LECTURE NOTES (PART 1), MATH 500 (FALL 2022)

CHARLES REZK

1. Review: groups

Given a binary operation $(x, y) \mapsto x \cdot y$ on a set G, we have the following properties it may or may not satisfy. **M 22 Aug**

(1) *associativity:* $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in G$.
(2) *identity:* there is an element $e \in G$ such that $e \cdot x = x = x \cdot e$ for all $x \in X$.
(3) *inverse:* for all $x \in G$, there exists an element $x^{-1} \in G$ such that $x \cdot x^{-1} = e = x^{-1} \cdot x$, where e is an identity element as in (2).
(4) *commutativity:* $x \cdot y = y \cdot x$ for all $x, y \in G$.

A **group** is a pair $(G, \cdot)$, consisting of a set G and a binary product $(x, y) \mapsto x \cdot y$, satisfying (1), (2), and (3). **group**

A group is **abelian** (or **commutative**) if in addition satisfies (4). **abelian** **commutative**

A **monoid** is a pair $(G, \cdot)$ satisfying (1) and (2). A **semigroup** is a pair $(G, \cdot)$ satisfying (1). **monoid** **semigroup**

Here are some remarks about the definition of group.

- It is a consequence of the definition of group (or monoid) that there is only one element $e \in G$ satisfying (2). Likewise, it is a consequence of the definition of group that for each $x \in G$ there is only one element $x^{-1} \in G$ satisfying (3).
- Many symbols can be used for the binary operation, instead of $\cdot$, such as $+$, $*$, $\bullet$, $\circ$, etc., or no symbol at all. What I'll use will depend on context, and most often I will use no symbol.
- Another standard symbol for e is 1.
- For $g \in G$ and $n \in \mathbb{Z}$ we define g^n in the obvious way for the "nth power" of g. This satisfies
$$g^m g^n = g^{m+n}, \qquad (g^m)^n = g^{mn}, \qquad g^0 = e,$$
and g^{-1} is in fact the inverse of g.
- The inverse of a product of elements in a group (or monoid) is a product of inverses, but in the opposite order: $(ab)^{-1} = b^{-1}a^{-1}$.
- An **additive group** is an abelian group in which the binary operation is written with "+". By convention, you only use "+" if the group is abelian, and in this 0 is the identity element, $-x$ is inverse of x, and nx is the nth power for $n \in \mathbb{Z}$. **additive group**
- The **order** $|G|$ of a group is just the cardinality of its set. **order**

2. Review: Examples of groups

Here are some important examples.

- *finite cyclic group:* $C_n := \{e, a, \dots, a^{n-1}\}$, with $a^i a^j = a^{i+j}$ if $i + j < n$ and $a^i a^j = a^{i+j-n}$ if $i + j \geq n$. DF write Z_n for this.
- *integers modulo n:* $\mathbb{Z}/n :=$ congruence classes modulo n. This is an additive group.
- *Dihedral group of order $2n$:* D_{2n} for $n \geq 3$ is the group of symmetries of a regular n-gon, viewed as an object in 3-space.

Date: January 27, 2023.

A standard presentation uses the regular n-gon in the xy-plane, with center at the origin and a vertex at $(1,0,0)$. Let $r \in D_{2n}$ be the rotation around the z-axis by angle $2\pi/n$, and $s \in D_{2n}$ be the rotation around the x-axis by angle π. Then one can check that

$$r^n = s^2 = e, \qquad rs = sr^{-1},$$

and that D_{2n} has $2n$ elements, which can be exhaustively listed as: $e, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}$.

- *Symmetric group on a set.* If Ω is a set, $\mathrm{Sym}(\Omega)$ (or S_Ω) is the group of permutations of the set, i.e., the set of bijections $\sigma\colon \Omega \to \Omega$, with group structure is defined by composition.

  We write $S_n := \mathrm{Sym}(\{1,\ldots,n\}$. Note that $|S_n| = n!$.

  We have the following *two-line notation* for elements in S_n:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \qquad \Longleftrightarrow \qquad \sigma(k) = a_k, \quad k \in \{1,\ldots,n\}.$$

  A *cycle* in S_n is an element written as

$$\sigma = (a_1\ a_2\ \cdots\ a_k),$$

  where $a_1,\ldots,a_k \in \{1,\ldots,n\}$ are pairwise distinct, and defined by

$$\begin{aligned} \sigma(a_i) &:= a_{i+1}, && \text{if } 1 \le i < k, \\ \sigma(a_k) &:= a_1, \\ \sigma(x) &:= x, && \text{if } x \notin \{a_1,\ldots,a_k\}. \end{aligned}$$

- *General linear group.* For any field F, we have the group $GL_n(F)$ of $n \times n$ invertible matrices, with product matrix multiplication.
- *Quaternion group.* $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, with group structure determined by:

$$-1 \cdot x = -x \ \ \forall x \in Q_8, \quad (-1)^2 = 1, \quad , ij = k, \quad jk = i, \quad ki = j.$$

3. Review: Subgroups

A **subgroup** of a group G is a subset $H \subseteq G$ such that

subgroup

(1) H is non-empty,
(2) if $x \in H$ then $x^{-1} \in H$,
(3) if $x, y \in H$ then $xy \in H$.

Note: you can replace (1) with

(1') $e \in H$,

without changing the meaning.

Here are some examples.

- *Special linear group.* The subgroup $SL_n(F) \le GL_n(F)$ of matrices A with $\det A = 1$.
- *Alternating group.* The subgroup $A_n \le S_n$ consisting of even permutations.

If H is a subgroup, then together with the the binary operation defined by that of G it is a group.

We write "$H \le G$" to mean "H is a subgroup of G".

If $S \subseteq G$ is a subset, let

$$\langle S \rangle := \bigcap_{\substack{H \le G \\ S \subseteq H}} H.$$

This is a subgroup of G, called the **subgroup generated by** S. (Note: $\langle \varnothing \rangle = \{e\}$.)

subgroup generated by S

Notation: if $S = \{a_1,\ldots,a_k\}$, we write $\langle a_1,\ldots,a_k \rangle = \langle S \rangle$.

A **word in** S is any element $g \in G$ which can be written as

word in S

$$g = g_1 \cdots g_k, \qquad k \ge 0, \quad \text{either } g_i \in S \text{ or } g_i^{-1} \in S \text{ for all } i = 1,\ldots,k.$$

Note: when $k = 0$ then by convention this corresponds to $g = e$.

Proposition. *For $S \subseteq G$, the set $\langle S \rangle$ is precisely the set of words in S.*

A **cyclic group** G is a group such that there exists $a \in G$ with $G = \langle a \rangle$. **cyclic group**

We write C_n (or Z_n) for the cyclic group of order n, where $n \in \mathbb{Z}_{>0}$ or $n = \infty$. These are written multiplicatively, in terms of a generator $a \in C_n$. Cyclic groups are always abelian.

We also have $\mathbb{Z}/n$ (for $n \in \mathbb{Z}_{>0}$) and $\mathbb{Z}$, which are additive cyclic groups.

The **order** of an element $g \in G$ is the order of the subgroup it generates. I'll write **order**

$$|g| := |\langle g \rangle| \in \mathbb{Z}_{>0} \cup \{\infty\}.$$

The **lattice of subgroups** of G is a partially ordered set, whose elements are subgroups $H \leq G$, **lattice of subgroups** ordered by the subset relation.

It is important to know the lattices of subgroups of cyclic subgroups.

4. Review: Cosets

Fix a subgroup $H \leq G$.

- A **left coset**[1] for H is any subset of the form **left coset**

  $$xH := \{\, xh \mid h \in H \,\}.$$

  The collection of left cosets partitions G into pairwise disjoint subsets. Thus xH is the unique left coset for H which contains x. For $x, y \in G$ we have

  $$xH = yH \qquad \text{iff} \qquad \exists h \in H,\ y = xh.$$

  We write $G/H := \{\, xH \mid x \in G \,\}$ for the set of left cosets.
- a **right coset** for H is any subset of the form **right coset**

  $$Hx := \{\, hx \mid h \in H \,\}.$$

  The collection of right cosets partitions G into pairwise disjoint subsets. Thus Hx is the unique right coset for H which contains x. For $x, y \in G$ we have

  $$Hx = yH \qquad \text{iff} \qquad \exists h \in H,\ y = hx.$$

  We write $H\backslash G := \{\, xH \mid x \in G \,\}$ for the set of right cosets.

Proposition. *Let $H \leq G$.*

1. *$eH = H$ as set.*
2. *For any $x, y \in G$ there is a bijection $xH \to yH$, defined by $xh \mapsto yh$.*
3. *For any $x \in G$ there is a bijection $xH \to Hx^{-1}$, defined by $xh \mapsto h^{-1}x^{-1}$.*
4. *There is a bijection $G/H \to H\backslash G$, defined by $xH \mapsto Hx^{-1}$.*

The **index** of H in G is denoted $|G : H|$ and defined by **index**

$$|G : H| := |G/H|,$$

the cardinality of left cosets of H, which is also the cardinality of right cosets of H. Note that this can be finite even if H and G are infinite.

The following is most useful when all cardinalities are finite.

Proposition. *For $H \leq G$ we have $|G| = |G : H| \cdot |H|$.*

More generally, if $K \leq H \leq G$ we have $|G : K| = |G : H| \cdot |H : K|$.

Proof. Right cosets of H partition G into pairwise disjoint subsets, each of which have the same cardinality. □

This implies **Lagrange's Theorem**: if G is a finite group and $H \leq G$, then $|H|$ and $|G : H|$ divide $|G|$. In particular, $|g|$ divides $|G|$ for all $g \in G$. **Lagrange's Theorem**

As a consequence, if $|G|$ is prime then G is cyclic.

[1] Apparently, I've been getting this exactly backwards in the videos.

5. Review: Homomorphisms and isomorphsims of groups

A **homomorphism of groups** is a function $\phi\colon G \to H$ between two groups such that

homomorphism of groups

$$\phi(xy) = \phi(x)\phi(y) \qquad \forall x, y \in G.$$

Exercise. If ϕ is a homomorphism of groups, then $\phi(e_G) = e_H$ and $\phi(x^{-1}) = \phi(x)^{-1}$.

Example. The determinant homomorphism $\det\colon GL_n(F) \to F^\times$, where $F^\times = F \smallsetminus \{0\}$ equipped with multiplication.

Example. If $H \leq G$ is a subgroup, the inclusion homomorphism $\iota\colon H \to G$ sends $\iota(h) = h$.

An **isomorphism of groups** is a homomorphism which is also a bijection.

isomorphism of groups

Note: if $\phi\colon G \to H$ is an isomorphism, then its inverse function $\phi^{-1}\colon H \to G$ is also an isomorphism.

