb{Z} \} \).

Claim. The function \( \phi : H \to C \) defined by \( x \mapsto xg \) is a bijection. Proof of claim. It is clear this is well-defined, since for \( a^k \in H \) we have \( a^kg \in C \). We also have a function \( C \to H \) by \( y \mapsto yg^{-1} \), and it is easy to check that this is the inverse function to \( \phi \).

Proof of order theorem. The equivalence relation partitions \( G \) into a collection of equivalence classes \( C_1, \ldots, C_m \) (finitely many because \( G \) is a finite set). The lemma proves that each of them satisfy \(|C_i| = d = \text{order}(a)\). Therefore \(|G| = md\), so \( d \) divides the order of \( G \).

The converse is not true. In fact, we earlier gave an example of a group of order 4 (the Klein 4-group) which has no elements of order 4.

19.4. Exercise (Do in class). \( \text{order}(a)|2 \) if and only if \( a = a^{-1} \).

19.5. Exercise (Do in class). If \( G \) is a finite group with an even number of elements, then \( G \) contains an element of order 2. (Hint: partition \( G \) into subsets of the form \( \{a, a^{-1}\} \). These subsets either have size 1 or size 2, depending on whether the element has order dividing 2 or not.)

What can we say about the order of a product of elements, if we know the orders of each? In general, not much. In fact, the product of elements of finite order can have infinite order.

19.6. Exercise (On PS 3). Let \( A = \left( \begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix} \right) \) and \( B = \left( \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \right) \), elements of \( GL_2(\mathbb{R}) \). Show that \( A \) and \( B \) have finite order, but \( AB \) has infinite order.

19.7. Proposition. If \( a, b \in G \) are elements of finite order, and \( ab = ba \), then the order of \( ab \) is finite. In fact, \( \text{order}(ab) \) divides the product \( \text{order}(a) \text{order}(b) \).

Proof. Let \( m = \text{order}(a) \) and \( n = \text{order}(b) \). If \( g = ab \), then
\[
g^{mn} = (ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e.
\]
Thus, \( \text{order}(g) \) divides \( mn \). \( \square \)

19.8. Exercise (On PS 3). Show that if an element \( a \) has odd order, then it is the square of an element: \( a = b^2 \) for some \( b \). Show also that \( \text{order}(b) = \text{order}(a) \).

20. Generators

Let \( G \) be a group, and \( S \subseteq G \) be a subset. The subgroup generated by \( S \) is
\[
\langle S \rangle := \bigcap_{S \subseteq H \leq G} H,
\]
the intersection of all subgroups which contain the subset \( S \). That this is a subgroup is because of the following.

20.1. Proposition. If \( \{H_i\} \) is a collection of subgroups of \( G \), then \( H := \bigcap H_i \) is also a subgroup.

Proof. Straightforward. \( \square \)

Notation: we write “\( H \leq G \)” for “\( H \) is a subgroup of \( G \)”.

Note that \( \langle S \rangle \) is the “smallest” subgroup of \( G \) containing \( S \), in the sense that: if \( H \leq G \) and \( S \subseteq H \), then \( \langle S \rangle \subseteq H \). (This is true by definition.)

We can also describe \( \langle S \rangle \) as the subset consisting of all products of elements of \( S \) or their inverses.

20.2. Proposition. We have that
\[
\langle S \rangle = \{ e \} \cup \{ x_1 \cdots x_k \mid \text{for all } k \geq 1, 1 \leq i \leq k, \text{ either } x_i \in S \text{ or } x_i^{-1} \in S \}.
\]
Proof. Let $K$ denote the right-hand side. It is straightforward to show that $K$ is a subgroup of $G$: it is obviously closed under products, contains $e$, and is closed under inverses since $(x_1 \cdots x_k)^{-1} = x_k^{-1} \cdots x_1^{-1}$. Also $S \subseteq K$.

If $H \leq G$ is any subgroup which contains the subset $S$, then $K \subseteq H$, since $H$ is also closed under products and inverses. Thus $K \subseteq \bigcap_{S \subseteq H \leq G} H = \langle S \rangle$. On the other hand, $K$ is itself one of these $H$s, i.e., it is a subgroup of $G$ which contains $S$. Thus $\langle S \rangle \subseteq K$, whence $\langle S \rangle = K$. □

If $S = \{a_1, \ldots, a_k\}$ we usually just write $\langle a_1, \ldots, a_k \rangle$ for $\langle S \rangle$.

Note that if $S = \{a\}$, then $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

This is the cyclic subgroup of $G$ generated by $a$. We have shown that order($a$) = $|\langle a \rangle|$.

We say that a group $G$ is cyclic if there exists $a \in G$ such that $G = \langle a \rangle$. We say that a group $G$ is finitely generated if there exists a finite subset $S$ such that $G = \langle S \rangle$.

20.3. Example. The additive group $\mathbb{Z}$ is cyclic. We have $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

20.4. Example. The group $\mathbb{Z}/n$ is cyclic, with $\mathbb{Z}/n = \langle [1] \rangle$. In this case, we also have $\mathbb{Z}/n = \langle [a] \rangle$ where $a$ is any integer which is relatively prime to $n$.

For instance, if $n = 12$, then $\mathbb{Z}/12 = \langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle$.

20.5. Example. Note that if $a, b \in \mathbb{Z}$ (additive group), then

$$\langle a, b \rangle = \{ax + by \mid x, y \in \mathbb{Z}\} = I(a, b),$$

the set of integer combinations of $a$ and $b$. We know that all subgroups of $\mathbb{Z}$ are actually cyclic. This is fine: even if a subgroup can be generated by a certain set, it is possible that it can be generated by a smaller set. E.g., $\langle 12, 20 \rangle$ is equal to $\langle 4 \rangle$.

20.6. Exercise. Let $G$ be a group. What is $\langle \emptyset \rangle$, the subgroup generated by the empty subset?

21. Cayley diagrams

One way to represent a finite group is by a Cayley diagram. Start with a $G$ group $G$ with a finite generating set $S = \{a_1, \ldots, a_k\}$. A Cayley diagram is a “labelled directed graph”:

- Draw one vertex for each element $g \in G$, and label the vertex by its element:

  $g$

- For each pair $(g, a_i)$ consisting of an element $g \in G$ and a generator $a_i \in S$, draw an arrow from the $g$ vertex to the $ga_i$ vertex, and label the arrow with $a_i$:

  $g \xrightarrow{a_i} ga_i$

The Cayley diagram contains complete information about the multiplication law of the group.
Here is a Cayley diagram for $D_3 = \{ I, R, R^2, A, RA, R^2A \}$ with generating set $\{ R, A \}$:

Do one for the quaternion group, with generating set $\{ A, B \}$.

22. $SO(2)$ and $SO(3)$

Let $A \in M_n(\mathbb{R})$ be a real square matrix.

- $A$ is **orthogonal** if $AA^\top = I = A^\top A$, i.e., the transpose of $A$ is also the inverse of $A$.
  Equivalently, $A = [u_1 \cdots u_n]$ is orthogonal if the columns form an orthonormal basis of $\mathbb{R}^n$.
- $A$ is **special orthogonal** if it is orthogonal and also $\det A = 1$. Equivalently, the columns form an orthonormal basis which has the “same orientation” as the standard basis $e_1, \ldots, e_n$.
  (Note that if $A$ is orthogonal, we already know that $\det A \in \{ \pm 1 \}$.)

We write $SO(n) \subseteq O(n) \subseteq GL_n(\mathbb{R})$ for the subsets of special orthogonal and orthogonal matrices.

**Exercise:** show that these are subgroups.

We need to know more about $SO(n)$ for $n = 2, 3$.

The group $SO(2)$. All elements of $SO(2)$ are rotation matrices of the form

$$R_{\theta} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$ 

Proof: if $A = [u_1 \ u_2]$ is orthonormal, then $u_1, u_2$ is an orthonormal basis. Thus, if we write $u_1 = (a, b)$ (as a column vector) we know that $a^2 + b^2 = 1$, so there is a $\theta$ such that $(a, b) = (\cos \theta, \sin \theta)$. Because $u_2$ is perpendicular to $u_1$ and length 1, we know that

either $u_2 = (-b, a)$ or $u_2 = (b, -a)$.

In the first case, $\det \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = a^2 + b^2 = 1$, while in the second case $\det \begin{bmatrix} a & b \\ b & -a \end{bmatrix} = -(a^2 + b^2) = -1$.

We note the following identities, which allow you to calculate in $SO(2)$:

- $R_{\alpha}R_{\beta} = R_{\alpha+\beta}$,
- $R_0 = I$,
- $(R_{\alpha})^{-1} = R_{-\alpha}$,
- $R_{\alpha+2\pi n} = R_{\alpha}$ for any $n \in \mathbb{Z}$.

22.1. *Exercise* (On PS?). Consider $A \in O(2) \setminus SO(2)$, which by the above analysis has the form $A = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ with $a^2 + b^2 = 1$. Let $\theta \in \mathbb{R}$ be such that $(a, b) = (\cos \theta, \sin \theta)$. Show that left-multiplication by $A$ describes a reflection across the line $L_{\theta}$ through $(0, 0)$ and $(\cos \theta, \sin \theta)$. 
The group \(SO(3)\). First consider

\[
R^e_\theta := \begin{pmatrix}
\cos \theta & -\sin \theta & 0 \\
\sin \theta & \cos \theta & 0 \\
0 & 0 & 1
\end{pmatrix}
\]

which describes rotation around the \(z\)-axis at angle \(\theta\). If \(P = [u_1 \ u_2 \ u_3]\) is any orthogonal matrix with \(u_3\) as the last column, then

\[
R^u_\theta := PR^e_\theta P^{-1}
\]
describes a rotation of angle \(\theta\) along the axis in the direction of \(u_3\) (counterclockwise as viewed from the endpoint of \(u_3\)). (Note. We can see that \(u_3\) is fixed by this, so must be along the axis: \(P^{-1}u_3 = e_3\), so \(R^u_\theta u_3 = u_3\).)

22.2. Remark. (1) We have \(R^u_0 = I\) for any \(u\), i.e., rotation of angle 0 is the identity. (2) We have \(R^u_{\theta + 2\pi n} = R^u_\theta\) for all \(n \in \mathbb{Z}\). (3) We have \(R^u_\theta = R^{-u}_{-\theta}\), i.e., a counterclockwise rotation viewed from the opposite side is a clockwise rotation.

22.3. Proposition. Every element of \(SO(3)\) can be written as \(R^u_\theta\) for some unit vector \(u\) and \(\theta \in \mathbb{R}\). (Typically in more than one way.)

This corollary can help you recognize the axis of rotation of an element of \(SO(3)\).

22.4. Corollary. If \(A \in SO(3) \setminus \{I\}\) and \(u\) is a unit vector, then \(Au = u\) if and only if \(A\) is one of the two unit vectors along the axis of rotation of \(A\).

I’ll write the proof below, but you don’t need to worry about it. It is a consequence of the “spectral theory/principal axis theorem” that you learned in linear algebra. The key idea is that every \(A \in SO(3)\) has 1 as an eigenvalue: if \(A \neq I\) then the corresponding eigenvector describes the axis of rotation.

An obvious question is: what is the formula for

\[
R^u_\alpha R^v_\beta = R^w_\gamma?
\]
The answer is: there is no convenient formula. To calculate: express \(R^u_\alpha\) and \(R^v_\beta\) as \(3 \times 3\) matrices, multiply them to get \(B\), then figure out \(w\) by looking for an eigenvector for \(\lambda = 1\), and then finally figure out \(\gamma\).

Proof of proposition, not done in class, merely provided for your information. Let \(A \in SO(3)\). Let \(f(t) = \det(tI - A)\) be the characteristic polynomial. Because \(A\) is a real matrix, \(f\) is a real polynomial. Thus any complex root \(\lambda\) of \(f\) must satisfy either (i) \(\lambda \in \mathbb{R}\), or (ii) \(\lambda \in \mathbb{C} \setminus \mathbb{R}\) and \(\bar{\lambda}\) is also a root of \(f\). Since \(\deg f = 3\), we either have three real roots (counted with multiplicity), or one real root and one conjugate pair of non-real roots.

Because \(A\) is orthogonal, it preserves lengths: \(|Av| = |v|\). (Proof: \(|Av|^2 = v^\top A^\top Av = v^\top Iv = |v|^2\). Thus if \(\lambda\) is an eigenvalue with (possibly complex) eigenvector \(v\), we have \(|v| = |Av| = |\lambda| |v|\), so \(|\lambda| = 1\). Thus, all eigenvalues have length 1.

Since \(\det A = 1\), the eigenvalues must multiply to 1. If all eigenvalues are real, they are 1 or \(-1\), in which case they are (listed with multiplicity): 1, 1, 1 or 1, \(-1\), \(-1\). If some eigenvalues are non-real, then they are: \(\{1, \lambda, \bar{\lambda}\}\) for some \(\lambda \in \mathbb{C} \setminus \mathbb{R}\).

In either case, there is a real eigenvector \(u_3\) for 1, i.e., \(Au_3 = u_3\). Assume \(|u_3| = 1\), extend to an orthonormal basis \(u_1, u_2, u_3\), and set \(P := [u_1 \ u_2 \ u_3]\). Then

\[
B := P^{-1}AP
\]
is also in \(SO(3)\) since \(P\) is orthogonal, and also \(B e_3 = e_3\). The matrix \(B\) expresses the action of \(A\) in terms of the orthonormal basis \(u_1, u_2, u_3\). To finish the proof, it suffices to show that \(B\) is a rotation around the \(z\)-axis, so \(A = PB P^{-1} = PR^e_\theta P^{-1}\) as desired.
In fact, since the columns of $B$ are orthonormal and the third column is $e_3$, it has the form

$$B = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $(a, c), (b, d)$ form an orthonormal basis of the $xy$-plane, whence

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

for some $\theta$. □

23. Dihedral groups

Consider a regular $n$-gon sitting in 3-space (with $n \geq 3$). Let’s assume its vertices are the collection of points $V_n := \{ (\cos 2\pi (k/n), \sin 2\pi (k/n), 0) \mid k \in \mathbb{Z} \}$. Note that $|V_n| = n$.

The dihedral group $D_n$ is the set of special orthogonal matrices which preserve the set of vertices of the regular $n$-gon. That is,

$$D_n = \{ A \in SO(3) \mid Av \in V \text{ for all } v \in V \}.$$  

Exercise (easy but important): $D_n$ is a subgroup of $SO(3)$.

23.1. Proposition. The set $D_n$ consists of the following:

- Rotation about the $z$-axis by an angle $2\pi (k/n)$, with $k = 0, \ldots, n - 1$. (Note: $k = 0$ is the identity matrix.)
- Rotation by angle $\pi$ around a line $L$ through the origin in the $xy$-plane which either:
  - joins opposite vertices (if $n$ is even),
  - joins the midpoints of opposite edges (if $n$ is even),
  - joins a vertex to the midpoint of the opposite side (if $n$ is odd).

The group $D_n$ has exactly $2n$ elements.

Write

$$R = \begin{pmatrix} \cos 2\pi/n & -\sin 2\pi/n & 0 \\ \sin 2\pi/n & \cos 2\pi/n & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$  

So $R = R_{2\pi/n}^{(2\pi/k)}$ and $A = R_{2\pi}^{(4\pi/k)}$. Note that we have the identities:

$$R^a = I, \quad A^2 = I, \quad AR = R^{-1}A.$$  

We can calculate that:

$$R^k = R_{2\pi/n}^{(2\pi/k)}, \quad R^k A = R_{2\pi}^{u(n/k)} \text{ where } u(\theta) = (\cos \theta, \sin \theta, 0).$$

Work out the cases of $n = 3$ and $n = 4$ explicitly.

If you list the elements of $D_n$ as $I, R, \ldots, R^{n-1}, A, RA, \ldots, R^{n-1}A$, then you can carry out any calculation in $D_n$ using just the above identities.

3There is a technical term for this: one says that $D_n$ is presented by: generators $R, A$ and relations $R^a = I, A^2 = I, AR = R^{-1}A$. 

24. Homomorphisms

A **homomorphism of groups** is a function \( \phi: G \to H \) between two groups such that
\[
\phi(xy) = \phi(x)\phi(y) \quad \text{for all } x, y \in G.
\]

24.1. **Example.** The exponential function defines a homomorphism
\[
\exp: (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot), \quad \exp(x) := e^x,
\]
because \( \exp(x + y) = e^{x+y} = e^x e^y = \exp(x)\exp(y) \).

Likewise, we can use logarithms to define a homomorphism \((\mathbb{R} \setminus \{0\}, \cdot) \to (\mathbb{R}, +)\), by
\[
x \mapsto \log|x|.
\]

24.2. **Example.** We get a homomorphism \( \phi: \mathbb{R} \to GL_2(\mathbb{R}) \), \( \phi(\theta) := \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \)
from the additive group of real numbers to \( 2 \times 2 \) matrices. That this is a homomorphism amounts to the addition formulas for sine and cosine (exercise: show it is a homomorphism using this); more conceptually, \( \phi \) sends \( \theta \) to the operation of rotation through angle \( \theta \).

24.3. **Example.** The determinant is a homomorphism
\[
det: GL_n(\mathbb{R}) \to \mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot),
\]
because \( \det(AB) = \det(A)\det(B) \).

24.4. **Example.** The projection map \( \pi: \mathbb{Z} \to \mathbb{Z}/n \) which sends an integer to its equivalence class is a homomorphism, because \( \pi(x + y) = [x + y] = [x] + [y] = \pi(x) + \pi(y) \).

Basic facts about a homomorphism \( \phi: G \to H \).

- \( \phi(e_G) = e_H \).
- \( \phi(a^{-1}) = \phi(a)^{-1} \).
- \( \phi(a^n) = \phi(a)^n \).

24.5. **Proposition.** If \( \phi: G \to H \) is a homomorphism, then the image set \( \phi(G) \) is a subgroup of \( H \).

**Proof.** Exercise. \( \square \)

For instance, the image of \( \theta \mapsto R_\theta : \mathbb{R} \to GL_2(\mathbb{R}) \) is exactly \( SO(2) \).

25. Isomorphisms

An **isomorphism** of groups is a homomorphism \( \phi: G \to H \) which is a bijection.

25.1. **Proposition.** If \( \phi: G \to H \) is an isomorphism, then its inverse function \( \phi^{-1}: H \to G \) is also an isomorphism.

25.2. **Example.** The exponential map \( \exp: \mathbb{R} \to \mathbb{R}^\times \) is not an isomorphism, but is an isomorphism to its image: \( (\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot) \).

25.3. **Example** (Not done in class). Define \( \phi: \mathbb{Z}/n \to SO(2) \) by \( \phi([k]) := R_{2\pi k/n} \). This defines an isomorphism \( \mathbb{Z}/n \cong G \) where \( G = \{ R_{2\pi k/n} | k \in \mathbb{Z} \} \) as a subgroup of \( SO(2) \).

25.4. **Exercise** (PS ?). Fix \( c > 0 \) and consider the group \( G = ((-c, c), *) \) with \( x * y = (x + y)/(1 + c^{-2}xy) \). Construct an isomorphism \( G \to \mathbb{R} \).
25.5. Example. Let \( G = \mathbb{Z}/2 \times \mathbb{Z}/2 \), an additive group, and let \( H = \{I, A, B, C\} \subseteq SO(3) \), where

\[
A = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}, \quad C = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}.
\]

This \( H \) is a subgroup, containing all \( 180^\circ \) rotations around the coordinate axes.

The groups \( G \) and \( H \) are isomorphic: there exists a bijection \( \phi: G \to H \) such that \( \phi(x + y) = \phi(x)\phi(y) \). One example is:

\[
\phi([0], [0]) = I, \quad \phi([0], [1]) = B, \\
\phi([1], [0]) = A, \quad \phi([1], [1]) = C.
\]

To check that this is a homomorphism means checking all 16 equations of the form \( \phi(x + y) = \phi(x)\phi(y) \). In this case, just write down the multiplication tables for both groups, and show they coincide.

We say that two groups \( G \) and \( H \) are isomorphic if there exists an isomorphism \( G \to H \). We often write \( G \approx H \) when the two groups are isomorphic.

25.6. Proposition. If \( \phi: G \to H \) is an isomorphism of groups, then the inverse function \( \phi^{-1}: H \to G \) is also an isomorphism of groups.

Proof. Exercise. \[\square\]

In general there can be more than one isomorphism between two groups.

25.7. Example. For the groups \( G = \mathbb{Z}/2 \times \mathbb{Z}/2 \) and \( H = \{I, A, B, C\} \subseteq SO(2) \) of the previous example, there are six different isomorphisms \( G \to H \). What are they?

The idea of isomorphism is that two groups which are isomorphic are in some sense the “same group”. This is actually a subtle idea, because of the fact that there can be many different isomorphisms \( G \to H \), so \( G \) and \( H \) can be “the same group in different ways”.

What is true is that isomorphic groups share the same properties.

25.8. Proposition. If \( G \approx H \), then \( G \) is abelian if and only if \( H \) is abelian.

Proof. Let \( \phi: G \to H \) be an isomorphism. I’ll show that \( G \) abelian implies \( H \) abelian. Since the inverse map \( \phi^{-1}: H \to G \) is also an isomorphism, that will give the other implication.

Suppose \( G \) is abelian, and consider \( h, h' \in H \). Because \( \phi \) is a bijection, there exist \( g, g' \in G \) such that \( \phi(g) = h \) and \( \phi(g') = h' \). Then

\[
hh' = \phi(g)\phi(g') = \phi(gg') = \phi(g')\phi(g) = h'h',
\]

where in the middle \( gg' = g'g \) because \( G \) is abelian. Thus we have proved that \( H \) is abelian. \[\square\]

As a consequence, \( D_3 \not\approx \mathbb{Z}/6 \), even though they have the same size, because \( \mathbb{Z}/6 \) is abelian but \( D_3 \) is not.

25.9. Proposition. If \( G \approx H \), then for any \( n \in \mathbb{N} \cup \{\infty\} \) the groups \( G \) and \( H \) have the same numbers of elements of order \( n \).

Proof. Let \( \phi: G \to H \). I’ll show that for any \( g \in G \), we have

\[
\text{order}(\phi(g)) = \text{order}(g).
\]

Thus \( \phi \) restricts to a bijection

\[
\{g \in G \mid \text{order}(g) = n\} \leftrightarrow \{h \in H \mid \text{order}(h) = n\}.
\]

Given \( g \in G \), write \( h = \phi(g) \in H \). Note that

\[
e_G = g^k \iff \phi(e_G) = \phi(g^k) \iff e_H = h^k.
\]
The first equivalence is because $\phi$ is a bijection, so it is injective, the second because $\phi$ is a homomorphism. Thus, the set of integers $k$ such that $g^k = e$ is the same as the set of $k$ such that $h^k = e$, so $g$ and $h$ have the same orders.

As a consequence, $\mathbb{Z}/2 \times \mathbb{Z}/2 \not\approx \mathbb{Z}/4$.

Given a homomorphism $\phi: G \to H$, if $G' \leq G$ is a subgroup, then $\phi(G') \leq H$ is also a subgroup. Here $\phi(G') = \{ \phi(x) \mid x \in G' \}$ is the image subset of the subset $G'$ under the function $\phi$.

25.10. Proposition. An isomorphism $\phi: G \to H$ gives a bijective correspondence

\[
\{ \text{subgroups of } G \} \xrightarrow{\sim} \{ \text{subgroups of } H \}
\]

by $G' \mapsto \phi(G')$.

26. Kernel and image of a homomorphism

The \textbf{image} of a homomorphism $\phi: G \to H$ is the image of $\phi$ as a function:

\[
\text{Im } \phi := \{ \phi(g) \in H \mid g \in G \}.
\]

Exercise: $\text{Im } \phi$ is a subgroup of $H$.

The \textbf{kernel} of a homomorphism $\phi: G \to H$ is the set

\[
\text{Ker } \phi := \{ g \in G \mid \phi(g) = e_H \}.
\]

Exercise: $\text{Ker } \phi$ is a subgroup of $G$.

Recall that a function $\phi: S \to T$ between sets is \textbf{injective} if $\phi(a) = \phi(b)$ implies $a = b$ for all $a, b \in S$.

One way to think of this is in terms of the \textbf{preimage sets}

\[
\phi^{-1}(\{t\}) := \{ s \in S \mid \phi(s) = t \}.
\]

(Do not confuse this use of “$\phi^{-1}$” with the inverse function, which might not even exist here.) $\phi$ is injective if and only if each $\phi^{-1}(\{t\})$ has \textit{at most} one element.

26.1. Proposition. A homomorphism $\phi: G \to H$ is injective if and only if $\text{Ker } \phi = \{ e_G \}$.

\textbf{Proof}. That injective homomorphisms have trivial kernels is obvious.

Suppose $\phi$ is a homomorphism and $\text{Ker } \phi = \{ e_G \}$. If $x, y \in G$ are such that $\phi(x) = \phi(y)$, then

\[
\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = e_H
\]

since $\phi(x) = \phi(y)$. Thus $xy^{-1} \in \text{Ker } \phi$, so $xy^{-1} = e$, so $x = y$. Thus, $\phi$ is injective.

\textbf{Discussion}. The examples of homomorphisms we gave before. Thus

- For $\exp: \mathbb{R} \to \mathbb{R}^\times$, the kernel is the trivial subgroup $\{0\}$.
- For $x \mapsto \log |x|: \mathbb{R}^\times \to \mathbb{R}$, the kernel is $\{ \pm 1 \}$.
- For $\theta \mapsto R_\theta: \mathbb{R} \to \text{GL}_2(\mathbb{R})$, the kernel is $2\pi \mathbb{Z} = \{ 2\pi n \mid n \in \mathbb{Z} \}$.
- For $\det: \text{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$, the kernel is $\text{SL}_2(\mathbb{R})$, called the \textbf{special linear group}.
- For $\pi: \mathbb{Z} \to \mathbb{Z}/n$, the kernel is $\mathbb{Z} n$.

27. Groups isomorphic to a direct product

27.1. Proposition. Let $G$ be a group with subgroups $A, B \leq G$. If

1. $ab = ba$ for all $a \in A$ and $b \in B$,
2. $AB = G$, where $AB = \{ ab \mid a \in A, b \in B \}$, and
3. $A \cap B = \{ e \}$,

then there is an isomorphism $A \times B \cong G$.

\textbf{Proof}. Left as exercise.
Remark: Condition (1) does not say that $G$ is abelian.

We have an isomorphism $\mathbb{Z}/6 \approx \mathbb{Z}/2 \times \mathbb{Z}/3$. This is a consequence of the following.

27.2. **Theorem** (“Chinese remainder theorem”). Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, and $a, b \in \mathbb{Z}$. Then there exists a solution $x \in \mathbb{Z}$ to the system of congruences

$$x \equiv a \pmod{m},$$
$$x \equiv b \pmod{n},$$

and furthermore the solution is unique modulo $mn$.

**Proof.** Write $1 = sm + tn$ for some $s, t \in \mathbb{Z}$. Set $x_1 = 1 - sm = tn$ and $x_2 = 1 - tb = sa$. Then

$$x_1 \equiv 1 \pmod{m}, \quad x_2 \equiv 0 \pmod{m},$$
$$x_1 \equiv 0 \pmod{n}, \quad x_2 \equiv 1 \pmod{n}.$$

Set $x := ax_1 + bx_2$ to get a solution.

If $x, x'$ are both solutions, then $y := x - x'$ is such that $m|y$ and $n|y$, whence $mn|y$ since $\gcd(m, n) = 1$. □

27.3. **Corollary.** If $\gcd(m, n) = 1$, there is an isomorphism $\mathbb{Z}/mn \sim \mathbb{Z}/m \times \mathbb{Z}/n$, defined by $[x]_{mn} \mapsto ([x]_m, [x]_n)$.

**Proof.** Check that the formula defines a homomorphism of groups. The Chinese remainder theorem says exactly that the map is a bijection. □

Note that relative primeness is very necessary here: $\mathbb{Z}/4 \not\approx \mathbb{Z}/2 \times \mathbb{Z}/2$.

We can iterate this.

27.4. **Theorem.** Let $m_1, \ldots, m_k \in \mathbb{N}$ be pairwise relatively prime, i.e., $\gcd(m_i, m_j) = 1$ if $i \neq j$. Let $a_1, \ldots, a_k \in \mathbb{Z}$. Then there exists a solution $x$ to the system of congruences

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \ldots, k,$$

and the solution is unique modulo $m := m_1 \cdots m_k$.

**Proof.** For existence, it is enough to produce $x_i \in \mathbb{Z}$ such that $x_i \equiv \delta_{ij} \pmod{m_j}$, for $i = 1, \ldots, k$. (Here $\delta_{ij}$ is the Kronecker delta.) Given this, $x := a_1 x_1 + \cdots + a_k x_k$ is a solution.

I'll write this for the case $i = k$; all other $i$ are proved in the same way.

Let $n := m/m_k = m_1 \cdots m_{k-1}$. Note that $\gcd(m_k, n) = 1$ (since $m_k$ is coprime to each factor of $n$.) Thus $1 = sm_k + tn$ for some $s, t \in \mathbb{Z}$. Set $x_k := 1 - sm_k = tn$, so that $x_k \equiv 1 \pmod{m_k}$ and $x_k \equiv 0 \pmod{m_i}$ for $i < k$.

For uniqueness, note that if $x, x'$ are solutions, then $m_i | x - x'$ for all $i$, so $m | x - x'$. □

27.5. **Corollary.** If $m := m_1 \cdots m_k$ with the $m_i$ pairwise relatively prime, there is an isomorphism of groups $\mathbb{Z}/m \sim \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_k$.