Two groups are **isomorphic groups** if there exists an isomorphism between them. This defines an equivalence relation on the collection of groups.

isomorphic groups

Example. S_3 and D_6 are isomorphic. One such isomorphism $\phi\colon D_6 \to S_3$ is determined by

$$\phi(r) = (1\ 2\ 3), \qquad \phi(s) = (1\ 2).$$

The kernel $\mathrm{Ker}(\phi)$ of a homomorphism $G \to H$ is the subset

$$\mathrm{Ker}(\phi) := \{\, g \in G \mid \phi(g) = e \,\}.$$

Proposition. *A homomorphism $\phi\colon G \to H$ is an injective function iff $\mathrm{Ker}(\phi) = \{e\}$.*

Proof. $\phi(x) = \phi(y)$ iff $xy^{-1} \in \mathrm{Ker}(\phi)$. □

6. Review: Quotient groups

A subgroup $H \leq G$ is **normal** if $xHx^{-1} = H$ for all $x \in G$, where $xHx^{-1} := \{\, xhx^{-1} \mid h \in H \,\}$. We write "$H \trianglelefteq G$" for "$H$ is a normal subgroup of G".

normal

Warning: although "$\leq$" is a transitive relation on subgroups, "$\trianglelefteq$" is not transitive.

Proposition. *If $\phi\colon G \to H$ is a homomorphism of groups, then $N := \mathrm{Ker}(\phi)$ is a normal subgroup of G.*

Proposition. *For $H \leq G$, we have $H \trianglelefteq G$ iff $xH = Hx$ for all $x \in G$ (i.e., iff left and right cosets are the same things).*

If $H \trianglelefteq G$, then define a binary operation on G/H by

$$xH \cdot yH := xyH.$$

This operation is well-defined exactly because H is normal in G. With this structure G/H is a group, called the **quotient group** of G by H. There is a surjective homomorphism

quotient group

$$\pi\colon G \to G/H, \qquad \pi(x) := xH,$$

called the **quotient homomorphism**. Note that $\mathrm{Ker}(\pi) = H$

quotient homomorphism

Example. Given $n \geq 1$ let $n\mathbb{Z} := \{\, nx \mid x \in \mathbb{Z} \,\}$, a normal subgroup of the additive group $\mathbb{Z}$. The quotient group $\mathbb{Z}/n\mathbb{Z}$ is precisely the set of congruence classes modulo n, equipped with addition of congruence classes.

Proposition. *A subgroup $H \leq G$ is normal iff it is the kernel of some homomorphism.*

7. First isomorphism theorem

W 24 Aug

Quotient groups come with a "recipe" for describing homomorphisms *from* them. I'll call this the "homomorphism theorem".

Theorem (Homomorphism theorem)**.** *Let $N \trianglelefteq G$ be a normal subgroup, and let $\pi\colon G \to G/N$ be the quotient homomorphism. If $\phi\colon G \to H$ is a homomorphism such that $\phi(N) = \{e\}$, then there exists a unique homomorphism $\psi\colon G/N \to H$ such that $\psi \circ \pi = \phi$.*

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, "\pi"'] & H \\
G/N \arrow[ur, dotted, "\psi"', "\exists!"] &
\end{tikzcd}$$

We say that "ϕ factors through the quotient G/N when $\phi(N) = \{e\}$".

Proof. Existence. Given ϕ, we define ψ by the rule $\psi(gN) := \phi(g)$. Since this rule depends on the element g on G, we need to check that it only depends on the equivalence class of G. Thus, if $gN = g'N$, we must show that $\phi(g) = \phi(g')$. In this case, $g' = gn$ for some $n \in N$, so $\phi(g') = \phi(gn) = \phi(g)\phi(n) = \phi(g)e = \phi(g)$ as desired.

It is straightforward to check that ψ is a homomorphism: $\psi(gNg'N) = \psi(gg'N) = \phi(gg') = \phi(g)\phi(g') = \psi(gN)\psi(g'N)$, and that $\psi \circ \pi = \phi$: $\psi(\pi(g)) = \psi(gN) = \phi(g)$ by definition.

Existence. This is immediate from the fact that π is surjective. I.e., if $\psi \circ \pi = \psi' \circ \pi$, then $\psi = \psi'$. □

We can formulate this in an equivalent way.

Corollary. *Let $N \trianglelefteq G$, with quotient homomorphism $\pi\colon G \to G/N$. Then the function*

$$\mathrm{Hom}(G/N, H) \to \mathrm{Hom}(G, H), \qquad \psi \mapsto \psi \circ \pi$$

is a monomorphism, whose image is the set of homorphisms $\phi\colon G \to H$ such that $\phi(N) = \{e\}$.

A consequence of this is called the "first isomorphism theorem".

Theorem (First isomorphism theorem)**.** *If $\phi\colon G \to H$ is a homomorphism, then $\operatorname{Ker}\phi \trianglelefteq G$ and we have an isomorphism $G/\operatorname{Ker}\phi \approx \phi(G)$.*

That is, the homomomorphism ϕ factors through an isomorphism $\overline{\phi}\colon G/\operatorname{Ker}\phi \xrightarrow{\sim} \phi(G)$.

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, two heads] & & H \\
& G/\operatorname{Ker}\phi \arrow[r, "\overline{\phi}", "\sim"'] & \phi(G) \arrow[u, tail]
\end{tikzcd}$$

Proof. It is easy to see that $N = \operatorname{Ker}\phi$ is normal: if $g \in \operatorname{Ker}\phi$, then $\phi(hgh^{-1}) = \phi(h)\phi(g)\phi(h)^{-1} = 1$.

The function ϕ also defines a homomorphism $\phi'\colon G \to \phi(G) \leq H$. By the homomorphism theorem, there exists a homomorphism $\psi\colon G/\operatorname{Ker}\phi \to \phi(G)$ such that $\psi \circ \pi = \phi'$. It is clear that ψ is surjective since ϕ' is, and that ψ is injective, since if $\psi(gN) = \psi(g'N)$, then $\phi(g) = \phi(g')$, whence $g^{-1}g' \in N$, and thus $gN = gg^{-1}g'N = g'N$. □

Note: the isomorphism $G/\operatorname{Ker}\phi \xrightarrow{\sim} \phi(G)$ is not mysterious: it is given *explicitly* by the formula $gN \mapsto \phi(g)$.

8. Second isomorphism theorem

Let G be a group with subgroups $A, B \leq G$. Then the intersection $A \cap B$ is also a subgroup. We can also consider the **product subset**

product subset

$$AB = \{\, ab \in G \mid a \in A,\ b \in B \,\}.$$

This is *not* generally a subgroup.

Example. Consider $G = D_6$ generated by $\{r, s\}$ with $r^3 = s^2 = (sr)^2 = 1$. Let $A = \langle s \rangle$ and $B = \langle sr \rangle$, both subgroups of order 2. Then $AB = e, s, sr, r$, which is not a subgroup since $r^2 \notin AB$.

Proposition. *If $A, B \leq G$, then AB is a subgroup of G iff $BA \subseteq AB$. When this is true, we actually have $AB = BA$.*

Proof. $\Longrightarrow$: If $AB \leq G$, then for $a \in A$ and $b \in B$, we have $a, b \in AB$ and thus $ba \in AB$, so $BA \subseteq AB$. The same idea shows that $AB \subseteq BA$, so $AB = BA$.

$\Longleftarrow$: Suppose $BA \subseteq AB$. Clearly $e \in AB$. If $a \in A$, $b \in B$, then $(ab)^{-1} = b^{-1}a^{-1} \in BA \subseteq AB$. Finally, suppose $a_1, a_2 \in A$, $b_1, b_2 \in B$. Then $b_1 a_2 = a' b'$ for some $a' \in A$, $b' \in B$, so

$$a_1 b_1 a_2 b_1 = a_1 a' b' b_2 \in AB$$

as desired. □

Given a subset $S \subseteq G$, the **normalizer** $N_G(S)$ of S in G is the set

normalizer

$$N_G(S) = \{\, g \in G \mid gSg^{-1} = S \,\}.$$

Exercise: This is a subgroup of G.

We usually consider normalizers of subgroups.

Exercise: If $H \leq G$ is a subgroup, then $H \trianglelefteq N_G(H)$.

Exercise: $N_G(H)$ is the "largest" subgroup of G that H is normal inside of.

Exercise: $N_G(H) = G$ iff $H \trianglelefteq G$.

Corollary. *If $A, B \leq G$, and if $A \leq N_G(B)$, then $AB = BA$ is a subgroup of G.*

Proof. Since $A \leq N_G(B)$ we have $aB = Ba$ for all $a \in A$, hence $AB = BA$ and thus $AB \leq G$. □

Exercise. Suppose $A, B \leq G$ (but not necessarily $AB \leq G$). Show that there is a bijection

$$\{\text{left } A \cap B\text{-cosets contained in } A\} \longleftrightarrow \{\text{left } B\text{-cosets contained in } AB\}$$

given by $x(A \cap B) \mapsto xB$. Conclude that if A, B are finite, then

$$|AB| = |B|[A : A \cap B] = |A||B|/|A \cap B|.$$

Use this to show that if $|A||B|/|A \cap B|$ does not divide $|G|$ (if finite), then neither A nor B are normal subgroups of G.

Theorem (Second ("Diamond") Isomorphism Theorem)**.** *Suppose $A, B \leq G$ and $A \leq N_G(B)$. Then:*

1. *AB is a subgroup of G,*
2. *$B \trianglelefteq AB$,*
3. *$A \cap B \trianglelefteq A$,*
4. *$A/(A \cap B) \approx AB/B$.*

$$\begin{tikzcd}
 & & & G & \\
 & & & N_G(B) \arrow[u, hook] & \\
 & AB/B & & AB \arrow[u, hook] & \\
A/A\cap B \arrow[ur, "\sim"] & & A \arrow[ur, hook] \arrow[uur, hook, bend left] & & B \arrow[ul, hook, "\trianglelefteq"'] \arrow[uul, hook, bend right, "\trianglelefteq"'] \\
 & & & A\cap B \arrow[ul, hook, "\trianglelefteq"] \arrow[ur, hook] &
\end{tikzcd}$$

Proof. (1) Immediate from the corollary.

(2) $A \leq N_G(B)$ immediately implies $B \trianglelefteq AB$.

(3) If $a \in A$ and $x \in A \cap B$, then $axa^{-1} \in A$ because A is a subgroup, and $axa^{-1} \in B$ because $a \in N_G(B)$.

(4) We have a homomorphism

$$\psi\colon A/(A\cap B) \to AB/B, \qquad x(A\cap B) \mapsto xB.$$

You can check that this is a well-defined homomorphism directly, or by applying the homomorphism theorem to

$$\begin{tikzcd}
A \arrow[r, tail, "x\mapsto x"] \arrow[d, "\pi"'] & AB \arrow[r, two heads, "x\mapsto xB"] & AB/B \\
A/A\cap B \arrow[urr, dotted, "\psi", "x(A\cap B)\mapsto xB"'] & &
\end{tikzcd}$$

since $x \in A \cap B$ implies $x \in B$ so $xB = eB$. We have:

(1) ψ is injective: $\psi(x(A\cap B)) = eB$ implies $xB = eB$, i.e., $x \in B$ whence $x \in A \cap B$ so $x(A\cap B) = e(A\cap B)$.
(2) ψ is surjective: given an element $abB \in AB/B$, with $a \in A$ and $b \in B$, we have $abB = aB$, so $\psi(a) = a$.