**Proof.** Given by $[x]_m \mapsto ([x]_{m_1}, \ldots, [x]_{m_k})$. □

28. **Groups of modular units**

Recall that $\mathbb{Z}/n$ admits multiplication as well as addition, which makes it a monoid, but not a group. Say that $a \in \mathbb{Z}/n$ is a **unit** if there exists $b \in \mathbb{Z}/n$ such that $ab = [1]$. Write $\Phi(n) \subseteq \mathbb{Z}/n$ for the set of units.
28.1. Example.

\[ \Phi(2) = \{1\} \]
\[ \Phi(3) = \{1, 2\} \]
\[ \Phi(4) = \{1, 3\} \]
\[ \Phi(5) = \{1, 2, 3, 4\} \]
\[ \Phi(6) = \{1, 5\} \]

28.2. Proposition. For an integer \( a \), we have \([a] \in \Phi(n)\) if and only if \( \gcd(a, n) = 1 \).

Proof. If \( \gcd(a, n) = 1 \) then \( ar + ns = 1 \) for some \( r, s \in \mathbb{Z} \), which implies \( [a][r] = [1] \), so \([a] \in \Phi(n)\).

Conversely, if \([a] \in \Phi(n)\) then there exists \( b \in \mathbb{Z} \) such that \( 1 \equiv ab \mod n \) i.e. \( 1 = ab + kn \) for some \( k \in \mathbb{Z} \), so \( \gcd(a, n) = 1 \). \( \square \)

The Euler \( \phi \)-function is a function \( \phi : \mathbb{N} \rightarrow \mathbb{N} \), defined by

\[ \phi(n) := \text{number of positive divisors of } n. \]

Thus \( \phi(1) = \phi(2) = 1, \phi(3) = \phi(4) = \phi(6) = 2, \phi(5) = 4 \), etc. Clearly, \( |\Phi(n)| = \phi(n) \).

We have that \((\Phi(n), \cdot)\) is a group under multiplication, called a group of modular units. It is a finite abelian group. Question: what is the structure of \( \Phi(n) \).

28.3. Example. \( \Phi(5) \) is cyclic: either \([2]\) or \([3]\) is a generator.

28.4. Example. \( \Phi(8) = \{[1], [3], [5], [7]\} \) is not cyclic, rather is isomorphic to \( \mathbb{Z}/2 \times \mathbb{Z}/2 \).

We can simply things a bit using the following.

28.5. Proposition. If \( n = ab \) with \( \gcd(a, b) = 1 \), then \( \Phi(n) \approx \Phi(a) \times \Phi(b) \).

Proof. The key observation is that for any integer \( x \), we have that: \( \gcd(x, n) = 1 \) if and only if both \( \gcd(x, a) = 1 \) and \( \gcd(x, b) = 1 \), a fact which uses that \( \gcd(a, b) = 1 \).

Define \( \phi : \Phi(n) \rightarrow \Phi(a) \times \Phi(b) \) by \( \phi([x]_n) := ([x]_a, [x]_b) \), the restriction of the bijection \( \mathbb{Z}/n \sim \mathbb{Z}/a \times \mathbb{Z}/b \) of the CRT. Now note that \( \phi \) is well-defined: if \([x]_a \in \Phi(n)\), then \( \gcd(x, n) = 1 \) so \( \gcd(x, a) = 1 = \gcd(x, b) \), so \([x]_a \in \Phi(a) \) and \([x]_b \in \Phi(b) \).

It is clear that \( \phi \) is a homomorphism (where we are now looking at groups under multiplication): \( \Phi([xy]_n) = ([xy]_a, [xy]_b) = ([x]_a[y]_a, [x]_b[y]_b) = ([x]_a, [x]_b)\Phi([y]_n) = \Phi([x]_a)\Phi([y]_n) \).

To show that \( \phi \) is a bijection, note that this function is the restriction of the bijection \( \mathbb{Z}/n \sim \mathbb{Z}/a \times \mathbb{Z}/b \) by the Chinese remainder theorem. This immediately implies \( \phi \) is injective. To show it is surjective, by the CRT any element of \( \Phi(a) \times \Phi(b) \) has the form \(([x]_a, [x]_b)\) with \( \gcd(x, a) = 1 = \gcd(x, b) \), which implies \( \gcd(x, n) = 1 \) so \([x]_n \in \Phi(n) \). \( \square \)

Example: \( \Phi(24) \approx \Phi(8) \times \Phi(3) \approx \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \).

28.6. Corollary. If \( n = ab \) with \( \gcd(a, b) = 1 \) we have \( \phi(n) = \phi(a)\phi(b) \). Therefore, if \( n = p_1^{k_1} \cdots p_r^{k_r} \) is the prime factorization of \( n \), then

\[ \phi(n) = (p_1 - 1)p_1^{k_1-1} \cdots (p_r - 1)p_r^{k_r-1}. \]

28.7. Theorem (Euler’s theorem). If \( \gcd(a, n) = 1 \), then \( a^{\phi(n)} \equiv 1 \mod n \).

Proof. Order theorem. \( \square \)

28.8. Corollary (Fermat’s little theorem). If \( p \) is prime and \( \gcd(a, p) = 1 \), then \( a^{p-1} \equiv 1 \mod p \).

There are theorems which completely describe the structure of \( \Phi(n) \) for any \( n \). Using the above result, it is enough to handle the case \( \Phi(p^k) \) where \( p \) is prime. Here is the case \( p = 2 \).
28.9. **Proposition.** Let \( k \geq 3 \). There is an isomorphism of the form \( \Phi(2^k) \cong \mathbb{Z}/2 \times H \), where \( H \) is a cyclic group such that \( |H| = 2^{k-2} \). In particular, \( \Phi(2^k) \) is not isomorphic to \( \mathbb{Z}/2^{k-1} \), even though \( |\Phi(2^k)| = 2^{k-1} \).

**Proof.** Left as an exercise. \( \square \)

29. **Permutation groups**

Let \( X \) be a set. A map \( \phi: X \to X \) which is a bijection is called a **permutation** of the set.

We are mainly interested in the case when \( X \) is a finite set, which we can take to be \( n := \{1, 2, \ldots, n\} \).

Let \( \text{Sym}(X) \) be the set of all bijections \( \phi: X \to X \). Composition of functions defines a binary operation of \( \text{Sym}(X) \), which has the same properties as that of symmetry groups. (You can think of \( \text{Sym}(X) \) as the symmetries of the set \( X \).)

We write \( S_n := \text{Sym}(n) \). Note that \( S_n \) has \( n! \) elements.

29.1. **Exercise.** If \( |X| = n \), then \( \text{Sym}(X) \) and \( S_n \) are isomorphic groups.

We have the following notation for permutations of \( n \), as a \( 2 \times n \) matrix. For instance, \[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
4 & 2 & 1 & 3
\end{pmatrix}
\]
is notation for the function \( \phi: \{1, 2, 3, 4\} \to \{1, 2, 3, 4\} \) given by
\[
\phi(1) = 4, \quad \phi(2) = 2, \quad \phi(3) = 1, \quad \phi(4) = 3.
\]
The matrix functions as a “look-up table” for the function \( \phi \). In general, \( \sigma \in S_n \) is represented by:
\[
\begin{pmatrix}
1 & 2 & 3 & \ldots & n \\
\sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n)
\end{pmatrix}
\]

We can compose these:
\[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
1 & 4 & 3 & 2
\end{pmatrix}
\begin{pmatrix}
1 & 2 & 3 & 4 \\
4 & 2 & 1 & 3
\end{pmatrix}
= \begin{pmatrix}
1 & 2 & 3 & 4 \\
2 & 4 & 1 & 3
\end{pmatrix}.
\]

*Notice that this is not matrix multiplication.* Note also that composition in the opposite order is different:
\[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
4 & 2 & 1 & 3
\end{pmatrix}
\begin{pmatrix}
1 & 2 & 3 & 4 \\
1 & 4 & 3 & 2
\end{pmatrix}
= \begin{pmatrix}
1 & 2 & 3 & 4 \\
4 & 3 & 1 & 2
\end{pmatrix}.
\]

29.2. **Example.** Consider the dihedral symmetries of the square, and label the vertices \( A, B, C, D \). Each symmetry gives a permutation of the set \( \{A, B, C, D\} \).

Thus, we get a homomorphism of groups \( \phi: D_4 \to \text{Sym}(\{A, B, C, D\}) \).

30. **Cycle permutations**

We can represent each permutation pictorially as a picture:

\[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
1 & 4 & 3 & 2
\end{pmatrix}:
\begin{array}{c}
\circlearrowright
\hline
\end{array}
\begin{array}{ccc}
1 & \overset{2}{\circlearrowleft} \\
3 & \underset{4}{\circlearrowright}
\end{array}
\]

\[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
4 & 2 & 1 & 3
\end{pmatrix}:
\begin{array}{c}
\circlearrowright
\hline
\end{array}
\begin{array}{ccc}
1 & \overset{2}{\circlearrowleft} \\
3 & \underset{4}{\circlearrowright}
\end{array}
\]

This suggests cycle notation. Thus \( (1 4 3) \in S_4 \) is notation for the permutation given by \( 1 \to 4 \to 3 \to 1 \), and which keeps all other elements fixed. It is called a “3-cycle”.

M 25 Sep
The above identity is
\[(2 \ 4)(1 \ 4 \ 3) = (1 \ 2 \ 4 \ 3)\].

Explicitly, the \(k\)-cycle \(\sigma = (a_1 \ \cdots \ a_k)\) (where the \(a_i\) are distinct) is defined by
\[
\sigma(x) := \begin{cases} 
  x & \text{if } x \not\in \{a_1, \ldots, a_k\}, \\
  a_{j+1} & \text{if } x = a_j \text{ for } j = 1, \ldots, k-1, \\
  a_1 & \text{if } x = a_k.
\end{cases}
\]

Some facts:
- The order of entries in a cycle \((a_1 \ a_2 \ \cdots \ a_k)\) usually matters. However, the permutation is unchanged if we move the front to the end:
  \[(a_1 \ a_2 \ \cdots \ a_k) = (a_2 \ \cdots \ a_k \ a_1) = (a_3 \ \cdots \ a_k \ a_1 \ a_2) = \cdots.\]

That is, there is no preferred “first element” in a cycle (which is obvious from the pictures). We think of these as two names for the same cycle.

- Two cycles \(\sigma = (a_1 \ \cdots \ a_k)\) and \(\tau = (b_1 \ \cdots \ b_\ell)\) are disjoint if they have no two elements in common. **Disjoint cycles commute:** \(\sigma \tau = \tau \sigma\).

  Example: \((1 \ 7 \ 3)(2 \ 6 \ 4 \ 5) = (2 \ 6 \ 4 \ 5)(1 \ 7 \ 3)\).

  Thus, if \(\sigma_1, \ldots, \sigma_d\) are cycles which are pairwise disjoint, then it doesn’t matter what order we multiply them in. (**Disjoint** is very important here.)

- Any cycle of length one (or zero) represents the identity element. We usually don’t write these.

30.1. **Exercise.** Give and prove a formula for the number of \(k\)-cycles in \(S_n\).

30.2. **Example.** Let \(G\) be a finite group, \(g \in G\) some element. Consider the function \(L_g: G \to G\) by \(L_g(x) := gx\). This is a bijection, so is a permutation of the set \(G\). We actually the cycle decomposition of \(L_g\) earlier: it is a product of disjoint cycles, each of which has size \(n = \text{order}(g)\).

Each cycle in the decomposition looks like \((a \ ga \ g^2a \ \cdots \ g^{n-1}a)\) for some \(a \in G\).

30.3. **Theorem.** Every permutation \(\phi: X \to X\) can be written uniquely (up to reordering) as a product of pairwise disjoint cycles of length \(\geq 2\).

Note: we regard the identity map \(e\) as being written by an “empty product” of cycles.

The idea of the proof is that suggested by the “pictures” we drew for a permutation on a finite set. These pictures partition the set in an obvious way, and for each component there is a corresponding cycle.

**Sketch proof: existence of cycle decomposition.**

Just give an outline of this in class.

**Step 1.** Fix \(\phi \in \text{Sym}(X)\). Define a relation \(\sim\) on \(x\) by
\[
x \sim y \quad \iff \quad \exists k \in \mathbb{Z} \text{ such that } \phi^k(x) = y.
\]

Exercise: show that this is actually an equivalence relation.

**Step 2.** List the equivalence classes \(C_1, \ldots, C_r\). Note that there are finitely many and each \(C_i\) is finite since \(X\) is finite.

For each \(i = 1, \ldots, r\), Define \(\sigma_i: X \to X\) by
\[
\sigma_i(x) := \begin{cases} 
  x & \text{if } x \not\in C_i, \\
  \phi(x) & \text{if } x \in C_i.
\end{cases}
\]
Exercise: prove that \( \sigma_i \) is a bijection, and that it is a \( k_i \)-cycle involving the elements of \( C_i \), where \( k_i = |C_i| \).

Note that since \( C_i \cap C_j = \emptyset \) if \( i \neq j \), the cycles \( \sigma_i \) and \( \sigma_j \) are disjoint.

**Step 3.** Prove that \( \sigma = \sigma_1 \sigma_2 \cdots \sigma_r \). Note: some of the \( \sigma_i \) may be 1-cycles, which are actually the identity map. We discard these to get the desired decomposition.

\[ \square \]

**Sketch proof: uniqueness of cycle decomposition.** Suppose a permutation \( \phi: X \to X \) has two cycle decompositions \( \phi = \sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_s \), where the \( \{ \sigma_i \} \) are pairwise disjoint cycles, and the \( \{ \tau_j \} \) are pairwise disjoint cycles. In both cases assumed cycles of length \( \geq 2 \).

Do this by induction on \( r \). Note: \( r = 0 \) means \( \phi = \text{id} \), so in this case \( s = 0 \) too.

If \( r \geq 1 \), pick an \( x \in X \) such that \( \sigma_i(x) \neq x \). This means \( \phi(x) \neq x \) since the cycles \( \sigma_i \) are disjoint. Therefore there exists a \( j \) such that \( \tau_j(x) \neq x \).

Set \( C := \{ \phi^d(x) \mid d \in \mathbb{Z} \} \). Set \( |C| = k \geq 2 \). Note that \( \phi \) sends elements of \( C \) to elements of \( C \), and in fact \( \phi(C): C \to C \) is a cycle: \( x \mapsto \phi(x) \mapsto \cdots \phi^{k-1}(x) \mapsto x \).

Claim: \( \sigma_r \) and \( \tau_j \) are both cycles on elements of \( C \), and in fact \( \sigma_r = \tau_j \).

Using this and the fact that disjoint cycles commute, we can cancel to get that \( \sigma_1 \cdots \sigma_{r-1} = \tau_1 \cdots \tau_{j-1} \tau_{j+1} \cdots \tau_s \) and get the result by induction.

To prove the claim, consider \( i \neq r \), whence \( \sigma_i(x) = x \). Fact: \( \phi \sigma_i = \sigma_i \phi \) (because disjoint cycles commute, and \( \sigma_i \) commutes with itself). Thus

\[ \sigma_i \phi^d(x) = \phi^d \sigma_i(x) = \phi^d(x). \]

That is, \( \sigma_i|C \) is the identity map of \( C \).

On the other hand, since \( \phi(y) \neq y \) for all \( y \in C \), we must have that \( \phi(y) = \sigma_r(y) \). That is, \( \sigma_r \) is a \( k \)-cycle on the elements of \( C \). The same argument applies to \( \tau_j \).

\[ \square \]

### 31. Cycle type classification

This means we can classify permutations by “cycle type”. I’ll just give examples.

\[
\begin{align*}
S_2: & \quad 2 \quad \text{(12)} \quad \text{e} \\
1+1 & \quad 2 \quad \text{(12)} \quad \text{e} \\
S_3: & \quad 3 \quad \text{(123), (132)} \\
2+1 & \quad \text{(12), (13), (23)} \quad \text{e} \\
1+1+1 & \quad \text{(12), (13), (14), (23), (24), (34)} \quad \text{e} \\
S_4: & \quad 4 \quad \text{(1234), (1243), (1324), (1342), (1423), (1432)} \\
3+1 & \quad \text{(123), (132), (124), (142), (134), (143), (234), (243)} \quad \text{e} \\
2+2 & \quad \text{(12)(34), (13)(24), (14)(23)} \quad \text{e} \\
2+1+1 & \quad \text{(12), (13), (14), (23), (24), (34)} \quad \text{e} \\
1+1+1+1 & \quad \text{e} \quad \text{e}
\end{align*}
\]

The number of “cycle types” in \( S_n \) is equal to the number \( p(n) \) of **partitions** of \( n \), i.e., the number of ways to write \( n \) as a sum of positive integers (repetitions allowed, order does not matter).

**31.1. Exercise.** Describe the cycle types and count the number of permutations of each cycle type in \( S_6 \).

### 32. Parity of permutations

A **transposition** is the same thing as a 2-cycle.

**32.1. Proposition.** Every element in \( S_n \) can be written as a product of transpositions (not uniquely, and they need not be disjoint). (The identity element is thought of as an empty product of transpositions.)
Proof. Since every element is a product of $k$-cycles, we just need to show that $\sigma = (a_1 \ a_2 \ \cdots \ a_k)$ is a product of transpositions:

$$(a_1 \ a_2 \ \cdots \ a_k) = (a_1 \ a_k)(a_1 \ a_3)(a_1 \ a_2).$$

32.2. Theorem. A permutation can either be written as a product of an even number of transpositions, or an odd number of transpositions (but not both).

Given this, we speak of even and odd permutations, which is called its parity.

- id is an even permutation.
- Any transposition is odd.
- A $k$-cycle is a product of $(k - 1)$ transpositions, so is even if $k$ is odd and odd if $k$ is even. (Confusing!)
- In general, the parity of a permutation is the parity of the number of even cycles in its cycle decomposition.

The proposition is tricky to prove from first principles. It is not hard if you know properties of determinants (but it is tricky to prove properties of determinants).

Given $\sigma \in S_n$, the associated permutation matrix is

$$A_\sigma := [e_{\sigma(1)} \ e_{\sigma(2)} \ \cdots \ e_{\sigma(n)}].$$

Note that left multiplication by $A_\sigma$ sends standard basis vectors to standard basis vectors according to the permutation $\sigma$:

$$A_\sigma e_k = e_{\sigma(k)}.$$

32.3. Exercise. The function $\sigma \mapsto A_\sigma$ defines a group homomorphism $S_n \to GL_n(\mathbb{R})$. (Hint: show $A_\sigma A_\tau e_k = A_{\sigma \tau} e_k$.)

We define $\text{sgn}: S_n \to \{\pm 1\} \subset \mathbb{R}^\times$ by

$$\text{sgn}(\sigma) := \det A_\sigma,$$

called the sign of the permutation. The function $\text{sgn}$ is a homomorphism: $\text{sgn}(\sigma \tau) = \text{sgn}(\sigma) \text{sgn}(\tau)$.

W 27 Sep

32.4. Exercise. The sign of a transposition is always $-1$. The sign of a $k$-cycle is $(-1)^{k-1}$.

Proof. We can divide permutations into two types: ones with $\text{sgn}(\sigma) = 1$ and ones with $\text{sgn}(\sigma) = -1$. It is clear that if $\sigma = \tau_1 \cdots \tau_k$ where $\tau_i$ are transpositions, then $\text{sgn}(\sigma) = (-1)^k$.

Thus, $\text{sgn}(\sigma) = 1$ implies that $\sigma$ can only be written as a product of an even number of transpositions, etc. \qed

The alternating group $A_n \leq S_n$ is the subset consisting of only even permutations. Since $A_n = \text{Ker} \text{sgn}$ it is a subgroup.

32.5. Example. The 15 puzzle.

33. Cayley’s theorem

33.1. Theorem (Cayley). Every group of order $n$ is isomorphic to a subgroup of $S_n$.

Proof. I’m going to use the facts (given as an exercise), that if a set $X$ has size $n$, then $\text{Sym}(X) \approx S_n$, and that this isomorphism sends subgroups of $\text{Sym}(X)$ isomorphically to subgroups of $S_n$. Thus, we will construct an isomorphism between $G$ and some subgroup of a $\text{Sym}(X)$.

Fix $G$ of order $n$, and let $X = G$. Define a homomorphism $\phi: G \to \text{Sym}(G)$ by

$$\phi(g) := L_g.$$
That is, $\phi(g)$ is defined to be the function $G \to G$ defined by left-multiplication by $x$, where $L_g(x) = gx$.

Exercise: Check that this is actually a homomorphism. (Note: for comparison, right-multiplication would not define a homomorphism.)

Claim: $\phi$ is injective. Since it is a group homomorphism, we just have to compute $\ker \phi$. If $g \in \ker \phi$ then $L_g(1) = e$. Thus $L_g(e) = ge = e$, whence $g = e$. Therefore $\ker \phi = \{e\}$.

Thus, $\phi$ restricts to an isomorphism between $G$ and the subgroup $\phi(G) \leq \text{Sym}(X)$.

34. Cosets

Let $H \leq G$ be a subgroup. Define an equivalence relation $\sim^r_H$ on $G$ (meaning “right $H$-equivalent), by

$$g \sim^r_H g' \iff \text{there exists } \ h \in H \text{ such that } g' = hg.$$  

Exercise: $\sim^r_H$ is an equivalence relation.

An equivalence class for $\sim^r_H$ is called a right $H$-coset. These all have the form

$$Hg = \{hg \mid h \in H\}$$

for some $g \in G$. They partition $G$ into pairwise disjoint nonempty subsets.

Note: $He = H$, so the subgroup is always one of the right cosets.

34.1. Example. $G = S_3$, $H = \{e, (1 2)\}$. $H' = \{e, (1 2 3), (1 3 2)\}$.

We can also define $\sim^l_H$ on $G$ by $g \sim^l g'$ if $g' = gh$ for some $h \in H$. An equivalence class for $\sim^l_H$ is called a left $H$-coset, having the form

$$gH = \{gh \mid h \in H\},$$

for some $g \in G$.

34.2. Example. Let $G = S_3$ and $H = \langle(1 2)\rangle$. Show that right cosets are not the same as left cosets in general.

We will write $H \backslash G$ for the set of right cosets, and $G/H$ for the set of left cosets. It is important to note that these may not be the same.

35. Lagrange’s theorem

35.1. Proposition. Let $H \leq G$ be a subgroup. Every right coset $Hg \subseteq G$ can be put in bijective correspondence with $H$.

Proof. $H \to Hg$ by $h \mapsto hg$ is a bijection, with inverse $Hg \to H$ by $x \mapsto xg^{-1}$.

We write $[G : H]$ for the number of right $H$-cosets in $G$. This is called the index of $H$ in $G$. It can be infinite. It will be finite if $G$ is finite, but it can be finite even if $G$ is infinite.

35.2. Example. The subgroup $\mathbb{R}^\times_{>0} \leq \mathbb{R}^\times$ has index 2.

35.3. Example. The subgroup $D_n \leq GL_3(\mathbb{R})$ has infinite index.

35.4. Theorem (Lagrange). If $G$ is a finite group, and $H$ is a subgroup, then $|G| = [G : H]|H|$. In particular, the order of a subgroup divides the order of the larger group.

Proof. Right cosets partition $G$ into pairwise disjoint subsets, all of which have the same size as $H$.

Remark: if $H = \langle a \rangle$ is a cyclic subgroup, then $|H| = \text{order}(a)$, and we recover the order theorem as a special case.
35.5. Exercise. Every left coset \( gH \subseteq G \) can also be put into bijective correspondence with \( H \). Thus, if \( G \) is finite, \([G : H]\) also counts the number of left \( H \)-cosets.

35.6. Exercise. Show that
\[ Hg \mapsto g^{-1}H \]
is a well-defined function, giving a bijection between the set of right \( H \)-cosets and the set of left \( H \)-cosets.

Note: \( Hg \mapsto gH \) is not generally well-defined; why not?

35.7. Example (On PS). Subgroups of \( D_4 \).

36. Normal subgroups

It is obvious that if \( G \) is abelian, then for any subgroup \( H \) we have \( Ha = aH \), so right cosets are the same as left cosets. This can happen sometimes in non-abelian groups.

A subgroup \( N \leq G \) is normal if for all \( n \in N \) and \( g \in G \), we have \( gng^{-1} \in N \).

36.1. Remark. For a subgroup \( H \leq G \) and \( g \in G \), we typically write \( gHg^{-1} \) for the set
\[ gHg^{-1} := \{ ghg^{-1} | h \in H \} \]
of all conjugates of elements of \( H \) by \( g \). Exercise: \( gHg^{-1} \) is also a subgroup of \( G \).

Thus, \( H \) is normal iff \( gHg^{-1} \subseteq H \) for all \( g \in G \). You can actually prove that if \( H \) is normal, then \( gHg^{-1} = H \).

36.2. Proposition. \( H \leq G \) is normal if and only if \( Ha = aH \) for all \( a \in G \).

Proof. If \( H \) is normal, then for \( a \in G \) and \( h \in H \) we have
\[ ah = ah(a^{-1}a) = (aha^{-1})a \in Ha, \]
so \( aH \subseteq Ha \), and conversely
\[ ha = (aa^{-1})ha = a(a^{-1}h(a^{-1})^{-1}) \in aH \]
so \( Ha \subseteq aH \). Together this says \( Ha = aH \).

Conversely, suppose \( Ha = aH \) for all \( a \in G \). Then for \( h \in H \) we have that \( ah = h'a \) for some \( h' \in H \). Thus
\[ aha^{-1} = h'aa^{-1} = h, \]
which proves \( H \) is normal. \( \square \)

If \( H \) is a normal subgroup, we can just talk about \( H \)-cosets (not left or right, since they are the same).

Normal subgroups are the only groups which can be kernels of homomorphisms.

36.3. Proposition. If \( \phi: G \to H \) is a homomorphism, then \( K = \text{Ker } \phi \) is a normal subgroup of \( G \).

Proof. If \( k \in K \) and \( g \in G \), then \( \phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)e\phi(g)^{-1} = e \), so \( gkg^{-1} \in K = \text{Ker } \phi \). \( \square \)

36.4. Example. The subgroup \( H = \langle a \rangle \) of \( D_3 = \{e, r, r^2, a, ra, r^2a\} \) is not normal.

36.5. Exercise (On PS ?). Let \( G = GL_2(\mathbb{R}) \) and \( H = SO(2) \). Is \( H \) normal in \( G \)?

36.6. Example. Let \( G = S_4 \) and let \( N = \langle e, (12)(13), (13)(24), (14)(23) \rangle \). Then \( N \) is a subgroup of \( G \), and \( N \) is normal in \( G \).

To check that \( N \) is a subgroup, just use the usual criterion. This involves checking all 16 possible products of pairs of elements of \( N \), but its not actually too bad.

To check that \( N \) is normal, just check that \( \sigma N \sigma^{-1} \subseteq N \) for all \( \sigma \in S_4 \). This is possible but tedious; I'll describe a shortcut soon.
37. Quotient groups

37.1. Example. The set of cosets of $m\mathbb{Z} \subseteq \mathbb{Z}$ are precisely the set $\mathbb{Z}/m\mathbb{Z}$ of congruence classes. Note that $\mathbb{Z}/m\mathbb{Z}$ is also a group, and the quotient map $\pi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is a surjective group homomorphism with kernel $m\mathbb{Z}$.

**Question:** If $H \leq G$ is a subgroup, can we give $G/H$ (the set of left cosets) an operation which makes it a group, so that the quotient map $\pi: G \to G/H$ is a group homomorphism? The quotient map is defined by

$$\pi(g) := gH.$$ 

Note that if this is so, then $\pi$ is surjective and $\ker \pi = H$.

**Answer:** This is possible exactly when $H$ is normal.

37.2. Proposition. Let $N \leq G$ be a normal subgroup. Then there exists a unique binary operation $\cdot: G/N \times G/N \to G/N$ which makes $G/N$ into a group, and the quotient map $\pi: G \to G/N$ into a group homomorphism.

**Proof.** Because $\pi$ is supposed to be a homomorphism, $\pi(ab) = \pi(a)\pi(b)$, which forces the formula for the operation:

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

To have an operation we first need this to be well-defined. We must show that if $aN = a'N$ and $bN = b'N$, then $abN = a'b'N$.

If $aN = a'N$ and $b = b'$ then $a' = an_1$ and $b = bn_2$ for some $n_1, n_2 \in N$. We have

$$a'b' = an_1bn_2 = a(b^{-1}n_1)n_2 = (ab^{-1})n_1n_2 = (ab)n_1b^{-1}n_2 \in abN.$$ 

Therefore $a'b'N = abN$ (because cosets are equivalence classes: if they share an element they are equal).

It remains to show that this operation satisfies the axioms of a group. This is basically straightforward:

- $eN$ is an identity element, since $(aN)(eN) = (ae)N = aN$ and $(eN)(aN) = (ea)N = aN$.
- $a^{-1}N$ is an inverse of $aN$, since $(aN)(a^{-1}N) = (aa^{-1})N = eN$ and $(a^{-1}N)(aN) = (a^{-1}a)N = eN$.
- Associative:
  
  $$(aN \cdot bN) \cdot cN = (ab)N \cdot cN = ((ab)c)N, \quad aN \cdot (bN \cdot cN) = aN \cdot (bc)N = (a(bc))N,$$
  
  which are equal because $(ab)c = a(bc)$.

Finally, that $\pi: G \to G/N$ by $\pi(a) := aN$ is a homomorphism is basically by definition. Note that $\pi$ is surjective with $\ker \pi = N$. \(\square\)

37.3. Example. Let $G = S_4$ and $N = \{e, (12)(34), (13)(24), (14)(23)\}$, which is a normal subgroup. Then we can form the quotient group $G' = G/N$, which is a group of order $[G : N] = |G| / |N| = (4!) / 4 = 6$. You can actually show that $G'$ is isomorphic to $S_3$.

38. Homomorphism theorem

38.1. Theorem. Let $\phi: G \to H$ be a homomorphism, with $N = \ker \phi$. Then there exists a unique isomorphism $\bar{\phi}: G/N \to \text{Im} \phi$ with $\bar{\phi}(aN) = \phi(a)$. 