□

Note: an easy way to satisfy the hypothesis that $A \leq N_G(B)$ is to suppose B is a normal subgroup of G. If G is abelian, this applies to all subgroups.

9. Third isomorphism theorem

Theorem (Third isomorphism theorem). *Let H, K be normal subgroups of G, with $H \leq K$. Then:*

(1) *$K/H \trianglelefteq G/H$, and*
(2) *$(G/H)/(K/H) \approx G/K$.*

$$\begin{tikzcd}
 & G/K \arrow[r, "\sim"] & (G/H)/(G/K) \\
H \arrow[r, hook, "\trianglelefteq"] \arrow[d, equal] & G \arrow[r, two heads] \arrow[u, two heads] & G/H \arrow[u, two heads] \\
H \arrow[r, hook, "\trianglelefteq"'] & K \arrow[r, two heads] \arrow[u, hook, "\trianglelefteq"] & K/H \arrow[u, hook, "\trianglelefteq"]
\end{tikzcd}$$

Proof. (1) is straightforward: for $gH \in G/H$, $kH \in K/H$, we have $gHkH(gH)^{-1} = gkg^{-1}H \subseteq KH$.

(2) The rule $xK \mapsto (xH)\overline{K}$ (where $\overline{K} = K/H \subseteq G/H$) defines a homomorphism $\phi\colon G/K \to (G/H)/(K/H)$, as can be proved directly, or by the homomorphism theorem:

$$\begin{tikzcd}
G \arrow[r, two heads, "x\mapsto xH"] \arrow[d, two heads] & G/H \arrow[r, two heads, "xH\mapsto(xH)\overline{K}"] & (G/H)/(G/K) \\
G/K \arrow[urr, dotted, "\phi"'] & &
\end{tikzcd}$$

as the kernel of the composite of maps on the top is $\{\, x \in G \mid xH \in \overline{K} \,\} = K$. The map ϕ is in fact an isomorphism by the first isomorphism theorem. □

10. Fourth isomorphism theorem

Theorem (Fourth ("Lattice") Isomorphism Theorem)**.** *Let $N \trianglelefteq G$ be a normal subgroup. Then we have inverse bijections*

$$\{\, A \leq G \mid N \leq A \,\} \xleftrightarrow{\sim} \{\overline{A} \leq G/N\}$$

$$A \longmapsto A/N$$

$$\pi^{-1}\overline{A} \longleftarrow\!\shortmid\; \overline{A}$$

where $\pi^{-1}\overline{A} = \{\, g \in G \mid \pi(g) \in \overline{A} \,\}$. Furthermore, for $A, B \leq G$ with $N \leq A \cap B$, we have

1. *$A \leq B$ iff $A/N \leq B/N$.*
2. *If $A \leq B$ then $|B : A| = |B/N : A/N|$.*
3. *$(A \cap B)/N = (A/N) \cap (B/N)$.*
4. *$A \trianglelefteq G$ iff $A/N \trianglelefteq G/N$.*

Proof. It is clear that both functions are well-defined: $A \leq G$ implies $A/N \leq G/N$, and $\overline{A} \leq G/N$ implies $\pi^{-1}\overline{A} \leq G$ and furthermore $N \subseteq \pi^{-1}\overline{A}$ since $n \in N$ implies $\pi(n) = nN = eN \in \overline{A}$.

It is straightforward to verify that these functions are inverse to each other:

- $A \mapsto A/N \mapsto \pi^{-1}(A/N)$. We have

$$\pi^{-1}(A/N) = \{\, x \in G \mid \pi(x) \in A/N \,\} = \{\, x \in G \mid xN \in A/N \,\} = \{\, x \in G \mid x \in A \,\} = A.$$

- $\overline{A} \mapsto \pi^{-1}\overline{A} \mapsto (\pi^{-1}\overline{A})/N$. We have

$$\begin{aligned}(\pi^{-1}\overline{A})/N &= \{\, xN \in G/N \mid x \in \pi^{-1}\overline{A} \,\} = \{\, xN \in G/N \mid \pi(x) \in \overline{A} \,\} \\ &= \{\, xN \in G/N \mid xN \in \overline{A} \,\} = \overline{A}.\end{aligned}$$

(1) Straightforward.

(2) This is a statement about cardinalities, but it follows from the existence of a bijection

$$B/A \xrightarrow{\sim} (B/N)/(A/N), \qquad xA \mapsto (xN)\overline{A}, \quad \overline{A} = A/N$$

between sets of left cosets. (This is similar to one part of the 3rd isomorphism theorem, but here we do not know that B/A or $(B/N)/(A/N)$ are groups.) We check this explicitly:

- *Surjective.* If $(xN)\overline{A} \in (B/N)/(A/N)$, then $x \in B$, and clearly $xA \mapsto (xN)\overline{A}$.
- *Injective.* If $xA, yA \in B/A$ such that $(xN)\overline{A} = (yN)\overline{A}$, then $(xN)(yN)^{-1} \in \overline{A}$, i.e., $xy^{-1}N \in A/N$, whence $xy^{-1} \in A$, so $xA = yA$.

(3) Straightforward.

(4) Straightforward.

□

11. Free group: definition

F 26 Aug

free group

Given a set S, we will constuct the **free group** on S, which will consist of a group F and a function $\iota\colon S \to F$ such that for every group G and function $\phi\colon S \to G$ there exists a unique homomorphism $\Phi\colon F \to G$ such that the diagram

$$\begin{tikzcd}
S \arrow[r, "\iota"] \arrow[dr, "\phi"'] & F \arrow[d, dotted, "\Phi"] \\
 & G
\end{tikzcd}$$

commutes. As a consequence of the construction, the map ι will be injective.

As a consequence of this definition, the free group on S is *unique up to isomorphism*: if F and F' are both free groups on S, then they are isomorphic.

To see this, we use the universal property to construct homomorphisms in either direction. For instance, suppose (F, ι) and (F', ι') are both free groups on S. Then there exists a unique group homomorphism $\phi\colon F \to F'$ such that $\phi \circ \iota = \iota'$:

$$\begin{tikzcd}
 & F \arrow[dd, "\phi"] \\
S \arrow[ur, "\iota"] \arrow[dr, "\iota'"'] & \\
 & F'
\end{tikzcd}$$

The same argument gives a unique homomorphism $\psi\colon F' \to F$ such that $\psi \circ \iota' = \iota$:

$$\begin{tikzcd}
 & F' \arrow[dd, "\psi"] \\
S \arrow[ur, "\iota'"] \arrow[dr, "\iota"'] & \\
 & F
\end{tikzcd}$$

Consider the composite homomorphisms $\psi \circ \phi\colon F \to F$ and $\psi \circ \phi\colon F' \to F'$. By construction we have identities

$$\psi \circ \phi \circ \iota = \psi \circ \iota' = \iota, \qquad \phi \circ \psi \circ \iota' = \phi \circ \iota = \iota'.$$

But the identity homomorphisms $\mathrm{id}_F\colon F \to F$ and $\mathrm{id}_{F'}\colon F' \to F'$ also satisfy identities like this: $\mathrm{id}_F \circ \iota = \mathrm{id}_F$, $\mathrm{id}_{F'} \circ \iota' = \mathrm{id}_{F'}$. Therefore, the uniqueness part of the universal property implies that $\psi \circ \phi = \mathrm{id}_F$ and $\phi \circ \psi = \mathrm{id}_{F'}$, so these are inverse isomorphisms.

12. Free group: construction

Refer to elements of S as **symbols**. symbols

- Choose a new set S^* which is disjoint to and in bijective correspondence with S, so that for each $s \in S$, there is a corresponding element $s^* \in S^*$.
- Refer to elements of $S \amalg S^*$ as **letters**. letters
- Extend the bijection $s \mapsto s^*$ to an involution on the set of letters, so that $(s^*)^* := s$.
- A **word** is a finite sequence $x = (x_1, \ldots, x_n)$ of letters $x_i \in S \amalg S^*$. We allow $n = 0$, and so write $()$ for the empty word. The **length** of a word $x = (x_1, \ldots, x_n)$ is $|x| := n$. word length
- A **reduced word** is a word $x = (x_1, \ldots, x_n)$ such that reduced word

  $$x_k^* \neq x_{k+1} \quad \text{for all } k = 1, \ldots, n-1.$$

  Note that the empty word and all length one words are reduced.
- Write F for the set of reduced words.
- Write $\iota\colon S \to F$ for the function $\iota(s) := (s)$.

Given reduced words $x, y \in F$, we define a new word $x \cdot y$ as follows. Suppose $|x| = m$ and $|y| = n$, and let k be the largest integer $0 \le k \le \min(m,n)$ such that

$$x^*_{m-j} = y_{j+1} \qquad \text{if} \qquad 0 \le j < k.$$

Define

$$(x_1,\dots,x_m)\cdot(y_1,\dots,y_n) := \begin{cases} (x_1,\dots,x_{m-k},y_{k+1},\dots,y_n), & \text{if } k < \min(m,n), \\ (x_1,\dots,x_{m-k}), & \text{if } k = n < m, \\ (y_{k+1},\dots,y_n), & \text{if } k = m < n, \\ (), & \text{if } k = m = n. \end{cases}$$

Observe that by construction, the word $x \cdot y$ is reduced; note that if $k < \min(m,n)$ then we must have $x^*_{m-k} \ne y_{k+1}$. Thus we have defined a binary operation

$$(x,y) \mapsto x \cdot y\colon \quad F \times F \to F.$$

Explaination. We can describe this operation as follows: *first* concatenate the two reduced words to obtain the word $(x_1,\dots,x_m,y_1,\dots,y_n)$. If $x^*_m \ne y_1$, then the new word is reduced, and is $x \cdot y$. If $x^*_m = y_1$, we remove these two letters, obtaining the word $(x_1,\dots,x_{m-1},y_2,\dots,y_n)$. If $x^*_{m-1} \ne y_2$, then the new word is reduced, and is $x \cdot y$. If not, remove these two letters. Repeat as necessary until a reduced word is obtained.

We will soon show that F equipped with this operation is a group. Note that $()$ acts as an identity element, and that $(x^*_m,\dots,x^*_1)$ acts as an inverse to $(x_1,\dots,x_m)$, so the only non-trivial part will be to prove associativity.

13. Free group: universal property

Proposition. *Let G be a group and let $\phi\colon S \to G$ be a function. Then there exists a unique function $\Phi\colon F \to G$ such that*

1. *$\Phi((s)) = \phi(s)$ for all $s \in S$, and*
2. *$\Phi(x \cdot y) = \Phi(x)\Phi(y)$ for all $x, y \in F$.*

Proof. First we prove existence. First, extend the definition of ϕ to $\phi\colon S \amalg S^* \to G$ by the rule $\phi(s^*) := \phi(s)^{-1}$. Then for a general reduced word $x = (x_1,\dots,x_n)$, define

$$\Phi(x) := \phi(x_1)\cdots\phi(x_n);$$

we let Φ of the empty word be the identity element. Property (1) is immediate. To prove (2), suppose $x = (x_1,\dots,x_m)$, $y = (y_1,\dots,y_n)$. In the case that we have $k < \min(m,n)$ such that $x^*_{m-k} \ne x_{k+1}$ and $x^*_{m-j} = x_{j+1}$ when $0 \le j < k$, then

$$x \cdot y = (x_1,\dots,x_{m-k},y_{k+1},\dots,y_n),$$

and we compute that

$$\begin{aligned}
\Phi(x)\Phi(y) &= \phi(x_1)\cdots\phi(x_m)\ \ \phi(y_1)\cdots\phi(y_n) \\
&= \phi(x_1)\cdots\phi(x_{m-k})\ \ \phi(x_{m-k+1})\cdots\phi(x_m)\ \ \phi(y_1)\cdots\phi(y_k)\ \ \phi(y_{k+1})\cdots\phi(y_n) \\
&= \phi(x_1)\cdots\phi(x_{m-k})\ \ \phi(x_{m-k+1})\cdots\phi(x_m)\ \ \phi(x_m)^{-1}\cdots\phi(x_{m-k+1})^{-1}\ \ \phi(y_{k+1})\cdots\phi(y_n) \\
&\hphantom{=}\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{using } y^*_{j+1} = x_{m-j} \text{ for } j < k) \\
&= \phi(x_1)\cdots\phi(x_{m-k})\ \ \phi(y_{k+1})\cdots\phi(y_n) \\
&= \Phi(x \cdot y).
\end{aligned}$$

The other cases of the definition of $x \cdot y$ are handled similarly.

Next we prove uniqueness. Assume Φ is a function satisfying (1) and (2). We first note that since $() \cdot () = ()$ in F, property (2) implies that $\Phi(()) = e$. Likewise, since $(s) \cdot (s^*) = () = (s^*) \cdot (s)$ for any $s \in S$, we must have that

$$\Phi((s^*)) = \Phi((s))^{-1} = \phi(s)^{-1}.$$

For a general reduced word $x = (x_1, \ldots, x_n)$, write $w_k := (x_1, \ldots, x_k)$ for $k = 1, \ldots, n$. Then $w_k = w_{k-1} \cdot (x_k)$ for each $k = 2, \ldots, n$, whence $\Phi(w_k) = \Phi(w_{k-1})\Phi((x_k))$, and thus a straighforward induction on k shows that must give $\Phi(x) = \Phi((x_1)) \cdots \Phi((x_n))$. That is, Φ must coincide with the function we constructed above. □

14. Free group: proof of associativity

Proposition. *The binary operation on reduced words makes F into a group.*

Proof. Let $G := \mathrm{Sym}(F)$, the permuation group of the set of reduced words. For each letter $a \in S \amalg S^*$, let $\lambda_a \colon F \to F$ be the function defined by left multiplication by a:

$$\lambda_a(x) := (a) \cdot x,$$

that is,

$$\lambda_a((x_1, \ldots, x_n)) := \begin{cases} (a, x_1, \ldots, x_n) & \text{if } x_1 \neq a^* \text{ or } n = 0, \\ (x_2, \ldots, x_n) & \text{if } x_1 = a^*. \end{cases}$$

We can calculate that the functions λ_s and λ_{s^*} are inverse to each other. For instance,

$$(s^*) \cdot \Big((s) \cdot (x_1, \ldots, x_n) \Big) = \begin{cases} (s^*) \cdot (s, x_1, \ldots, x_n) = (x_1, \ldots, x_n) & \text{if } x_1 \neq s^* \text{ or } n = 0, \\ (s^*) \cdot (x_2, \ldots, x_n) = (x_1, \ldots, x_n) & \text{if } x_1 = s^*, \end{cases}$$

so $\lambda_{s^*} \circ \lambda_s = \mathrm{id}$; a similar argument shows $\lambda_s \circ \lambda_{s^*} = \mathrm{id}$. Thus $\lambda_a \in G$ for any letter $a \in S \amalg S^*$.

Let $\Phi \colon F \to G$ be the unique function guaranteed by the previous proposition, which is multiplicative and extends the function $\phi \colon S \to G$ given by $s \mapsto \lambda_s$. The construction of Φ in the proof of that proposition and the fact that $(\lambda_s)^{-1} = \lambda_{s^*}$ shows that

$$\Phi((x_1, \ldots, x_n)) = \lambda_{x_1} \circ \cdots \circ \lambda_{x_n}.$$

We can evaluate any element of G at the empty word. In particular, we easily compute that

$$\Phi(x)(()) = (\lambda_{x_1} \circ \cdots \circ \lambda_{x_n})(()) = x \qquad \text{if } x = (x_1, \ldots, x_n),$$

and thus we see that $\Phi \colon F \to G$ is an injective function. Since

$$\Phi((x \cdot y) \cdot z) = \Phi(x \cdot y) \circ \Phi(z) = \Phi(x) \circ \Phi(y) \circ \Phi(z)$$

is equal to

$$\Phi(x \cdot (y \cdot z)) = \Phi(x) \circ \Phi(y \cdot z) = \Phi(x) \circ \Phi(y) \circ \Phi(z),$$

we conclude that $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in F$, i.e., the operation is associative. The remaining axioms for a group are straightforward: the identity element of F is the empty word, and the inverse of $(x_1, \ldots, x_n)$ is $(x_n^*, \ldots, x_1^*)$. □

Theorem. *The free group on S exists.*

Proof. We have produced a group F and a function $\iota \colon S \to F$, such that every function $\phi \colon S \to G$ to a group extends to a unique multiplicative function $\Phi \colon F \to G$, i.e., to a group homomorphism. □

15. Group presentations

I'll write $F(S)$ for the free group on a set S. **M 29 Aug**

A **group presentation** is a pair (S, R) consisting of (i) a set S, and (ii) a subset $R \subseteq F(S)$. The group *presented* by this data is defined to be **group presentation**

$$\langle S \mid R\rangle := F(S)/N,$$

where N is the **normal closure** of R in $F(S)$ (i.e., the smallest normal subgroup of $F(S)$ contaning R, which is the smallest subgroup of $F(S)$ containing $\bigcup_{g\in F(S)} gRg^{-1}$.) **normal closure**

We say that (S, R) is a **presentation** of a group G if there exists an isomorphism $G \approx \langle S \mid R\rangle$ of groups. **presentation**

We say that G is **finitely presentable** if it has a presentation (S, R) where S and R are both finite. **finitely presentable**

When $S = \{a_1, \dots, a_n\}$ and $R = \{r_1, \dots, r_k\}$, we often write

$$\langle S \mid R\rangle = \langle a_1, \dots, a_n \mid r_1, \dots, r_k\rangle.$$

Example. $\langle S \mid \varnothing\rangle$ is a presentation of the free group $F(S)$.

Example. $\langle \varnothing \mid \varnothing\rangle$ is a presentation of $F(\varnothing)$, which is the trivial group.

Example. $\langle a \mid a^n\rangle$ is a presentation of the cyclic group of order n.

Example. $\langle a, b \mid aba^{-1}b^{-2}, bab^{-1}a^{-2}\rangle$ is a presentation of the trivial group. (*Exercise:* prove this.)

Thus, a group can have many different presentations.

Example. $\langle r, s \mid r^n, s^2, srsr\rangle$ is a presentation of the dihedral group D_{2n} of order $2n$.

This is worth a proof. Consider the real 3×3-rotation matrices

$$R_\theta := \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad J_\theta := R_\theta \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} R_{-\theta} = \begin{bmatrix} \cos 2\theta & \sin 2\theta & 0 \\ \sin 2\theta & -\cos 2\theta & 0 \\ 0 & 0 & 1, \end{bmatrix}$$

which are respectively: rotation by angle θ around the z-axis, and rotation by angle π around the line through the vector $(\cos\theta, \sin\theta, 0)$. The subgroup $D_{2n} \leq GL_3(\mathbb{R})$ is the subset

$$\{\, R_{2\pi k/n}, J_{\pi k/n} \mid k = 0, \dots, n \,\},$$

which is easily seen to be a subgroup of order $2n$ using the identities

$$R_\alpha R_\beta = R_{\alpha+\beta}, \qquad R_\alpha J_\beta = J_\beta R_{-\alpha} = J_{\beta+\frac{\alpha}{2}}, \qquad J_\alpha J_\beta = R_{2(\alpha-\beta)}, \qquad R_{2\pi} = I.$$

Let $\phi\colon F(\{r, s\}) \to GL_3(\mathbb{R})$ be the unique homomorphism such that $\phi(r) = R_{2\pi/n}$ and $\phi(s) = J_0$. It is straightforward to verify that the image of ϕ equals D_{2n}.

Note that since

$$R_{2\pi/n}^n = I, \quad J_0^2 = I, \qquad J_0 R_{2\pi/n} = R_{-2\pi/n} J_0,$$

we see that $\phi(r^n) = \phi(s^2) = \phi(srsr) = I$, so the the homomorphism ϕ extends to a homomorphism $\overline{\phi}$ making the following diagram commute:

$$\begin{tikzcd}
\langle r, s\rangle \arrow[r, "\phi"] \arrow[d] & D_{2n} \\
G := \langle r, s \mid r^n, s^2, srsr\rangle \arrow[ur, dotted, "\overline{\phi}"'] &
\end{tikzcd}$$

I claim that $\overline{\phi}$ is an isomorphism to its image $\overline{\phi}(G) = D_{2n}$. Since $\overline{\phi}$ is surjective and its image has order $2n$, it suffices to show that $|G| \leq 2n$. To see this, note that in G any word w in r and s can be rewritten, using the identity $sr = r^{-1}s$, into a word of the same length of the form $r^a s^b$. The rules $r^n = 1$ and $s^2 = 1$ then let us rewrite this so that $0 \le a < n$ and $0 \le b < n$. Thus the list $1, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s$ exhausts the elements of G so $|G| \le 2n$.

Remark. I wrote out the above proof to indicate that identifying presentation of a group is generally non-trivial, even for very familiar groups such as the dihedral group.

In fact, the situation is tricky: there exist finitely presentable groups whose word problem is *undecidable.* (Theorem of P. Novikov and W. Boone in the 1950s.) The word problem for $G = \langle S \mid R\rangle$ is the following: to provide an algorithm which decides, for every element $w \in F(S)$, whether its image in G is the identity element.

The dihedral group example above has decidable word problem. In fact, I outlined an algorithm for deciding! However, there are presentations whose word problem is undecidable, and in fact such exist with relatively few generators and relations. (See wikipedia page on “Word problem for groups” for an example.)

Exercise. Show that $G = \langle a, b \mid aba^{-1}b^{-2},\ bab^{-1}a^{-2}\rangle$ is the trivial group.