\(\text{M 2 Oct} 3\)
Proof. First, we want to define \( \overline{\phi} \) by the formula \( \overline{\phi}(aN) = \phi(a) \). Check that this is well-defined: if \( aN = a'N \), then \( a' = an \) for some \( n \in N \), so
\[
\phi(a') = \phi(an) = \phi(a)\phi(n) = \phi(a)
\]
since \( n \in N = \text{Ker} \phi \).
Next, check that \( \overline{\phi} \) is a homomorphism. (Straightforward exercise.)
The function \( \overline{\phi} : G/N \to \text{Im} \phi \) is obviously surjective.
The kernel of \( \overline{\phi} \) is
\[
\text{Ker} \overline{\phi} = \{aN \mid \overline{\phi}(aN) = e_H \} = \{aN \mid \phi(a) = e_N \} = \{aN \mid a \in N \} = \{eN\}
\]
so \( \overline{\phi} \) is injective. Therefore \( \overline{\phi} \) is an isomorphism of groups.
For uniqueness, this is forced by the identity \( \overline{\phi}(aN) = \phi(a) \).
\( \square \)

38.2. Corollary. A subgroup is normal if and only if it is the kernel of some homomorphism.

38.3. Example. Consider \( \phi : \mathbb{R} \to SO(2) \) by \( \phi(\theta) = R_\theta \). This is surjective with \( \text{Ker} \Phi = 2\pi\mathbb{Z} \). Thus we get an isomorphism \( \mathbb{R}/2\pi\mathbb{Z} \cong SO(2) \).

38.4. Example (On PS?). We can define a homomorphism \( \phi : S_4 \to S_3 \) in the following way. Given a group of 4 people (e.g., Alice, Bob, Carol, Dave), we can divide them into pairs in three different ways:
\[
P_1 = \{\text{Alice&Bob, Carol&Dave}\}, \quad P_2 = \{\text{Alice&Carol, Bob&Dave}\}, \quad P_3 = \{\text{Alice&Dave, Bob&Carol}\}.
\]
If we permute the 4 people, we change the pairing. For instance, if we switch Alice with Bob, then the \( P_1 \) pairing would be unchanged, but the \( P_2 \) pairing would become the \( P_3 \) pairing and vice versa.
If we just number the people 1=Alice, 2=Bob, 3=Carol, and 4=Dave, the pairings become
\[
P_1 = \{(1,2), (3,4)\}, \quad P_2 = \{(1,3), (2,4)\}, \quad P_3 = \{(1,4), (2,3)\}.
\]
Then we get function \( \phi : S_4 \to S_3 \), by the rule:
\[
\phi(\sigma)(\{(a,b), (c,d)\}) = \{(\sigma(a), \sigma(b)), (\sigma(c), \sigma(d))\}.
\]
Here \( \sigma \in S_4 \), and \( \phi(\sigma) \in S_3 \), and the rule tells us how to compute \( \phi(\sigma) \) on an element \( P_k \). For instance,
\[
\phi((1 2 3))(P_1) = \phi((1 2 3))(\{(1,2), (3,4)\}) = \{(2,3), (1,4)\} = P_3,
\phi((1 2 3))(P_2) = \phi((1 2 3))(\{(1,3), (2,4)\}) = \{(2,1), (3,4)\} = P_1,
\phi((1 2 3))(P_3) = \phi((1 2 3))(\{(1,4), (2,3)\}) = \{(2,4), (3,1)\} = P_2.
\]
Thus \( \phi((1 2 3)) = (1 3 2) \). Exercises: \( \phi((1 4)) = (1 2), \phi((1 2 3 4)) = (1 2) \).

Exercise: show that \( \phi \) is a homomorphism of groups. Identify the subgroup \( N = \text{Ker} \phi \leq S_4 \), and show that \( N \) has exactly four elements. Use the isomorphism theorem to deduce that \( S_4/N \cong S_3 \).

39. Conjugation, Automorphisms, and Centers

Given \( g \in G \), the conjugation map is the function \( \text{conj}_g : G \to G \) defined by \( \text{conj}_g(x) := gxg^{-1} \).

39.1. Proposition. \( \text{conj}_g : G \to G \) is an isomorphism from \( G \) to itself.

39.2. Example. Conjugation by various elements in \( D_4 \).

An automorphism of \( G \) is any isomorphism \( G \to G \) from the group \( G \) to itself. That is, its a permutation of the set of \( G \) which is also a homomorphism. The set \( \text{Aut}(G) \) of automorphisms is a group under composition.
Every function \( \text{conj}_g \) is an automorphism of \( G \); these are called inner automorphisms. Note every automorphism is inner.
The inner automorphisms form a subgroup of \( \text{Aut}(G) \). In fact, we have
39.3. **Proposition.** The function $\phi : G \to \text{Aut}(G)$ defined by $g \mapsto \text{conj}_g$ is a homomorphism of groups. Its image is the subgroup $\text{Inn}(G) \leq \text{Aut}(G)$ of inner automorphisms.

**Proof.** Check:

$$\text{conj}_a(\text{conj}_b(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \text{conj}_{ab}(x).$$

39.4. **Exercise (On PS 6).** The kernel of $g \mapsto \text{conj}_g$ is 

$$\text{Center}(G) := \{g \in G \mid gx = xg \text{ for all } x \in G \}.$$ 

By the homomorphism theorem, it follows that $\text{Inn}(G) \cong G/\text{Center}(G)$.

39.5. **Example.** The inner automorphisms of $D_4$ consist of:

$$\text{id} = \text{conj}_e = \text{conj}_{r^4}, \quad \text{conj}_r = \text{conj}_{r^3}, \quad \text{conj}_a = \text{conj}_{a^2}, \quad \text{conj}_{ra} = \text{conj}_{r^3a}.$$ 

The group $\text{Inn}(D_4) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. Note that $\text{Center}(D_4) = \langle r^2 \rangle$.

39.6. **Example.** Compute $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$. Also $\text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$.

39.7. **Example.** For any $n \geq 1$, we have $\text{Aut}(\mathbb{Z}/n) \cong \Phi(n)$. This is because any homomorphism from a group is determined by where it sends the generators.

For $\mathbb{Z}/n = \langle [1] \rangle$, every homomorphism $\phi : \mathbb{Z}/n \to \mathbb{Z}/n$ is of the form $\phi([x]) = [a][x]$ for some $[a] \in \mathbb{Z}/n$. It is an automorphism iff $\phi([1]) = [a]$ is a generator of $\mathbb{Z}/n$, i.e., $[a] \in \Phi(n)$. The composite $[x] \mapsto [a][x]$ with $[x] \mapsto [b][x]$ is $[x] \mapsto [a][b][x]$, so $\text{Aut}(\mathbb{Z}/n) \cong \Phi(n)$.

39.8. **Example.** Let $G = \mathbb{Z}/2 \times \mathbb{Z}/2$. Then $\text{Aut}(G) \cong S_3$.

In the last three examples, $G$ was abelian, so there are no non-trivial inner automorphisms.

39.9. **Example.** Let $G = D_4$. Then $\text{Aut}(D_4) \cong D_4$. As we noted above, $\text{Inn}(D_4) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. An example of an “outer automorphism”, i.e., an automorphism which is not inner, of $D_4$ is $\phi$, which is characterized by $\phi(r) = r$, $\phi(a) = ra$.

39.10. **Exercise (On PS 6).** Show that $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

39.11. **Exercise (On PS 6).** Recall the quaternion group $Q$. Describe the conjugation maps for the quaternion group. Show that $\text{Inn}(Q) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. Show that $\text{Aut}(Q)/\text{Inn}(Q)$ is isomorphic to $S_3$, by constructing a surjective homomorphism $\text{Aut}(Q) \to S_3$ whose kernel is $\text{Inn}(Q)$. (This is not obvious!)

Thus $|\text{Aut}(Q)| = 24$. Bonus: show $\text{Aut}(Q) \cong S_4$.

Here is an interesting fact, which I will not prove and which is not at all obvious.

39.12. **Theorem.** $\text{Aut}(S_n) \cong S_n$ except when $n = 2$ or $n = 6$.

**Proof.** We know that $\text{Inn}(S_n) \approx S_n/\text{Center}(S_n)$. You can show that if $n \geq 3$, then $\text{Center}(S_n) = \{e\}$; given any non-identity permutation $\sigma$, you can find another one that doesn’t commute with it. (This is an exercise on PS6.)

Thus for $n \geq 3$, $\text{Inn}(S_n) \approx S_n$. The theorem amounts from the fact that $S_n$ has no outer automorphisms except when $n = 6$. This is not so easy to prove. 

39.13. **Example.** (I probably won’t do this in class. You don’t need to know it, it’s just here for fun.)

I’ll try to construct an outer automorphism of $S_n$, using the following idea.

Suppose we can find a subgroup $H \leq S_n$ of index $n$. Consider the left $H$-cosets: there are exactly $n$ of them. Let’s number them: $G/H = \{g_1H, g_2H, \ldots, g_nH\}$. Left multiplication by $S_n$ permutes the cosets: i.e., given $\sigma \in S_n$, we get a permutation of $G/H$ sending $g_iH \mapsto \sigma g_iH$. Since $G/H$
has six elements numbered 1, . . . , n, we can think of this as another element of $S_n$. Thus, we get a homomorphism
\[ \phi: S_n \to S_n \]
induced by this choice of $H$.

There is a boring choice of $H$, which gives an inner automorphism. For instance, let $H = \{ g \in S_6 \mid g(6) = 6 \}$, the subgroup of permutations which fix 6. This gives you an inner automorphism. (Which one you get depends on how you number the cosets.)

However, there is an “exotic” subgroup of index 6 in $S_6$, which gives you an outer homomorphism. It is a subgroup $H$ which is isomorphic to $S_5$, but which acts on six things in an interesting way.

Draw “mystic pentagons”, i.e., 2-colorings of the complete graph on 5 vertices so that each colored set is a 5-cycle. This gives an action of $S_5$ on a six element set, so a subgroup $H \leq S_6$ such that $H \cong S_5$.

Give a reference here.

Conjugation also gives rise to other $G$ actions. For instance, let $\text{Sub}(G)$ be the set of all subgroup of $G$. Note that if $H \leq G$ is a subgroup, then so is $gHg^{-1}$. Thus we get an action of $G$ on $\text{Sub}(G)$ by conjugation. We say that two subgroups are conjugate subgroups if they are related this way: i.e., $H$ and $H' = gHg^{-1}$ are conjugate.

40. Conjugacy classes

Conjugation defines an equivalence relation on the elements of a group $G$: so $x \sim_{\text{conj}} y$ if and only if there exists $g \in G$ such that $y = gxg^{-1}$. The equivalence classes are called conjugacy classes, and we write
\[ \text{Cl}(x) = \{ gxg^{-1} \mid g \in G \}. \]

40.1. Example. Conjugacy classes in $D_4$ are:
\{e\}, \{r^2\}, \{r, r^3\}, \{a, r^2a\}, \{ra, r^3a\}.

Given an element $g \in G$, its centralizer is
\[ \text{Cent}(g) = \{ x \in G \mid gx = xg \}. \]

Warning. The centralizer of an element is not the same as the center of a group.

40.2. Proposition. $H = \text{Cent}(g)$ is a subgroup, and there is a bijection
\[ G/H \cong \text{Cl}(g). \]

Proof. We leave checking subgroup as an exercise. For the second, the bijection is given by
\[ xH \mapsto xgx^{-1}. \]
We need to check that this is well-defined, and is a bijection. \hfill \square

40.3. Corollary. In a finite group, the size of a conjugacy class divides the order of the group.

41. Conjugacy classes in symmetric groups.

We have a nifty formula for conjugation in $S_n$.

41.1. Proposition. For any $\sigma \in S_n$, and for $\gamma = (a_1 \cdots a_k)$ a k-cycle in $S_n$, we have that
\[ \text{conj}_\sigma \gamma = \sigma(a_1 \cdots a_k)\sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_k)). \]

Proof. Just a calculation. Let $x \in \{1, \ldots, n\}$. There are two cases:
\begin{itemize}
  \item If $x = \sigma(a_i) \in \{\sigma(a_1), \ldots, \sigma(a_k)\}$, then $y = \sigma^{-1}(x) = a_i$, so
  \[ \sigma(a_1 \cdots a_k)\sigma^{-1}(x) = \sigma(a_1 \cdots a_k)a_i = \sigma(a_{i+1}), \]
  except that if $i = k$, then we actually get $\sigma(a_1 \cdots a_k)\sigma^{-1}(x) = \sigma(a_1)$.
\end{itemize}
• If \( x \not\in \{ \sigma(a_1), \ldots, \sigma(a_k) \} \), then \( y = \sigma^{-1}(x) \) is not in \( \{a_1, \ldots, a_k\} \), so
\[
\sigma(a_1 \cdots a_k)\sigma^{-1}(x) = \sigma(a_1 \cdots a_k)(y) = \sigma(y) = x.
\]
So \( \sigma \gamma \sigma^{-1} \) cyclically permutes the \( \sigma(a_1), \ldots, \sigma(a_k) \), and fixes all other elements. \( \square \)

Because conjugation is a homomorphism, you can apply this to products: for instance, if \( \sigma = (2\,7\,1) \) in \( S_9 \), then
\[
\sigma((3\,9\,2\,4\,5)(1\,7)(6\,8))\sigma^{-1} = (3\,9\,7\,4\,5)(2\,1)(6\,8).
\]
The moral is that, though it is hard to compose permutations written in cycle decomposition, it is easy to conjugate them.

41.2. Corollary. The conjugacy classes of \( S_n \) correspond exactly to cycle decomposition types.

Proof. It remains to show that if two permutations \( \sigma \) and \( \tau \) have the same cycle type, they are conjugate. In fact, you can always find a \( g \) such that \( \tau = g\sigma g^{-1} \) by inspection. For instance, if
\[
\sigma = (3\,9\,7)(4\,8)(6\,2), \quad \tau = (7\,5\,6)(3\,8)(1\,9)
\]
in \( S_9 \), then just choose a permutation that sends
\[
3 \to 7, \quad 9 \to 5, \quad 7 \to 6, \quad 4 \to 3, \quad 8 \to 8, \quad 6 \to 1, \quad 2 \to 9,
\]
and then fill in the remaining elements. Thus we can take
\[
g = 
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
* & 9 & 7 & 3 & * & 1 & 6 & 8 & 5
\end{pmatrix}
\]
where the \( * \) are either 2 or 4 (it doesn’t matter which is which.). \( \square \)

Example. The conjugacy classes in \( S_5 \):

<table>
<thead>
<tr>
<th>cycle type</th>
<th>form</th>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>((a,b,c,d,e))</td>
<td>((5\cdot4\cdot3\cdot2\cdot1)/5 = 24)</td>
</tr>
<tr>
<td>4 + 1</td>
<td>((a,b,c,d))</td>
<td>((5\cdot4\cdot3)/4 = 30)</td>
</tr>
<tr>
<td>3 + 2</td>
<td>((a,b,c)(d,e))</td>
<td>((5\cdot4\cdot3)/3 \times (2\cdot1)/2 = 20)</td>
</tr>
<tr>
<td>3 + 1 + 1</td>
<td>((a,b,c))</td>
<td>((5\cdot4\cdot3)/3 = 20)</td>
</tr>
<tr>
<td>2 + 2 + 1</td>
<td>((a,b)(c,d))</td>
<td>((5\cdot4)/2 \times (3\cdot2)/2 = 15)</td>
</tr>
<tr>
<td>2 + 1 + 1 + 1</td>
<td>((a,b))</td>
<td>((5\cdot4)/2 = 10)</td>
</tr>
<tr>
<td>1 + 1 + 1 + 1</td>
<td>(e)</td>
<td>(1)</td>
</tr>
</tbody>
</table>

Note that \( 24 + 30 + 20 + 20 + 15 + 10 + 1 = 120 = 5! \), as expected.