16. A presentation of the symmetric group

Proposition. *For $n \ge 1$, we have*

$$S_n \approx \langle s_1, \dots, s_{n-1} \mid R\rangle,$$

where R consists of the relations

$$\begin{aligned} s_i^2 &= 1, && \textit{for } i = 1, \dots, n-1, \\ (s_i s_j)^2 &= 1, && \textit{when } |i-j| \ge 2, \\ (s_i s_{i+1})^3 &= 1, && \textit{for } i = 1, \dots, n-1. \end{aligned}$$

Proof. Let

$$G_n := \langle s_1, \dots, s_{n-1} \mid s_i^2,\ (s_i s_{i+1})^3,\ (s_i s_j)^2 \text{ for } |i-j| \ge 2\rangle.$$

Note that each s_i has order 2, so $s_i^{-1} = s_i$, and that s_i and s_j commute if $|i-j| \ne 1$.

We can define a homomorphism

$$\phi\colon G_n \to S_n, \qquad \phi(s_i) = (i\ i+1)$$

by sending each generator to the transposition of consecutive numbers. To check that this is well-defined, verify the identities

$$(i\ i+1)^2 = \mathrm{id}, \qquad ((i\ i+1)(j\ j+1))^2 = \mathrm{id} \quad \text{for } |i-j| \ge 2, \quad ((i\ i+1)(i+1\ i+2))^3 = \mathrm{id}\,.$$

This is a straightforward exercise: 2-cycles have order 2, as do products of disjoint 2-cycles, while the product of two non-disjoint 2-cycles is always a 3-cycle.

It’s not hard to see that $\{\phi(s_1), \dots, \phi(s_{n-1})\}$ generates the symmetric group, and thus that ϕ is surjective. Let’s make this precise in the following way. For $\sigma \in S_n$, define the “length” of σ by

$$|\sigma| := |\{\, (i,j) \mid 1 \le i < j \le n,\ \sigma(i) > \sigma(j) \,\}|,$$

the size of the set of pairs in $\{1, \dots, n\}$ that σ “reverses the order of”. Thus $0 \le |\sigma| \le \binom{n}{2}$, where $|\sigma| = 0$ iff $\sigma = \mathrm{id}$, and $|\sigma| = \binom{n}{2}$ iff $\sigma(x) = n - x + 1$. It is straightforward to verify that

$$|(k\ k+1)\sigma| = \begin{cases} |\sigma| + 1 & \text{if } u < v, \\ |\sigma| - 1 & \text{if } u > v, \end{cases} \qquad \text{where } k = \sigma(u) \text{ and } k+1 = \sigma(v).$$

Using this, it is easy to prove by induction on $|\sigma|$ that σ is in the subgroup of S_n generated by the image of ϕ. In fact, this shows that every $\sigma \in S_n$ can be written as a product of exactly $|\sigma|$ transpositions of the form $(k\ k+1)$, and no fewer.

To complete the proof, it suffices to show that $|G_n| \le |S_n| = n!$. We do this by induction on n, where the base case $n = 1$ is just the observation that G_1 is the trivial gorup.

Suppose $n \geq 1$. Let $H \leq G_{n+1}$ be the subgroup generated by $\{s_1, \ldots, s_{n-1}\}$. There is an evident surjective homomorphism $G_n \to H$, so $|H| \leq |G_n|$, so by the inductive hypothesis $|H| \leq n!$. Now consider the following left H-cosets:

$$H_{n+1} = H, \quad H_n = s_n H_{n+1}, \quad H_{n-1} = s_{n-1} H_n, \quad \ldots, \quad H_1 = s_1 H_2.$$

Let $K = H_1 \cup \cdots \cup H_{n+1}$, so that $|K| \leq (n+1)|H| \leq (n+1)!$. (The cosets are actually pairwise distinct so $|K| = (n+1)|H|$, but I don't need to prove that now.) I'll show that $s_i K = s_i^{-1} K \subseteq K$ for all $i = 1, \ldots, n$, and thus $G_{n+1} K \subseteq K$. Since $e \in K$ this implies $G_{n+1} \subseteq K$ so $G_{n+1} = K$, so $|G_{n+1}| \leq (n+1)!$ as desired.

In fact, I claim

$$s_i H_j = \begin{cases} H_{j+1} & \text{if } i = j, \\ H_{j-1} & \text{if } i = j-1, \\ H_j & \text{otherwise.} \end{cases}$$

(In other words, s_i permutes the set $\{H_1, \ldots, H_{n+1}\}$ by transposing H_i and H_{i+1}.) We can prove this using downward induction on j. When $j = n+1$, we have $H_{n+1} = H$, and

$$s_i H = H \quad \text{if } i \leq n+1, \qquad s_n H = H_n.$$

When $j < n+1$, we have $s_i H_j = s_i s_j H_{j+1}$. Thus, using the induction hypothesis, we have

- $s_i H_j = s_i s_j H_{j+1} = s_j s_i H_{j+1}$ if $i < j-1$ or $i > j+1$, since in that case $s_i s_j = s_j s_i$,
- $s_{j-1} H_j = H_{j-1}$ by definition,
- $s_j H_j = s_j s_j H_{j+1} = H_{j+1}$ (since $s_j^2 = e$),
- $s_{j+1} H_j = s_{j+1} s_j H_{j+1} = s_j s_{j+1} s_j s_{j+1} H_{j+1} = s_j s_{j+1} s_j H_{j+2} = s_j s_{j+1} H_{j+2} = s_j H_{j+1} = H_j$, using the identity $(s_j s_{j+1})^3 = e$ and the inductive hypothesis (which gives $s_j H_{j+2} = H_{j+2}$).

□

Exercise. Given $1 \leq a \leq b \leq n$, write $[a, b] := (a\ a+1\ \cdots\ b-1\ b) \in S_n$. For instance, $[2, 2] = e$, $[2, 3] = (2\ 3)$, $[2, 4] = (2\ 3\ 4)$, etc.

Show that for any $\sigma \in S_n$, there exists a unique sequence of integers $a_1, \ldots, a_n$ with $a_k \in \{1, \ldots, k\}$ such that

$$\sigma = [a_n, n]\,[a_{n-1}, n-1]\,\cdots\,[a_2, 2]\,[a_1, 1].$$

(Hint: Use induction on n; think about the proof of the presentation of S_n described above; note that $[a, b] = (a\ a+1)(a+1\ a+2)\cdots(b-2\ b-1)(b-1\ b)$.)

17. Group actions

Definition from DF §1.7.

A **(left) group action** of a group G on a set X is a map $G \times X \to X$, written as a binary operation $(g, x) \mapsto g \cdot x$ (or $(g, x) \mapsto gx$), such that

(left) group action

(1) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $g_1, g_2 \in G$, $x \in X$, and
(2) $e \cdot x = x$ for all $x \in X$.

Given a binary operation $G \times X \to X$, we can define for each $g \in G$ a function $\phi_g \colon X \to X$ by

$$\phi_g(x) := g \cdot x.$$

Proposition. *A binary operation $G \times X \to X$ is a group action if and only if $g \mapsto \phi_g$ defines a group homomorphism $\phi \colon G \to \mathrm{Sym}(X)$.*

Proof. Suppose we have a group action of G on X. First we need to check that each ϕ_g is an isomorphism. We have

$$\phi_{g^{-1}}(\phi_g(x)) = g^{-1} \cdot (g \cdot x) = (g^{-1} g) \cdot x = e \cdot x = x,$$

for all $g \in G$, which also implies $\phi_g(\phi_{g^{-1}}(x)) = x$. Thus ϕ_g and $\phi_{g^{-1}}$ are inverse to each other and so are bijections, so each $\phi_g \in \mathrm{Sym}(X)$. Then we have

$$\phi_{g_1 g_2}(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \phi_{g_1}(\phi_{g_2}(x)),$$

so $\phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2}$, so that $g \mapsto \phi_g$ is a homomorphism.

Now suppose $g \mapsto \phi_g$ is a group homomorphism. Then $\phi_e = \mathrm{id}$ so $e \cdot x = \phi_e(x) = x$, and $g_1 \cdot (g_2 \cdot x) = \phi_{g_1}(\phi_{g_2}(x)) = \phi_{g_1 g_2}(x) = (g_1 g_2) \cdot x$. □

So we have an equivalent way of talking about a group action: as a homomorphism $G \to \mathrm{Sym}(X)$.

A set X equipped with a G-action is called a **G-set**. **G-set**

Example. Every set X has a *tautological* action by its permutation group $G = \mathrm{Sym}(X)$. In this case, the "action" notation is compatible with "function" notation:

$$\sigma \cdot x = \sigma(x) \qquad \text{for } \sigma \in \mathrm{Sym}(X),\ x \in X.$$

The corresponding homomorphism is just the identity map $G \to \mathrm{Sym}(X)$.

Example (Left cosets). Recall that for $H \leq G$ we have a set $G/H = \{\, xH \mid x \in G \,\}$ of left-cosets of H. This set admits a natural G-action, by

$$g \cdot xH := gxH.$$

We can rewrite this as a homomorphism $\lambda\colon G \to \mathrm{Sym}(G/H)$ with $\lambda_g(xH) = gxH$.

Example (Right cosets). We also have a set $H\backslash G = \{\, Hx \mid x \in G \,\}$ of right cosets for H. This also admits a natural G-action, by

$$g \cdot Hx := Hxg^{-1}.$$

Let's verify $g_1 \cdot (g_2 \cdot Hx) = (g_1 g_2) \cdot Hx$:

$$g_1 \cdot (g_2 \cdot Hx) = g_1 \cdot (Hxg_2^{-1}) = Hxg_2^{-1}g_1^{-1} = Hx(g_1 g_2)^{-1} = (g_1 g_2) \cdot Hx.$$

Note: this does *not work* if we try to have $g \cdot Hx = Hxg$, unless G is abelian.

Example (Conjugation). Every group G has a **conjugation action** on its underlying set $X = G$, by **conjugation action**

$$\mathrm{conj}_g(x) := gxg^{-1}.$$

Thus $g \mapsto \mathrm{conj}_g$ gives a homomorphism $G \to \mathrm{Sym}(G)$. Note: it is not recommended to try to write $g \cdot x$ for gxg^{-1}.

18. Properties of group actions

W 31 Aug

We have the following definitions associated to a group action.

(1) The **kernel** of an action $G \curvearrowright X$ is **kernel of group action**

$$\{\, g \in G \mid g \cdot x = x \text{ for all } x \in X \,\} = \mathrm{Ker}(G \xrightarrow{g \mapsto \phi_g} \mathrm{Sym}(X)),$$

a normal subgroup of G.

(2) For $x \in X$, the **stabilizer** of x is **stabilizer**

$$\mathrm{Stab}(x) = G_x := \{\, g \in G \mid g \cdot x = x \,\}.$$

Verify that G_x is a subgroup of G. Also, note that the kernel of the action is the intersection $\bigcap_{x \in X} G_x$.

(3) An action is **faithful** if the kernel is trivial. **faithful group action**

(4) An action is **free** if all the stabilizers G_x are trivial. **free group action**

Different elements of X can have different stabilizers. However, we have the following.

Proposition. *If G acts on X, then if $x, y \in X$ are such that $y = gx$ for some $g \in G$, then*

$$G_y = gG_xg^{-1}.$$

Proof. If $a \in G_x$, then $a \cdot x = x$, so $(gag^{-1}) \cdot y = gag^{-1}gx = gax = gx = x$, and therefore $gag^{-1} \in G_y$. We have shown $gG_xg^{-1} \subseteq G_y$.

Conversely, if $b \in G_y$, let $a = g^{-1}bg$. Then $ax = g^{-1}bg \cdot g^{-1}y = g^{-1}bx = g^{-1}x = y$, and therefore $G_y \subseteq gG_xg^{-1}$. □

Example (Trivial action). For any set X and group G, we can define the **trivial action** by $g \cdot x := x$. In this case:

trivial action

- The kernel of the action is the whole group G, as is every stabilizer G_x.
- The action is neither nor faithful, unless $G = \{e\}$.

Example (Tautological action of S_n). Consider the tautological action of $G = S_n$ on $X = \{1, \dots, n\}$, so the corresponding homomorphism $G \to \mathrm{Sym}(X)$ is identity. We have that:

- For $x \in \{1, \dots, n\}$, the stabilizer is $G_x = \{\, \sigma \in S_n \mid \sigma(x) = x \,\}$.
- The kernel of the action is the trivial subgroup, so it is a faithful action.
- The action of S_n on X is not free, since each G_x is non-trivial.
- Each G_x is isomorphic to S_{n-1}, but each is a *distinct* subgroup of S_n.
- The G_x are conjugate to each other: if $\sigma \in S_n$ is such that $\sigma(x) = y$, then $G_y = \sigma G_x \sigma^{-1}$.

Exercise. Let $H \leq G$, and consider the left multiplication action $G \curvearrowright X = G/H$ on left cosets for H.

(1) $G_{eH} = H$.
(2) More generally, $G_{xH} = xHx^{-1} = \{\, xhx^{-1} \mid x \in G \,\}$.
(3) The kernel of the action is $\bigcap_{x \in G} xHx^{-1}$, which is the largest normal subgroup of G which is contained in H.

19. Applications of group actions

Theorem (Cayley's theorem). *Every group is isomorphic to a subgroup of some permutation group* $\mathrm{Sym}(X)$.

Proof. Given G, it suffices to produce a faithful action on some set X, so that the induced homomorphism $\phi\colon G \to \mathrm{Sym}(X)$ is injective, and therefore defines an isomorphism $G \approx \phi(G)$.

In fact, let $X = G$ equipped with the natural left action by G, so $g \cdot x := gx$. Then this action is faithful, since $gx = x$ for all $x \in X$ certainly implies $g = e$. □

The following is a generalization (for finite groups) of the fact that subgroups of index 2 are always normal.

Proposition. *If G is a finite group, and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.*

Proof. Let $H \leq G$ be a subgroup of index p, and consider the left action of G on $X = G/H$, which gives a homomorphism $\phi\colon G \to \mathrm{Sym}(G/H) \approx S_p$. Let $K = \mathrm{Ker}\,\phi$ be the kernel of the action. Note that $K \leq H$ since if $\phi(g) = \mathrm{id}$, then in particular $g(eH) = eH$ so $g \in H$.

By the first isomorphism theorem, G/K is isomorphic ot a subgroup of S_p, and so $|G : K|$ must divide $|S_p| = p!$. Furthermore, since $K \leq H$ we have $|G : K| = |G : H||H : K| = p|H : K|$, so $|H : K|$ divides $(p-1)!$ and divides $|G|$. But by hypothesis $|G|$ and $(p-1)!$ have no common factors, so $|H : K| = 1$, so $K = H$. Thus H is equal to the kernel of a homomorphism, so is a normal subgroup. □

Remark. The above can be modified to apply to non-finite groups: the hypothesis needed is that for any finite index subgroup of G, no prime divisor of the index is $< p$.

20. Orbits of group actions

Consider a group action $G \curvearrowright X$. Define a relation $\sim$ on X by

$$x \sim y \qquad \Longleftrightarrow \qquad \exists g \in G,\ g \cdot x = y.$$

This in an equivalence relation: $e \cdot x = x$, $g \cdot x = y \ \Rightarrow\ g^{-1} \cdot y = x$, $g \cdot x = y,\ g' \cdot y = z \ \Rightarrow\ (g'g) \cdot x = z$.

An equivalence class for this relation is called an **orbit** of the action. Thus, any action of G on X partitions X into pairwise disjoint orbits. I write $Gx = \{\, g \cdot x \mid g \in G \,\}$ for the orbit which contains $x \in X$. **orbit**

Warning. Unfortunately, "Gx" can look a lot like "G_x", especially in handwriting. Sometimes I'll write $G \cdot x$ for the orbit.

An action is **transitive** if it has exactly one orbit. **transitive**

Example. If $X = G/H$ with left action by G, then this is a transitive action, so has a single orbit.

Recall that elements which are in the same orbit have *conjugate* stabilizer subgroups: if $g \cdot x = y$, then $G_y = gG_xg^{-1}$.

Theorem (Orbit/Stabilizer theorem). *Consider an action $G \curvearrowright X$, and an element $x \in X$. Then there is a bijection*

$$G/G_x \xrightarrow{\sim} Gx, \qquad gG_x \mapsto g \cdot x,$$

between the orbit containing x and the set of left cosets of its stabilizer.

Thus for an orbit $\mathcal{O}$ we have $|\mathcal{O}| = |G : G_x|$ for any $x \in \mathcal{O}$.

Proof. Let $H = G_x$. The function $G/G_x \to G \cdot x$ is certainly well-defined: if $gH = g'H$, then $g' = gh$ for some $h \in H$, and $g' \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$.

Surjectivity is clear: any $x' \in Gx$ has the form $x' = gx$ for some $g \in X$, and then $gH \mapsto gx = x'$. Injectivity: if $gH, g'H$ are such that $g \cdot x = g' \cdot x$, then $g^{-1}g' \cdot x = x$ so $g^{-1}g' \in G_x = H$, and thus $g'H = gH$ as desired. □

When G acts on a finite set X, we can put everything together as follows.

Proposition. *Let G act on a finite set X. We have*

$$|X| = \sum_{k=1}^{r} |G : G_{x_k}|,$$

where $x_1, \dots, x_r \in X$ are representatives of the orbits of the action. (That is: $Gx_i \cap Gx_j = \varnothing$ when $i \neq j$, and $\bigcup_{k=1}^{r} Gx_k = x$.)

Proof. The set X is partitioned into pairwise disjoint orbits $\mathcal{O}_1, \dots, \mathcal{O}_r$, so $|X| = \sum |\mathcal{O}_k|$. By the orbit/stabilizer theorem, $|\mathcal{O}_k| = |G : G_{x_k}|$ for any $x_k \in \mathcal{O}_k$. □

21. Cauchy's theorem

Theorem (Cauchy's theorem). *Let G be a finite group. If a prime p divides $|G|$, then G has an element of order p.*

I'll give a clever proof of Cauchy's theorem, due to McKay, which uses easy facts about a group acting on a set.

Proof. Assume the prime p divides $|G|$. Consider the set

$$X := \{\, (g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = e \,\}$$

of p-tuples of elements of G whose product is the identity element. Note that $(g_1, \dots, g_p) \in X$ iff $g_p = (g_1 \cdots g_{p-1})^{-1}$, so there is a bijection $X \leftrightarrow G^{p-1}$. Thus $|X| = |G|^{p-1}$. The consequence we need is that p divides $|X|$.

Let $\phi\colon X \to X$ be the function defined by

$$\phi\big((g_1, \dots, g_p)\big) := (g_2, \dots, g_p, g_1).$$

This is well-defined, since $g_2 \cdots g_p g_1 = g_1^{-1}(g_1 \cdots g_p)g_1$, so $g_1 \cdots g_p = e$ implies $g_2 \cdots g_p g_1 = e$.

Now suppose $x = (g_1, \dots, g_p) \in X$ is a *fixed point* of ϕ, i.e., is such that $\phi(x) = x$. This can happen iff $g_1 = g_2 = \cdots = g_p$. Since $x \in X$ we must have that $e = g_1 \cdots g_p = g_1^p$. That is, there is a bijection

$$\{\, x \in X \mid \phi(x) = x \,\} \longleftrightarrow \{\, g \in G \mid g^p = e \,\}.$$

We know the right-hand set has at least one element, namely $g = e$. We want to show there is a $g \neq e$ with $g^p = e$, since then $|g| = p$.

Note that $\phi^p = \mathrm{id}$, i.e., iterating ϕ p-times gives the identity map. Thus we can define an action of the cyclic group $H = \langle \phi \mid \phi^p \rangle$ on X by $\phi^k \cdot x := \phi^k(x)$. Since $|H| = p$, orbits of the action are either of size 1 or size p. Let $m =$ number of orbits of size 1 and $n =$ number of orbits of size p, so that

$$|X| = m + pn.$$

Since $p \mid |X|$, we conclude that $p \mid m$.

Orbits of size 1 correspond exactly to fixed points of ϕ, which correspond to elements of G with order dividing p. As we noted, $m \geq 1$, so $m \geq p \geq 2$, and thus there exists an element of order p in G. □

22. Cycle decomposition of permutations

Let X be a set, e.g., $X = \{1, \dots, n\}$. Given a finite ordered list $(x_1, \dots, x_d)$ of pairwise distinct elements X, with $d \geq 2$, the ***d*-cycle** defined by this list is the permutation $\sigma \in \mathrm{Sym}(X)$ defined by **F 2 Sep** ***d*-cycle**

$$\begin{aligned} \sigma(x_j) &= x_{j+1} && \text{if } j \in \{1, \dots, d-1\}, \\ \sigma(x_d) &= x_1, && \\ \sigma(x) &= x, && \text{if } x \notin \{x_1, \dots, x_d\}. \end{aligned}$$

We use the notation $\sigma = (x_1 \ \cdots \ x_d)$ for this d-cycle.

Note:

- The order of the elements in the cycle matters, but only "cyclically". That is, $(x_1 \ \cdots \ x_d) = (x_d \ x_1 \cdots \ x_{d-1})$, etc.
- We can extend the cycle notation to sequences of length 1, but this means that $(x) = \mathrm{id}$ for all $x \in X$. We don't regard these as cycles for the purposes of the theorem below.
- Cycles $\sigma = (x_1 \ \cdots \ x_d)$ and $\tau = (y_1 \ \cdots \ y_e)$ are **disjoint** if $\{x_1, \dots, x_d\} \cap \{y_1, \dots, y_e\} = \varnothing$. **disjoint** If the cycles are disjoint, then they commute: $\sigma\tau = \tau\sigma$.
- There is a formula for conjugating cycles: if $\sigma \in \mathrm{Sym}(X)$, then

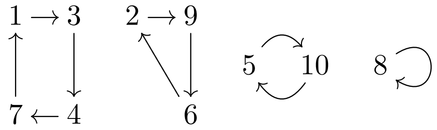
  $$\sigma(x_1 \ \cdots \ x_d)\sigma^{-1} = (\sigma(x_1) \ \cdots \ \sigma(x_d)).$$

  This is straightforward to verify.