41.3. Proposition. The only normal subgroups in \( S_5 \) are \( \{e\} \), \( A_5 \), and \( S_5 \).

Proof. A normal subgroup \( N \leq G \) has \( gNg^{-1} = N \). That is, if \( x \in N \) then so is every element of its conjugacy class. So normal subgroups are always unions of conjugacy classes.

We also know that \( |N| \) divides \( |G| \), and that \( e \in N \). So we look for collections of conjugacy classes in \( S_5 \) that add up to a divisor of 120 which can be written as a sum of some of the numbers in the list: 1, 10, 15, 20, 24, 30, where we must use 1 as one of numbers in the sum.

The divisors of 120 = \( 2^3 \cdot 3 \cdot 5 \) are:
\[
1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120.
\]
By going through the possibilities, the only ones that we can write as sums of conjugacy classes are:
\[
1, \quad 40 = 1 + 15 + 24, \quad 60 = 1 + 15 + 20 + 24, \quad 120 = \text{sum of all}.
\]
To get \(|N| = 40\), we must have \( N \) consists of: \( e \), all elements of the form \((a\,b\,c\,d\,e)\), and all elements of the form \((a\,b)(c\,d)\). But we can compute \((1\,2\,3\,4\,5)(1\,2)(3\,4) = (1\,3\,5)\) a 3-cycle. So this cannot be a subgroup.

To get \(|N| = 60\), we have two ways (there are two conjugacy classes of size 20):

1. \( (1\,2\,3\,4\,5)(1\,2)(3\,4) = (1\,3\,5) \)
2. \( (1\,2\,3\,4\,5)(1\,2)(3\,4) = (1\,3\,5) \)
• all elements of forms $e$, $(a \ b)(c \ d)$, $(a \ b \ c)$, $(a \ b \ c \ d \ e)$. These are exactly all the even permutations, so this is $A_5$.
• all elements of forms $e$, $(a \ b)(c \ d)$, $(a \ b \ c)(c \ d)$, $(a \ b \ c \ d \ e)$. But this is not a subgroup, e.g., $(1 \ 2 \ 3)(4 \ 5)((1 \ 2)(3 \ 4)) = (1 \ 2)$ is not in this set.

So the only non-trivial normal subgroup is $A_5$. □

Conjugacy classes in $A_5$

If $C \subseteq S_n$ is a conjugacy class consisting of odd permutations, then $C \cap A_n = \emptyset$; if it consists of even permutations, then $C \subseteq A_n$. However, $C$ might or might not be a conjugacy class in $A_n$.

41.4. Example. The conjugacy class $C = \{(a \ b \ c)\} = \text{Cl}_{S_5}((1 \ 2 \ 3))$ in $S_5$ is also a conjugacy class in $A_5$. To see this, suppose given $g = (a \ b \ c), g' = (a' \ b' \ c') \in C$. We know that there exists a permutation (in fact, many permutations) such that $g' = \sigma g \sigma^{-1}$; the problem is whether there is an even permutation which does this. But that is ok: if $\sigma$ is odd, then $\tau = \sigma(d \ e)$ is even (where $\{d, e\} \cap \{a, b, c\} = \emptyset$), and $\tau g \tau^{-1} = g'$ also.

41.5. Example. The conjugacy class $C = \{(a \ b \ c \ d \ e)\}$ in $S_5$ is not a conjugacy class in $A_5$. For instance, there is no even permutation $\sigma$ such that

$$\sigma(1 \ 2 \ 3 \ 4 \ 5)\sigma^{-1} = (1 \ 2 \ 3 \ 5 \ 4).$$

Proof: $\sigma(1 \ 2 \ 3 \ 4 \ 5)\sigma^{-1} = (\sigma(1) \ \sigma(2) \ \sigma(3) \ \sigma(4) \ \sigma(5))$. I want to show this cannot be $(1 \ 2 \ 3 \ 5 \ 4)$, but remember that this 5-cycle can be written in 5 ways:

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

In each of the 5 cases we can see exactly what $\sigma$ needs to be, and we check in each case that it is an odd permutation. (In this example, they are $\sigma = (45), (1235), (134)(25), (153)(24), (1432)$.)

In fact we get two conjugacy classes in $A_5$:

$$C = \text{Cl}_{S_5}((1 \ 2 \ 3 \ 4 \ 5)) = C_1 \cup C_2, \quad C_1 = \text{Cl}_{A_5}((1 \ 2 \ 3 \ 4 \ 5)), \quad C_2 = \text{Cl}_{A_5}((1 \ 2 \ 3 \ 5 \ 4)).$$

If $g = \sigma(1 \ 2 \ 3 \ 4 \ 5)\sigma^{-1} \in C$, then either $\sigma$ is even, so $g \in \text{Cl}_{A_5}((1 \ 2 \ 3 \ 4 \ 5))$, or $\sigma$ is odd, and if we set $\tau = \sigma(4 \ 5)$ so $\sigma = \tau(4 \ 5)$ then

$$g = \sigma(1 \ 2 \ 3 \ 4 \ 5)\sigma^{-1} = \tau(4 \ 5)(1 \ 2 \ 3 \ 4 \ 5)(4 \ 5)\tau^{-1} = \tau(1 \ 2 \ 3 \ 5 \ 4)\tau^{-1},$$

so $g \in \text{Cl}_{A_5}((1 \ 2 \ 3 \ 5 \ 4))$.

I did not do the following proof in class, though I did examples in the case $n = 5$. You don’t need to know it.

41.6. Proposition. If $C \subseteq S_n$ is a conjugacy class of even permutations in $S_n$, then either:

1. $C \subseteq A_n$ is a conjugacy class in $A_n$, or
2. $C = C_1 \cup C_2$ where $C_1, C_2 \subseteq A_n$ are distinct conjugacy classes in $A_n$. In this case $C_1 \cap C_2 = \emptyset$ and $|C_1| = |C_2| = |C|/2$.

Case (1) happens if and only if there exists an odd permutation $\tau \in S_n \setminus A_n$ such that $\tau g \tau^{-1} = g$.

Proof. Let $C = \text{Cl}_{S_n}(g)$ be a conjugacy class of $S_n$ which is contained in $A_n$. Define:

- $C_1 := \{\sigma g \sigma^{-1} \mid \sigma \in A_n\}$,
- $C_2 := \{\tau g \tau^{-1} \mid \tau \in S_n \setminus A_n\}$.

It is clear that $C_1 = \text{Cl}_{A_n}(g)$, the conjugacy class of $g$ in $A_n$. The set $C_2$ is also a conjugacy class in $A_n$, since if $\tau$ is an odd permutation, then for any even permutation $\sigma$ we have

$$\sigma(\tau g \tau^{-1})\sigma^{-1} = (\sigma \tau)g(\sigma \tau)^{-1} \in C_2,$$

since $\sigma \tau$ is also an odd permutation.

It is obvious that $C = C_1 \cup C_2$. 

W 11 Oct
Because $C_1$ and $C_2$ are $A_n$-conjugacy classes, either: (1) they are equal, or (2) they have empty intersection. Let’s think about the two cases.

(1) If $C_1 = C_2$, then this set is also equal to $C$: the $S_n$-conjugacy class is also an $A_n$-conjugacy class. Because they are equal the element $g \in C_2$, so there exists an odd permutation $\tau$ such that $g = \tau g \tau^{-1}$.

(2) If $C_1 \cap C_2 = \emptyset$, then $C$ is partitioned into the two subsets $C_1$ and $C_2$. In this case, there cannot be an odd permutation $\tau$ such that $g = \tau g \tau^{-1}$, since if that were true then $g$ would be in both sets.

In this case there is a bijection $C_1 \sim C_2$ given by $x \mapsto (1 2)x(1 2)^{-1}$, so $|C_1| = |C_2| = \frac{1}{2} |C|$.

\[ \square \]

So the conjugacy classes in $A_5$ are:

<table>
<thead>
<tr>
<th>cycle type</th>
<th>example</th>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5_1$</td>
<td>(1 2 3 4 5)</td>
<td>12</td>
</tr>
<tr>
<td>$5_2$</td>
<td>(1 2 3 5 4)</td>
<td>12</td>
</tr>
<tr>
<td>$3 + 1 + 1$</td>
<td>(1 2 3)</td>
<td>20</td>
</tr>
<tr>
<td>$2 + 2 + 1$</td>
<td>(1 2)(3 4)</td>
<td>15</td>
</tr>
<tr>
<td>$1 + 1 + 1 + 1 + 1$</td>
<td>$e$</td>
<td>1</td>
</tr>
</tbody>
</table>

41.7. **Corollary.** The only normal subgroups of $A_5$ are $e$ and $A_5$. In particular, if $\phi: A_5 \to G$ is a homomorphism that sends one non-identity element to a non-identity element, then $\phi$ is injective.

**Proof.** Check that no divisor of 60 is a sum of 1 plus a subset of 12, 12, 15, 20. \[ \square \]

A **simple group** is a group $G$ which is not equal to $\{e\}$ and has no normal subgroups other than $\{e\}$ and $G$. Thus $A_5$ is simple. Also, $\mathbb{Z}/p$ is simple for $p$ prime.

One way to try to classify finite groups is the following: given $G$, find a non-trivial normal subgroup $N \leq G$. Then you get two smaller groups: $N$ and $G/N$. Iterate this process on $N$ and $G/N$ until you only have finite simple groups.

**Neat fact (Jordan-Holder theorem).** No matter how you do this to a finite group $G$, the list of finite simple groups $H_1, \ldots, H_k$ you get from this process is the same. These are called the **composition factors** of $G$.

**Problem.** Classify all finite simple groups.

**Answer.** This was done around 1983. The proof takes about 10000 pages. The finite simple groups are:

- The cyclic groups of prime order $\mathbb{Z}/p$.
- The alternating groups $A_n$ for $n \geq 5$.
- The groups of “Lie type”, which are basically groups of matrices with entries in a finite field (like $\mathbb{Z}/p$). For instance, $SL_n(\mathbb{Z}/p) = \text{matrices with entries in } \mathbb{Z}/p \text{ with det } = 1$. (This is not actually simple, but $PSL_n(F) = SL_n(F)/F^\times$ is simple.) The groups of Lie type fit into a small number of infinite families that are not hard to list.
- 26 “sporadic” simple groups, that don’t fit into one of the above classes. The largest of these is called the **monster group**, it has about $8 \times 10^{53}$ elements.

42. **Group actions**

An **action** of a group $G$ on a set $X$ is a map $(g, x) \mapsto g \cdot x: G \times X \to X$

satisfying the identities

\[ e \cdot x = x \quad \text{and} \quad g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \quad \text{for all } g_1, g_2 \in G, x \in X. \]
Exercise: why is this true?) The orbits of this action correspond exactly to the cycles in the cycle example.

Example 43.2. Proposition. Given a permutation \( \phi \) of \( G \) of the identities \( e \) at elements \( x \) for the orbit it is contained in.

Example 42.4. Proposition. Given an action of \( G \) on \( X \), define \( \phi : G \to \text{Sym}(X) \) by \( \phi(g)(x) := g \cdot x \). Then \( \phi \) is a homomorphism of groups.

Conversely, if \( \phi : G \to \text{Sym}(x) \) is a homomorphism of groups, then the operation defined by \( g \cdot x := \phi(g)(x) \) is an action.

Proof. Easy. We are just messing around with notation.

Given an action “\( \cdot \)”, we check that \( \phi \) is a homomorphism: to show \( \phi(g_1 g_2) = \phi(g_1) \phi(g_2) \), evaluate at elements \( x \in X \):

\[
\phi(g_1 g_2)(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \phi(g_1)(g_2 \cdot x) = (\phi(g_1) \phi(g_2))(x).
\]

Conversely, given a homomorphism \( \phi : G \to \text{Sym}(X) \), to show we need an action we need to check the identities \( e \cdot x = x \) and \( g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \):

\[
e \cdot x = \phi(e)(x) = x,
g_1 \cdot (g_2 \cdot x) = \phi(g_1)(\phi(g_2)(x)) = (\phi(g_1) \phi(g_2))(x) = \phi(g_1 g_2)(x) = (g_1 g_2) \cdot x.
\]

\( \square \)

43. Orbits and stabilizers

Given an action of \( G \) on \( X \), we get:

- a partition of \( X \) into pairwise disjoint orbits, and
- for each element \( x \in X \), a subgroup of \( G \) called the stabilizer of \( x \).

Given an action, define an equivalence relation on \( X \) by

\[x \sim x' \iff \text{exists } g \in G \text{ such that } x' = g \cdot x.\]

I.e., two elements are related if one can be sent to the other using the action of an element of \( G \).

43.1. Exercise (PS 7). This is an equivalence relation.

The equivalence classes of the action are called orbits. Given \( x \in X \), write

\[G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X\]

for the orbit it is contained in.

43.2. Example. Let \( G \) be a group isomorphic to \( \mathbb{Z} \), but written multiplicatively. Thus, the elements of \( G \) will be written \( f^n \) for \( n \in \mathbb{Z} \), where \( f \) is a symbol, and the group law is \( f^m f^n = f^{m+n} \).

Given a permutation \( \phi \in \text{Sym}(X) \), we get an action of \( G \) on \( X \) by

\[f^n \cdot x := \phi^n(x).\]

(Exercise: why is this true?) The orbits of this action correspond exactly to the cycles in the cycle decomposition of \( \phi \).
The **stabilizer subgroup** of an element \( x \in X \) is 

\[
\text{Stab}(x) := \{ g \in G \mid g \cdot x = x \},
\]

the subset of elements of \( G \) that “act trivially” on \( x \).

43.3. **Exercise** (PS 7). Exercise: \( \text{Stab}(x) \) is a subgroup of \( G \).

43.4. **Exercise** (Important, PS 7). Suppose \( G \) acts on \( X \), and suppose \( y = g \cdot x \) for some \( x, y \in X \) and \( g \in G \). Show that the function 

\[
\text{conj}_g \colon \text{Stab}(x) \to \text{Stab}(y)
\]

is well-defined, and gives an isomorphism between the subgroups \( \text{Stab}(x) \) and \( \text{Stab}(y) \).

Thus, elements in the same orbit have **conjugate** stabilizers.

43.5. **Theorem** (Orbit-stabilizer theorem). If group \( G \) acts on a set \( X \), then there is a bijective correspondence 

\[
G / \text{Stab}(x) \sim [G : \text{Stab}(x)] \to W \subseteq G \cdot x
\]

between left-cosets of \( \text{Stab}(x) \) and elements in the orbit of \( x \).

In particular, if \( G \) is finite then 

\[
[G : \text{Stab}(x)] = |G : x|, \quad |G| = |G : x| |\text{Stab}(x)|,
\]

so the size of an orbit divides the order of \( G \).

**Proof.** Left as an exercise (PS 7).

44. **Examples of group actions**

44.1. **Example** (Left action by a subgroup). Let \( G \) be a group and \( H \leq G \) a subgroup. Then \( H \) acts on the set \( X = G \) by the formula:

\[
h \cdot g := hg, \quad h \in H, g \in G.
\]

This is called the **left action** of \( H \) on \( G \).

Exercise: The orbits of this action are exactly the **right** \( H \)-**cosets**.

Question: For \( g \in G \), what is \( \text{Stab}_H(g) \)?

44.2. **Example** (Right action by a subgroup). Let \( G \) be a group and \( H \leq G \) a subgroup. Then \( H \) acts on the set \( X = G \) by the formula:

\[
h \cdot g := gh^{-1}, \quad h \in H, g \in G.
\]

This is called the **right action** of \( H \) on \( G \).

Exercise: The orbits of this action are exactly the **right** \( H \)-**cosets**.

Question: For \( g \in G \), what is \( \text{Stab}_H(g) \)?

44.3. **Exercise** (PS 7). Show that for \( H \leq G \), the formula \( h \cdot g := gh \) gives a well-defined action of \( H \) on the set of \( G \) if and only if \( H \subseteq \text{Center}(G) \).

44.4. **Example** (Conjugation action). Let \( G \) be a group. Then \( G \) acts on the set \( X = G \) by the formula:

\[
g \cdot x := gxg^{-1}, \quad x, g \in G.
\]

This is called the **conjugation action** of \( G \) on itself.

**Warning.** We try very hard to avoid using the “\( \cdot \)” notation for the conjugation action, because it looks too much like multiplication. E.g., better to write \( \text{conj}_g(x) \). However, it is still an action.

Exercise: The orbits of this action are exactly the **conjugacy classes**.

Exercise: The stabilizers of this action are exactly the **centralizers**, i.e., \( \text{Stab}(x) = \text{Cent}(x) \).

The orbit stabilizer theorem \([G : \text{Stab}(x)] = |G : x|\) becomes the conjugacy class theorem: \([G : \text{Cent}(x)] = |\text{Cl}(x)|\).
44.5. Example (Permutation action of \( S_n \)). Let \( G = S_n \) and \( X = \mathbb{n} = \{1, \ldots, n\} \). Then \( S_n \) acts on \( X \) by \[
\sigma \cdot k := \sigma(k).
\]
Orbit(s)? Centralizers?

44.6. Example (Action of cycles). Let \( \sigma \in S_n \) and let \( G = \langle \sigma \rangle \), and let \( X = \mathbb{n} \). Then we get an action of \( G \) on \( X \).

Orbits= cycles in the cycle decomposition of \( \sigma \).

What are centralizers?

44.7. Example (Action of \( \text{SO}(3) \) on \( \mathbb{R}^3 \). Important!). Elements of \( \text{SO}(3) \) act on \( \mathbb{R}^3 \) by matrix multiplication: \( A \cdot x := Ax \).

Orbits. The orbits of the action are precisely the sets \[
S_r := \{ x \in \mathbb{R}^3 \mid |x| = r \}, \quad r \geq 0.
\]
There is one finite orbit: \( S_0 = \{0\} \). The remaining orbits \( S_r \) with \( r > 0 \) are spheres centered around the origin. The idea is that given two vectors \( x \) and \( x' \) of the same length, you can always find a rotation \( A \) such that \( Ax = x' \).

Stabilizers. The stabilizer of \( x = 0 \) is the whole group:

\[
\text{Stab}(0) = \text{SO}(3).
\]

For any non-zero vector \( x \), the stabilizer is a subgroup \[
\text{Stab}(x) \leq \text{SO}(3).
\]

Claim. Every \( \text{Stab}(x) \) for \( x \neq 0 \) is isomorphic to \( \text{SO}(2) \).

Sketch proof. By an earlier fact, if \( x \) and \( y \) are in the same orbit, \( \text{Stab}(x) \) and \( \text{Stab}(y) \) are conjugate subgroups, and therefore are isomorphic as groups. Thus we can assume WLOG that \( x = (r,0,0) \) for some \( r > 0 \). The second step is to explicitly identify this subgroup of \( \text{SO}(3) \) with \( \text{SO}(2) \). [PS 7]

44.8. Example (Action of \( D_4 \) on \( \mathbb{R}^3 \)). Standard action of \( D_4 \) on \( \mathbb{R}^3 \), as symmetries of the square with vertices \((\pm 1, \pm 1, 0)\). For each point in \( \mathbb{R}^3 \), we can compute a stabilizer group.

45. Regular polyhedra

A regular polyhedron is a polyhedron all of whose faces are congruent regular polygons, and which have the same number of faces at each vertex. There are five: tetrahedron, cube and octahedron, dodecahedron and icosahedron.

<table>
<thead>
<tr>
<th></th>
<th>vertices</th>
<th>edges</th>
<th>faces</th>
<th>vertices/edges per face</th>
<th>faces/edges per vertex</th>
</tr>
</thead>
<tbody>
<tr>
<td>tetrahedron</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>cube</td>
<td>8</td>
<td>12</td>
<td>6</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>octahedron</td>
<td>6</td>
<td>12</td>
<td>8</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>dodecahedron</td>
<td>20</td>
<td>30</td>
<td>12</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>icosahedron</td>
<td>12</td>
<td>30</td>
<td>20</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

Plato observed that these are all the regular polyhedra (which is why they are called “platonic solids”). We are going to sketch a proof of this.

The symmetry group of a polyhedron (centered at the origin, with vertices \( V \)) is the subgroup \( G \subseteq \text{SO}(3) \) such that \( g \cdot v \in V \) for all \( v \in V \).

Because every element of \( G \) is a rotation, it must take vertices to vertices, edges to edges, and faces to faces. Here is one way to compute the order of the symmetry group \( G \). Fix an edge, and label its endpoints \( A \) and \( B \). (I like to think of attaching a “handle” to this edge.) Any symmetry
must take the “vector” \( \overrightarrow{AB} \) to another vector \( \overrightarrow{A'B'} \), where \( A' \) and \( B' \) are also the endpoints of an edge. This information completely determines the symmetry, and for every directed edge \( \overrightarrow{A'B'} \) there is a unique symmetry taking \( \overrightarrow{AB} \) to \( \overrightarrow{A'B'} \). Thus we have

\[ |G| = 2 \times (\text{number of edges}). \]

<table>
<thead>
<tr>
<th>symmetry group</th>
<th>order of symmetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>tetrahedron</td>
<td>12</td>
</tr>
<tr>
<td>cube</td>
<td>24</td>
</tr>
<tr>
<td>octahedron</td>
<td>24</td>
</tr>
<tr>
<td>dodecahedron</td>
<td>60</td>
</tr>
<tr>
<td>icosahedron</td>
<td>60</td>
</tr>
</tbody>
</table>

All non-identity symmetries will be rotations through an axis which passes through the center of the polyhedron (which we will assume is the origin), through an angle \( 2\pi/n \). So we can organize symmetries according to (i) the axis of the symmetry, and (ii) their order.

45.1. **Symmetries of the tetrahedron.** Here are the symmetries of the tetrahedron.

<table>
<thead>
<tr>
<th>axis of symmetry</th>
<th>number of axes</th>
<th>angle of rotation</th>
<th>number of symmetries</th>
<th>order of symmetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>vertex/centroid of opposite faces</td>
<td>4</td>
<td>( \pm 2\pi/3 )</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>midpoint of opposite edges</td>
<td>3</td>
<td>( 2\pi/2 )</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

45.2. **Proposition.** The group \( G \) of symmetries of the tetrahedron is isomorphic to \( A_4 \), the subgroup of even permutations in \( S_4 \). Furthermore, there are four conjugacy classes in \( G \) (corresponding to the four conjugacy classes in \( A_4 \)), which consist of: \{e\}, \{2\pi/2-rotations\}, \{+2\pi/3-rotations\}, and \{-2\pi/3-rotations\}.

**Proof.** Symmetries of the tetrahedron permute its four vertices. Check that all such permutations are even.

To see that these classes are the conjugacy classes, you can argue directly. For instance, let \( g \) be a \(+1/3\) rotation, around some axis \( VC \) (where \( V \) is a vertex), and let \( g' \) be another one around some axis \( V'C' \). Let \( h \) be a rotation of the tetrahedron that takes \( VC \) to \( V'C' \). Then \( g' = hgh^{-1} \); to see this, note that both \( V' \) and \( C' \) will be fixed points of \( g' \), e.g., \( g'(V') = hgh^{-1}(V') = hg(V) = h(V) = V' \).

45.3. **Symmetries of the cube and octohedron.** Here are the symmetries of the cube.

<table>
<thead>
<tr>
<th>axis of symmetry</th>
<th>number of axes</th>
<th>angle of rotation</th>
<th>number of symmetries</th>
<th>order of symmetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>vertex/ opposite vertex (diagonal)</td>
<td>4</td>
<td>( \pm 2\pi/3 )</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>midpoints of opposite edges</td>
<td>6</td>
<td>( 2\pi/2 )</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>centroids of opposite faces</td>
<td>3</td>
<td>( \pm 2\pi/4 )</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

45.4. **Proposition.** The group of symmetries of the cube is isomorphic to \( S_4 \), and the above classes are precisely the conjugacy classes.
Proof. Let $X$ be the set consisting of the four diagonals of the cube. Symmetries of the cube permute its four diagonals, so we get a homomorphism $\phi: G \to \text{Sym}(X) \approx S_4$. The claim is that this is an isomorphism. Since both groups have order 24, it is enough to show that $\phi$ is injective.

Do this the “brute force” way, by showing that $\phi$ sends every non-identity symmetry to a non-identity permutation of diagonals. Thus $\ker \phi = \{I\}$ and so $\phi$ is injective.

• Each 4-fold symmetry (around centroids of opposite faces) induces a 4-cycle on the set of diagonals.
• Each 2-fold symmetry around centroids of opposite faces (the squares of the above elements), induces a square of a 4-cycle, i.e., a product of two disjoint 2-cycles.
• Each 3-fold symmetry (around a diagonal) induces a 3-cycle on the set of diagonals.
• Each 2-fold symmetry through opposite edges switches two diagonals (namely, the ones which touch the edges through the axis), but preserve the other two. Thus it induces a 2-cycle on the set of diagonals.

This also gives the relation between conjugacy classes. □

45.5. Remark. Here is another way to show $\phi$ is injective. First show that the conjugacy classes in $G$ are as in the chart. Then note that the only possible normal subgroups of $G$ are $\{e\}$, $G$, and $N = \text{union of conjugacy classes of sizes } 8, 3, 1$.

Now do a direct computation to show that $\phi(g) \neq e$, where $g =$ any non-identity element in $N$ (e.g., a $\pi$-rotation around the centroid of opposite faces). Then neither $N$ nor $G$ can be the kernel, so $\phi$ is injective.

The octahedron is “dual” to the cube. You can get the octahedron by putting at vertex at the centroid of each face of the cube. The axes of symmetry don’t change. Here are the symmetries of the octahedron.

<table>
<thead>
<tr>
<th>axis of symmetry</th>
<th>number of axes</th>
<th>angle of rotation</th>
<th>number of symmetries</th>
<th>order of symmetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>centroids of opposite faces</td>
<td>4</td>
<td>$\pm 2\pi/3$</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>midpoints of opposite edges</td>
<td>6</td>
<td>$2\pi/3$</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>vertex/opposite vertex (diagonal)</td>
<td>3</td>
<td>$\pm 2\pi/4$</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

The symmetry group of the octahedron is $S_4$, same as the cube.

45.6. Symmetries of the dodecahedron and icosahedron. Here are the symmetries of the dodecahedron.

<table>
<thead>
<tr>
<th>axis of symmetry</th>
<th>number of axes</th>
<th>angle of rotation</th>
<th>number of symmetries</th>
</tr>
</thead>
<tbody>
<tr>
<td>vertex/ opposite vertex (diagonal)</td>
<td>10</td>
<td>$\pm 2\pi/3$</td>
<td>20</td>
</tr>
<tr>
<td>midpoints of opposite edges</td>
<td>15</td>
<td>$2\pi/2$</td>
<td>15</td>
</tr>
<tr>
<td>centroids of opposite faces</td>
<td>6</td>
<td>$\pm 2\pi(1/5)$</td>
<td>12</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

45.7. Proposition. The group of symmetries of the dodecahedron is isomorphic to $A_5$, the subgroup of even permutations in $S_5$. The classes in the chart are the conjugacy classes.
Proof. Find five “things” in the dodecahedron that the symmetry group permutes. For instance, you can group the 30 edges into five subsets of 6 edges each. The six edges in one of these subsets are all either parallel or perpendicular to each other. It needs a bit of work to visualize these. Write $X = \{U_1, \ldots, U_5\}$ for the set whose elements are these five subsets.

This produces a homomorphism $\phi: G \rightarrow \text{Sym}(X) \approx S_5$. The claim is (i) $\phi$ is injective, so $G$ is isomorphic to a subgroup of $S_5$, and (ii) $\phi(G) = A_5$. Again, we do this by brute force.

- Each vertex is incident to three edges, which are elements of three distinct points of $X$. A 3-fold symmetry (around axis through opposite vertices) must cyclically permute these three elements, while fixing the other two. Thus it induces a 3-cycle in $S_5$.
- Each face contains one edge from each of the five elements of $X$. Therefore, any order 5 symmetry (around axis through opposite centroids) induces a 5-cycle in $S_5$.
- Each 2-fold symmetry (around axis through midpoints of opposite edges) fixes exactly one element of $X$ (namely, that containing that the axis passes through). So it induces a product of disjoint 2-cycles.

Thus, every non-identity element of $G$ goes to a non-identity even permutation in $S_5$. \hfill $\square$

Since the icosahedron is dual to the dodecahedron, the symmetry group is the same. Here are the symmetries of the icosahedron.

<table>
<thead>
<tr>
<th>axis of symmetry</th>
<th>number of axes</th>
<th>angle of rotation</th>
<th>number of symmetries</th>
</tr>
</thead>
<tbody>
<tr>
<td>centroids of opposite faces</td>
<td>10</td>
<td>$\pm 2\pi/3$</td>
<td>20</td>
</tr>
<tr>
<td>midpoints of opposite faces</td>
<td>15</td>
<td>$2\pi/2$</td>
<td>15</td>
</tr>
<tr>
<td>vertex/opposite vertex (diagonal)</td>
<td>6</td>
<td>$\pm 2\pi(1/5)$</td>
<td>12</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

46. Classification of finite subgroups of $SO(2)$ and $O(2)$

Recall $SO(2) = \{ A \in GL_2(\mathbb{R}) \mid AA^\top = I = A^\top A, \det A = 1 \} = \{ R_\theta \mid \theta \in \mathbb{R} \}$.