A **cycle decomposition** of a permutation $\sigma \in \mathrm{Sym}(X)$ is an expression $\sigma = \sigma_1 \cdots \sigma_k$, where **cycle decomposition** $k \geq 1$, each σ_j is a cycle, and the cycles $\sigma_1, \dots, \sigma_k$ are pairwise disjoint.

Example. Here is picture a cycle decomposition of

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 9 & 4 & 7 & 10 & 2 & 1 & 8 & 6 & 5 \end{pmatrix} = (1\ 3\ 4\ 7)(2\ 9\ 6)(5\ 10) \in S_{10}.$$



Theorem (Cycle decomposition of permutations)**.** *Let X be a finite set, and $\sigma \in \mathrm{Sym}(X)$ with $\sigma \neq \mathrm{id}$. Then σ admits a cycle decompostion, which is unique up to reordering the cycles.*

Proof. Let $G = \langle \sigma \rangle \leq \mathrm{Sym}(X)$ be the cyclic group generated by σ. Since X is finite, $|G| < \infty$. We have an evident action of G on X, by restricting the tautological action.

Decompose X as a disjoint union of its orbits under the G-action. For each orbit $\mathcal{O}$ of the action, pick $x \in \mathcal{O}$. Then there is a bijection

$$G/G_x \xrightarrow{\sim} \mathcal{O}, \qquad \sigma^i G_x \mapsto \sigma^i(x),$$

and $d := |G : G_x| = |\mathcal{O}|$. Since G is cyclic, so is G/G_x, so the d distinct elements of $\mathcal{O}$ are

$$x, \quad \sigma(x), \quad \cdots, \quad \sigma^{d-1}(x).$$

Write $\mathcal{O}_1, \ldots, \mathcal{O}_k$ for the pairwise disjoint orbits of G acting on X which have size ≥ 2. For each $1 \leq j \leq k$ pick $x_j \in \mathcal{O}_j$ and define $\sigma_j = (x_j \ \sigma(x_j) \ \cdots \ \sigma^{d-1}(x_j))$, where $d = |\mathcal{O}_j|$. It is straightforward to verify that

$$\sigma = \sigma_1 \cdots \sigma_d,$$

and that the ordering of the orbits doesn't matter here. (Note: if $y \notin \bigcup_{j=1}^k \mathcal{O}_j$, then $\sigma(y) = y$ since the orbit $G \cdot y$ will have size 1. If $y \in \mathcal{O}_j$, then $\sigma(y) = \sigma_j(y)$, and $\sigma_i(y) = y$ for $i \neq j$.) We have shown a cycle decomposition exists for σ. .

For uniqueness, consider any cycle decomposition $\sigma = \sigma_1 \cdots \sigma_k$. The orbits of the G action on X are as follows:

- Orbits of size 1, which correspond to the elements of X not contained in any of the cycles σ_j.
- For each $j \in \{1, \ldots, k\}$, an orbit $\mathcal{O}_j$ of size equal to the order of σ_j. Furthermore, for any $x \in \mathcal{O}_j$ we have $\sigma(x) = \sigma_j(x)$.

We discover that we can recover the list of cycles (up to reordering) directly from the action of G on X. The recipe is: for each orbit $\mathcal{O}_j$ of size $d_j \geq 2$, pick $x \in \mathcal{O}_j$ and let $\sigma_j = (x \ \sigma(x) \ \cdots \ \sigma^{d_j - 1}(x))$. □

23. Alternating groups are simple

A group G is **simple** if its only normal subgroups are $\{e\}$ and G. By convention, the trivial group $\{e\}$ is *not* simple. **simple**

Example. Let p be a prime. Then the cyclic group $G = C_p$ of order p is simple.

I'll sketch a general proof that the alternating group A_n is simple for all $n \geq 5$.

First, we have a sequence of observations.

- Elements of A_n are precisely the even permutations, i.e., the permutations which can be written as a product of an even number of 2-cycles (not necessarily disjoint).
- Thus, A_n is generated by the subset of elements which are products of two 2-cycles (not necessarily disjoint). Notice that there are three types of such elements (in the following, a, b, c, d are always pariwise distinct):

$$(a\ b)(a\ b), \qquad (a\ b)(a\ c), \qquad (a\ b)(c\ d).$$

- We have

$$(a\ b)(a\ b) = e, \qquad (a\ b)(a\ c) = (a\ c\ b), \qquad (a\ b)(c\ d) = (a\ d\ c)(a\ b\ c).$$

  Thus, A_n is also generated by its subset of 3-cycles.
- If $N \trianglelefteq A_n$ is a nomal subgroup which contains some 3-cycle $(a\ b\ c)$, it must contain every 3-cycle and thus $N = A_n$.

  First note that $(x\ y\ z)^{-1} = (x\ z\ y)$, so it's enough to produce for each subset $\{x, y, z\} \subseteq \{1, \ldots, n\}$ a 3-cycle in N with those three elements.

Next, note that if a, b, c, x are pairwise distinct,

$$(c\ b\ x)(a\ b\ c)(c\ b\ x)^{-1} = (a\ x\ b),$$

so if $(a\ b\ c) \in N$ then $(a\ x\ b), (a\ b\ x) \in N$. Iterating this constructs all 3-cycles as elements of N.

Thus, to prove A_n is simple, we must show that if $N \trianglelefteq A_n$ is a non-trivial normal subgroup, it must contain at least one 3-cycle. This is where we will need $n \geq 5$.

We start by assuming some element $g \in N$ with $g \neq e$, which we can write as a product of disjoint cycles: $g = c_1 \cdots c_k$ with $k \geq 1$. I'll assume the cycles are listed in terms of descending order, so $\text{order}(c_1) \geq \text{order}(c_2) \geq \cdots$.

We use the following trick. If $t \in A_n$ is any 3-cycle, then $tgt^{-1}g^{-1} \in N$. Because disjoint cycles commute, we see that if the elements of t are disjoint from those of $c_{j+1}, \ldots, c_k$, then

$$tgt^{-1}g^{-1} = t(c_1 \cdots c_k)t^{-1}(c_1 \cdots c_k)^{-1} = t(c_1 \cdots c_j)t^{-1}(c_1 \cdots c_j)^{-1}.$$

(a) Suppose $\text{order}(c_1) = m \geq 4$. Write $c_1 = (a_1\ \cdots\ a_m)$, and let $t = (a_1\ a_2\ a_3)$. Observe that

$$tgt^{-1}g^{-1} = tc_1t^{-1}c_1^{-1} = (a_2\ a_3\ a_1\ a_4\ \cdots\ a_m)(a_1\ a_2\ \cdots\ a_m)^{-1} = (a_1\ a_2\ a_4),$$

a 3-cycle in N.

(b) Now suppose $\text{order}(c_1) = \text{order}(c_2) = 3$, so $g = (a_1\ a_2\ a_3)(a_4\ a_5\ a_6)x$ with x disjoint from c_1 and c_2. Let $t = (a_2\ a_3\ a_4)$. Then

$$tc_1c_2t^{-1} = (a_1\ a_3\ a_4)(a_2\ a_5\ a_6)$$

and thus

$$tgt^{-1}g^{-1} = t(c_1c_2)t^{-1}\,(c_1c_2)^{-1} = (a_1\ a_4\ a_2\ a_3\ a_5)$$

is a 5-cycle in N, so N contains a 3-cycle by (a).

(c) Now suppose $\text{order}(c_1) = 3$ is the only 3-cycle in the decomposition, so $g = c_1x$ with x a product of disjoint 2-cycles which are also disjoint from c_1. Then $x^2 = e$, so $g^2 = c_1xc_1x = c_1^2x^2 = c_1^2$ which is a 3-cycle in N.

(d) Now suppose all c_i are 2-cycles, so $g = c_1c_2x$, with $c_1 = (a_1\ a_2)$, $c_2 = (a_3\ a_4)$, and x a product of disjoint 2-cycles also disjoint from the first two. Let $t = (a_2\ a_3\ a_4)$. Then

$$tc_1c_2t^{-1} = (a_1\ a_3)(a_4\ a_2)$$

and thus

$$h := tgt^{-1}g^{-1} = t(c_1c_2)t^{-1}\,(c_1c_2)^{-1} = (a_1\ a_4)(a_2\ a_3) \in N.$$

Let $a_5 \notin \{a_1, a_2, a_3, a_4\}$. (This is the place where we use $n \geq 5$.) Let $u = (a_1\ a_4\ a_5)$. Then

$$uhu^{-1} = (a_4\ a_5)(a_2\ a_3) \in N,$$

and thus

$$uhu^{-1}h^{-1} = (a_1\ a_5\ a_4) \in N$$

is a 3-cycle in N.

Note: A_4 is not simple, because the subgroup $V = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$ generated by the products of disjoint 2-cycles is normal. Part (d) of the proof fails here.

Remark. Using this, we can completely describe all the normal subgroups of S_n. They are, with one exception:

$$\{e\}, \qquad A_n, \qquad S_n.$$

Note that when $n \leq 2$, some of these subgroups are equal to each other. The only exception is a normal subgroup $V \trianglelefteq S_n$ of order 4, which is the subgroup of A_4 described above.

To see this, suppose $N \trianglelefteq S_n$, and assume $n \geq 5$. Then $N \cap A_n$ must be normal in A_n, so either $A_n \leq N$ (so $N = A_n$ or $N = S_n$), or $N \cap A_n = \{e\}$. So suppose $N \neq \{e\}$ and $N \cap A_n = \{e\}$.

Then $NA_n = S_n$, and the diamond isomorphism theorem gives $|NA_n : A_n| = |N : N \cap A_n|$, whence $|N| = 2$. So $N = \{e, \sigma\}$ with $|\sigma| = 2$, so g can only be a product of disjoint 2-cycles $g = (a_1\ b_1) \cdots (a_k\ b_k)$. Now use the cycle conjugation formula to find $g \in S_n$ so that $g\sigma g^{-1} \neq \sigma$.

24. Conjugation action

Recall the conjugation action of G on itself:

$$\operatorname{conj}_g(x) = gxg^{-1}, \qquad g, x \in G.$$

- The *orbits* for the conjugation action are precisely the conjugacy classes.
- There doesn't seem to be a standard notation for the conjugacy class which contains an element x. I'll write.
$$\mathrm{Cl}(x) := \{\, gxg^{-1} \mid g \in G \,\}.$$
- The *stabilizer* of $x \in G$ under the conjugation action is the **centralizer subgroup** of x:
$$C_G(x) := \{\, g \in G \mid gxg^{-1} = x \,\} = \{\, g \in G \mid gx = xg \,\}.$$
Note: this is *not* the center of G.
- The kernel of $\operatorname{conj}\colon G \to \mathrm{Sym}(G)$ is precisely the center
$$Z_G = \{\, g \in G \mid gx = xg\ \forall x \in G \,\}.$$
Thus, the conjugation action is faithful iff $Z_G = \{e\}$.
- Note that $\mathrm{Cl}(e) = \{e\}$ and $C_G(e) = G$. Thus, the conjugation action is not free or transitive (unless $G = \{e\}$).

centralizer subgroup

Example (Conjugation in abelian groups). If G is abelian, then $gxg^{-1} = x$, so the conjugation action is trivial. So all orbits have size 1, and all centralizers $C_G(x) = G$.