46.1. Theorem. A complete list of finite subgroups of $SO(2)$ is given by

$$C_n := \{ R_{2\pi k/n} \mid k \in \mathbb{Z} \}, \quad n \geq 1.$$ 

The subgroup $C_n$ is cyclic of order $n$.

Proof. Step 1. It is clear that these $C_n$ are finite subgroups. In fact, they are cyclic subgroups: $C_n = \langle R_{2\pi/n} \rangle$, and in fact $C_n = \langle R_{2\pi(k/n)} \rangle$ whenever $\gcd(k, n) = 1$ (because there exists $\ell$ such that $k\ell \equiv 1 \mod n$.)

Step 2. An element $R_{2\pi x} \in SO(2)$ has finite order if and only if $x$ is a rational number. This is straightforward: if $R_{2\pi x}^b = I$ for some $b > 1$, then $2\pi x b \in 2\pi \mathbb{Z}$, so $a := bx \in \mathbb{Z}$ and thus $x = a/b$. Conversely, if $x = a/b \in \mathbb{Q}$ then clearly $R_{2\pi(x/a)}^b = I$.

Step 3. This shows that every finite cyclic subgroup of $SO(2)$ is one of the $C_n$s: if $H = \langle R_{2\pi x} \rangle$ is finite, then $x \in \mathbb{Q}$, so write $x = k/n$ in lowest terms (i.e., $\gcd(k, n) = 1$). Then $H = C_n$.

Step 4. Let $H \subseteq SO(2)$ be a finite subgroup. Write the elements as $R_{2\pi(a_1/b_1)}, \ldots, R_{2\pi(a_r/b_r)}$ for rational numbers $a_k/b_k \in \mathbb{Q}$. Let $N := b_1 \cdots b_r$. Then each of these elements is a power of $R_{2\pi(1/N)}$:

$$R_{2\pi k/N} = R_{2\pi(a_k/b_k)},$$

and so $H \subseteq \langle R_{2\pi(1/N)} \rangle$. But we know that every subgroup of a cyclic group is cyclic, so $H$ is cyclic, and therefore equal to some $C_n$ by Step 3. \hfill $\square$
47. Classification of finite subgroups of $SO(3)$

We are going to sketch the classification of finite subgroups of $SO(3)$. Note that if $H \leq SO(3)$ is a finite subgroup, so is any conjugate $gHg^{-1}$ for any $g \in SO(3)$. Thus, we will really classify finite subgroups up to conjugacy.

47.1. Theorem. Every finite subgroup of $SO(3)$ is conjugate to exactly one of the following list.

(1) The trivial group.
(2) The cyclic group $\mathbb{Z}/m$ of order $m \geq 2$, as a subgroup of rotations around a single axis through angles which are multiples of $2\pi/m$.
(3) The dihedral group $D_m$ of order $2m$ with $m \geq 2$, as the group of symmetries of a regular $m$-gon.
(4) The symmetry group of a tetrahedron (isomorphic to $A_4$).
(5) The symmetry group of a cube/octahedron (isomorphic to $S_4$).
(6) The symmetry group of a dodecahedron/icosahedron (isomorphic to $A_5$).

Note: the case of $D_2$ is a bit anomalous: it is not really the group of symmetries of the “regular 2-gon”. Rather, it is a subgroup isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, consisting of the identity map together with $\pi$-rotations around each of the three perpendicular axes.

Let $G \leq SO(3)$ be a subgroup. A pole is a unit vector $u$ in $\mathbb{R}^3$ such that $gu = u$ for some $g \in G \setminus \{e\}$. Note that poles come in pairs $\pm u$, and point along the axis of rotation of $g$. Let $X$ be the set of poles.

Every non-identity element of $G$ is associated to two poles (though a pole can be associated to many elements in $G$). Thus $X$ is a finite set.

47.2. Example. In each of the examples in the list, we can identify the poles.

- For $C_m$, there are only two poles, which lie on the axis of rotation.
- For $D_m$, there are $2 + 2m$ poles: 2 for the rotations of the $m$-gon, and $2m$ for each of the $m$ “flips” of the $m$-gon.
- For symmetries of regular polyhedra, the poles are in the direction of: vertices, midpoints of edges, centroids of faces.
- The trivial subgroup has no poles.

The group $G$ acts on the set $X$ of poles: if $u$ is a pole with $gu = u$, then for any $h \in G$ we have

$$(hgh^{-1})hu = hgu = hu.$$ 

That is, $hu$ is a pole associated with $hgh^{-1}$.

The action $G \acts X$ on the set of poles will be crucial for the classification of finite subgroups $G$. We are going to think carefully about orbits and stabilizers for this action. Let $n = |G|$.

(a) Write $O_1, \ldots, O_r \subseteq X$ for the distinct orbits of the action of $G$ on $X$, and assume that we list them in descending order of size: $|O_1| \geq \cdots \geq |O_r|$. Remember that the orbits partition $X$, so $X = O_1 \cup \cdots \cup O_r$ and $O_i \cap O_j = \emptyset$ if $i \neq j$.

(b) By the orbit stabilizer theorem, $|O_k| = |G|/|\text{Stab}(x)|$ for any $x \in O_k$. So $|O_k| = n/c_k$ where $c_k = |\text{Stab}(x)|$ for any $x \in O_k$.

(c) As a consequence,

$$2 \leq c_1 \leq \cdots \leq c_r.$$ 

Note that each $c_k \geq 2$ by definition: a pole $x \in X$ must have the property that it is fixed by some non-identity element in $G$, so $\text{Stab}(x) \neq \{e\}$.

(d) For any unit vector $u$, the subgroup $T_u := \{ A \in SO(3) \mid Au = u \}$ is isomorphic to $SO(2)$ (because $Au = u$ implies that $A$ is a rotation around the axis of $u$). Thus if $x \in X$ is a pole, then $\text{Stab}(x) \leq T_u \approx SO(2)$, and therefore $\text{Stab}(x)$ is always a cyclic group. I.e.,

$$x \in O_k \quad \implies \quad \text{Stab}(x) \approx \mathbb{Z}/c_k.$$
We also know that $\text{Stab}(x) = \text{Stab}(-x)$, since a rotation that fixes $x$ also fixes $-x$.

(e) For each pole $x$ we have a subset

$$R_x := \text{Stab}(x) \setminus \{e\} \subset G \setminus \{e\},$$

the set of “non-identity rotations around the axis through $x$ in $G$”. Since every non-identity element of $G$ fixes some pole, we have that

$$G \setminus \{e\} = \bigcup_{x \in X} R_x$$

On the other hand, the only unit vectors fixed by elements of $R_x$ are $\pm x$, so

$$R_x = R_{-x}, \quad \text{and} \quad R_{x'} \cap R_x = \varnothing, \quad \text{if } x' \neq \pm x.$$

Now we put this information together. Fact (e) says that $G \setminus \{e\}$ is partitioned into the subsets $R_x$, which are pairwise disjoint if we only choose one for each antipodal pair of poles. Thus,

$$n - 1 = |G \setminus \{e\}| = \sum_{\{\pm x\} \subseteq X} |R_x| = \frac{1}{2} \sum_{x \in X} |R_x|.$$

The size of $R_x$ is determined by the orbit of $x$, i.e., if $x \in O_k$ then $|R_x| = c_k - 1$, so if we group things together by orbit using (a) we get

$$n - 1 = \frac{1}{2} \sum_{x \in X} |R_x| = \frac{1}{2} \sum_{k=1}^{r} \sum_{x \in O_k} |R_x| = \frac{1}{2} \sum_{k=1}^{r} |O_k| (c_k - 1) = \frac{1}{2} \sum_{k=1}^{r} \frac{n}{c_k} (c_k - 1),$$

using $|O_k| = n/c_k$ by (b).

Dividing through by $n/2$, we obtain the key equation

$$2 - \frac{2}{n} = \sum_{k=1}^{r} \left(1 - \frac{1}{c_k}\right),$$

which we can rewrite as

$$(r - 2) + \frac{2}{n} = \frac{1}{c_1} + \cdots + \frac{1}{c_r},$$

where

$$r \geq 0, \quad n \geq 1, \quad 2 \leq c_1 \leq \cdots \leq c_r, \quad c_k | n,$$

with $r, n, c_k \in \mathbb{Z}$, using (b) and (c).

**Claim.** The only solutions to the key equation are:

| Case 1 | $n = 1$ | $r = 0$ | $0$ poles |
| Case 2 | any $n \geq 2$ | $r = 2$ | $(c_1, c_2) = (n, n)$ | $1+1$ poles |
| Case 3 | any even $n \geq 2$ | $r = 3$ | $(c_1, c_2, c_3) = (2, 2, n/2)$ | $(n/2) + (n/2) + 2$ poles |
| Case 4 | $n = 12$ | $r = 3$ | $(c_1, c_2, c_3) = (2, 3, 3)$ | $6+4+4$ poles |
| Case 5 | $n = 24$ | $r = 3$ | $(c_1, c_2, c_3) = (2, 3, 4)$ | $12+8+6$ poles |
| Case 6 | $n = 60$ | $r = 3$ | $(c_1, c_2, c_3) = (2, 3, 5)$ | $30+20+12$ poles |

**Proof of claim.** We prove that these are the only possibilities.

- First note that the key equation gives

  $$r - 2 < (r - 2) + \frac{2}{n} = \frac{1}{c_1} + \cdots + \frac{1}{c_r} \leq \frac{r}{2},$$

  since $n$ is positive and each $c_k \geq 2$. Thus $\frac{r}{2} > r - 2$, which is the same as $r < 4$. Thus $r \in \{0, 1, 2, 3\}$.
- (Case 1.) If $r = 0$ then the key equation is just $-2 + \frac{2}{n} = 0$, so $n = 1$. The group is trivial, and there are no poles.
• $r = 1$ is impossible: in this case the key equation is $-1 + 2/n = 1/c_1$ with $c_1 \in (0, 1/2]$, which is not possible since $n \in \mathbb{N}$.

• (Case 2.) If $r = 2$, the key equation is $2/n = 1/c_1 + 1/c_2$, so $2 = n/c_1 + n/c_2$ where $n_1/c_1$ and $n_2/c_2$ are positive integers. Thus $n = c_1 = c_2$ with $n \geq 2$.

• If $r = 3$, the key equation gives

$$\frac{1 + 2}{n} = \frac{1}{c_1} + \frac{1}{c_2} + \frac{1}{c_3}.$$  

The LHS > 1, but each $1/c_k \in \{1/2, 1/3, 1/4, \ldots \}$. There are not many ways to get a number greater than 1 as a sum of three fractions from this set. For instance, since $1/2 \geq 1/c_1 \geq 1/c_2 \geq 1/c_3$ we must have $c_1 = 2$.

• If $r = 3$ and $c_1 = 2$, the key equation gives $1 + 2/n = 1/2 + 1/c_2 + 1/c_3$. Since the LHS is $> 1$, we cannot have $c_2 \geq 4$. Thus $c_2 \in \{2, 3\}$.

• (Case 3.) If $r = 3$ and $c_1 = c_2 = 2$, then the key equation gives $1 + 2/n = 1 + 1/c_3$, so $c_3 = n/2$ with $n$ even.

• (Cases 4, 5, 6.) If $r = 3$, $c_1 = 2$, and $c_2 = 3$, then we have $1 + 2/n = 1/2 + 1/3 + 1/c_3$. We know that $c_3 \geq 3$, and since the LHS > 1 we must have $c_3 \leq 5$. Check that the three remaining possibilities $c_3 \in \{3, 4, 5\}$ work: $(c_3, n) = (3, 12), (c_3, n) = (4, 24), (c_3, n) = (5, 60)$.

These cases are exactly compatible with the symmetry subgroups of $SO(3)$ that we have already listed, so all of these possibilities are realized by finite subgroups of $SO(3)$.

It remains to show that, in each case, the items listed in the statement of the theorem is the only possibility. That is, we need to show that there isn’t some other finite subgroup we hadn’t thought of which also has the same numbers and sizes of orbits of poles as one of the things on this list.

First a note: poles come in antipodal pairs $\{\pm x\}$. These two do not need to be in the same orbit (e.g., in the cyclic group or tetrahedron cases). However, if they are in different orbits, those two orbits must have the same size (since $\text{Stab}(x) = \text{Stab}(-x)$).

• Case 1 is clear: this must be the trivial subgroup.

• For case 2, $|X| = 2$ so $X = \{\pm x\}$, and all elements of $G$ are rotations about this one axis. Thus $G$ must be a cyclic group.

• For case 3, we have that $G$ contains a cyclic group $\langle r \rangle$ of order $m = n/2$ and index 2, which is the stabilizer of an element $x \in O_3$. Since $O_3$ is the only orbit of size 2, we must have $O_3 = \{\pm x\}$.

An element $g \in G \setminus \langle r \rangle$ does not fix $x$ or $-x$. Since $\{\pm x\}$ is a single orbit, we must have that $g(x) = -x$ and $g(-x) = x$. Thus, each such $g$ is an angle $\pi$-rotation around and axis perpendicular to $\pm x$. The poles of $g$ will lie in either $O_1$ or $O_2$, which must lie on the plane perpendicular to $\pm x$.

No non-identity element of the subgroup $\langle r \rangle$ can fix any element of either $O_1$ or $O_2$. Thus, if $y \in O_1$ then $y, r(y), \ldots, r^{m-1}(y)$ are distinct elements of $O_1$, so $O_1 = \{y, r(y), r^2(y), \ldots, r^{m-1}(y)\}$ are the points of a regular $m$-gon, and similarly for $O_2$. Thus $G$ is the symmetry group of either of these regular $m$-gons, i.e., $G \cong D_m$.

• For case 4, consider $O_3$ which has size 4 (the same argument will work with $O_2$). Consider an arbitrary element $x \in O_3$, and consider $\text{Stab}(x) = \langle g \rangle$, a cyclic subgroup of order 3. Because $O_3$ is a $G$-orbit, the subgroup $\langle g \rangle$ acts on $O_3$. Since $\text{order}(g) = 3$, the orbits of $\langle g \rangle$ have size either 1 or 3. We know that $g(x) = x$, and that there are only two elements of $X$ fixed by $g$, namely $\pm x$. Thus we must have

$$O_3 = \{x, y, g(y), g^2(y)\},$$

where $g$ is any other element of $O_3$. (And note that $-x \notin O_3$.)

Because $g$ preserves dot product of vectors, it preserves distances, so

$$|x - y| = |x - g(y)| = |x - g^2(y)|.$$
Thus, $x$ is equidistant to the other three points in $O_3$. But $x$ was an arbitrary element of $O_3$, so all points in $O_3$ are equidistant, i.e., it is a regular tetrahedron, and $G$ acts as symmetries of it.

(Exercise: show that $x \cdot y = -1/3$.)

• Cases 5 and 6 are similar: the points in $O_2$ and $O_3$ form regular polyhedra. These cases are a little more involved, because we can’t simply check that all points in the orbit are pairwise equidistant (because they aren’t).

(For more detail, including about the remaining cases, see e.g., Hannah Mark, “Classifying finite subgroups of $SO(3)$”, http://homepages.math.uic.edu/~kauffman/FiniteRot.pdf or the discussion and exercises in §11.3 of Goodman’s textbook.)