Example (Conjugation in D_{2n}). Consider

$$D_{2n} = \langle r, s \mid r^n, s^2, (sr)^2 \rangle = \{e, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}.$$

To understand the conjugation action, we first understand conj_g when g is one of the elements of the generating set $\{r, s\}$.

- Conjugation by r acts as:
$$r^k \mapsto r(r^k)r^{-1} = r^k, \qquad sr^k \mapsto r(sr^k)r^{-1} = sr^{k-2}.$$
- Conjugation by s acts as:
$$r^k \mapsto s(r^k)s^{-1} = r^{-k}, \qquad sr^k \mapsto s(sr^k)s^{-1} = sr^{-k}.$$

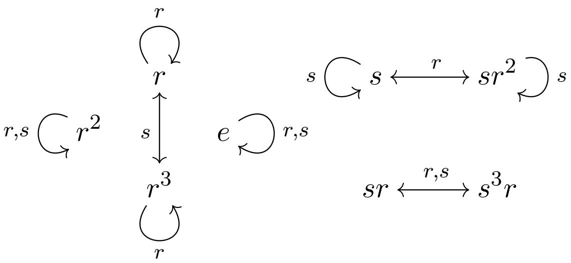
You can read off other conjugation functions from these. For instance, $\operatorname{conj}_{rs} = \operatorname{conj}_r \circ \operatorname{conj}_s$. However, to figure out the orbits, it's enough to draw a picture of conj_r and conj_s, and see what's connected. It is harder to read off the stabilizers; it is very helpful to remember the formula $|C_G(x)| = |G|/|\mathrm{Cl}(x)|$.

This sorts out differently depending on whether n is even or odd.

- If $n = 2m$, then $G = D_{2n}$ has a non-trivial center $\langle r^m \rangle = \{e, r^m\}$. In this case, the conjugacy classes are:
$$\{e\}, \quad \{r^m\}, \quad \{r, r^{-1}\}, \quad , \cdots , \quad \{r^{m-1}, r^{-(m-1)}\}, \quad \{s, sr^2, \dots, sr^{2n-2}\}, \quad \{sr, sr^3, \dots, sr^{2n-1}\}.$$
Thus, two conjugacy classes of size 1, $m-1$ classes of size 2, and two classes of size m. The centralizers are described by
$$C_G(e) = C_G(r^m) = G, \quad C_G(r^k) = \langle r \rangle,\ (m \nmid k), \quad C_G(sr^k) = \langle r^m, sr^k \rangle,$$
having orders $2n$, n, and 4 respectively.

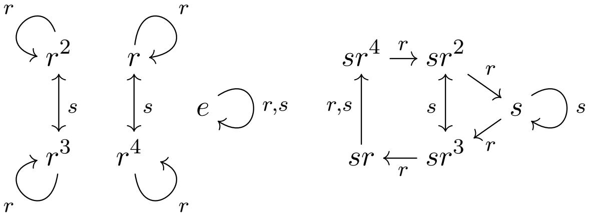
- If $n = 2m + 1$, then $G = D_{2n}$ has trivial center. In this case, the conjugacy classes are:
$$\{e\}, \quad \{r, r^{-1}\}, \quad \{r^m, r^{-m}\}, \quad \{s, sr, \ldots, sr^{n-1}\}.$$
Thus, one conjugacy class of size 1, m classes of size 2, and one class of size n. The centralizers are described by
$$C_G(e) = G, \quad C_G(r^k) = \langle r \rangle, \ (n \nmid k), \quad C_G(sr^k) = \langle sr^k \rangle,$$
having orders $2n$, n, and 2 respectively.

Example. For $g = D_8$, we have



So the conjugacy classes are: $\{e\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}$. The stabilizers cannot always be read off directly from this picture, but we can use the fact that $|C_G(x)| = |G|/|\mathrm{Cl}(x)|$ to help compute them:
$$C_G(e) = C_G(r^2) = G, \qquad C_G(r) = C_G(r^3) = \langle r \rangle,$$
$$C_G(s) = C_G(sr^2) = \langle r^2, s \rangle, \qquad C_G(sr) = C_G(s^3r) = \langle r^2, sr \rangle.$$

Example. For $G = D_{10}$ we have



So the conjugacy classes are $\{e\}, \{r, r^4\}, \{r^2, r^3\}, \{s, sr, sr^2, sr^3, sr^4\}$. The stabilizers are
$$C_G(e) = G, \qquad C_G(r) = C_G(r^2) = C_G(r^3) = C_G(r^4) = \langle r \rangle,$$
$$C_G(s) = \langle s \rangle, \qquad C_G(sr) = \langle sr \rangle, \qquad C_G(sr^2) = \langle sr^2 \rangle, \qquad C_G(sr^3) = \langle sr^3 \rangle, \qquad C_G(sr^4) = \langle sr^4 \rangle.$$

You can extend this to general dihedral groups D_{2n}, where there are two cases depending on whether n is even or odd.

25. The class equation

Recall that the center of a group G is $Z_G = \{\, g \in G \mid gx = xg \ \forall x \in G \,\}$. It is a normal subgroup of G.

Theorem (Class equation)**.** *For a finite group G, we have*
$$|G| = |Z_G| + \sum_{k=1}^{r} |G : C_G(g_k)|,$$
where $g_1, \ldots, g_r$ are representatives of the distinct conjugacy classes of G not contained in the center Z_G.

Note that each of the terms on the right-hand side is positive and divides $|G|$, and that for each $1 \leq k \leq r$ we have $1 < |G : C_G(g_k)| < |G|$.

Proof. Consider the orbits of the conjugation action of G. There are two types:

- Orbits $\mathcal{O} = \{x\}$ of size 1. By the orbit/stabilizer theorem, $|G \cdot x| = 1$ iff $C_G(x) = G$, i.e., if and only if $x \in Z_G$.
- Orbits $\mathcal{O}$ of size ≥ 2. By the orbit/stabilizer theorem, $|\mathcal{O}| = |G : G_x|$ for any $x \in \mathcal{O}$.

Putting this together, if we pick representatives $g_1, \dots, g_r$ for distinct conjugacy classes not contained in the center, we get

$$|X| = \sum_{\substack{\text{orbits } \mathcal{O}, \\ |\mathcal{O}|=1}} |\mathcal{O}| + \sum_{\substack{\text{orbits } \mathcal{O}, \\ |\mathcal{O}|\geq 2}} |\mathcal{O}| = |Z_G| + \sum_{k=1}^{r} |G : C_G(g_k)|$$

□

A key feature of the class equation is the fact that each of its terms divides $|G|$.

Let p be a prime. A **p-group** is a non-trivial finite group whose order is a power of p. **p-group**

Proposition. *Every p-group has a non-trivial center.*

Proof. The class equation for G gives

$$p^d = |Z_G| + \sum_{k=1}^{r} |G : C_G(g_k)|,$$

with $d \geq 1$. Since $C_G(g_k) \neq G$, we have that p divides each $|G : C_G(g_k)|$. Therefore p divides $|Z_G|$. Since $|Z_G| \geq 1$ we conclude that p divides $|Z_G|$. □

Corollary. *If $|G| = p^2$ for some prime p, then G is abelian.*

Proof. First we note a general fact: if G/Z_G is cyclic, then G is abelian (and thus $G = Z_G$). To see this, pick $g \in G$ which projects to a generator of G/Z_G. Then every element in G can be written $g^k x$ for some $k \in \mathbb{Z}$ and $x \in Z_G$. Since $(g^i x)(g^j y) = g^{i+j} xy = (g^j y)(g^i x)$ whenever $x, y \in \mathbb{Z}_G$, we see that G is abelian.

If $|G| = p^2$, then by the previous result, $|Z_G| \in \{p, p^2\}$, whence $|G/Z_G| \in \{1, p\}$ and thus is cyclic..

□

26. Automorphism groups of groups

An **endomorphism** of a group is a homomorphism $\phi \colon G \to G$. **W 7 Sep**

An **automorphism** of a group G is an isomorphism $\phi \colon G \to G$. **endomorphism**

The collection $\mathrm{Aut}(G)$ of automorphisms is a subgroup of the permutation group $\mathrm{Sym}(G)$ of the underlying set of G. The collection $\mathrm{End}(G)$ of endomorphisms is not usually a group, but it is a monoid under composition of functions, and it contains $\mathrm{Aut}(G)$. I'll concentrate here on automorphisms, but endomorphisms can be interesting too. **automorphism**

Conjugation always gives an automorphism. Thus, we have a homomorphism

$$\mathrm{conj} \colon G \to \mathrm{Aut}(G).$$

The kernel is the center $Z_G \leq G$, while the image is the group

$$\mathrm{Inn}(G) := \{\, \mathrm{conj}_g \mid g \in G \,\} \leq \mathrm{Aut}(G)$$

of **inner automorphisms** of G. The first isomorphism theorem gives an isomorphism **inner automorphisms**

$$G/Z_G \approx \mathrm{Inn}(G).$$

Example (Automorphisms of D_6). Consider $D_6 = \langle r, s \mid r^3, s^2, (sr)^2 \rangle = \{e, r, r^2, s, sr, sr^2\}$. First, note that all endomorphisms $\phi\colon D_6 \to D_6$ can be constructed as follows: let $x, y \in D_6$ be elements such that

$$x^3 = e, \quad y^2 = e, \quad (yx)^2 = e.$$

Then there exists a unique endomorphism ϕ such that $\phi(r) = x$ and $\phi(s) = s$. This is immediate from the universal property of the free group and the homomorphism theorem:

$$\begin{tikzcd}
F(r,s) \arrow[r, "r\mapsto x,\ s\mapsto y"] \arrow[d, two heads, "\pi"'] & D_6 \\
\langle r, s \mid r^3, s^2, (sr)^2 \rangle \arrow[ur, dotted, "\phi"'] &
\end{tikzcd}$$

Furthermore, there is a necessary condition for ϕ to be an isomorphism: $\phi(g)$ and g must have the *same* order.

Thus, to find candidate automorphisms, we consider all pairs (x, y) where

$$x \in \{r, r^2\}, \qquad y \in \{s, sr, sr^2\}, \qquad \text{such that } (yx)^2 = e.$$

It turns out that all such pairs satisfy this, and so we get 6 endomorphisms, which are easily seen to be bijective.

Since $Z_{D_6} = \{e\}$, we know that $\operatorname{Inn}(D_6) \approx D_6$, so we conclude that $\operatorname{Aut}(D_6) \approx D_6$.

27. Outer automorphisms

Proposition. $\operatorname{Inn}(G)$ *is a normal subgroup of* $\operatorname{Aut}(G)$.

Proof. Let $\phi \in \operatorname{Aut}(G)$ and $g, x \in G$. We compute

$$\phi(\operatorname{conj}_g(\phi^{-1}(x))) = \phi(g\,\phi^{-1}(x)\,g^{-1}) = \phi(g)\phi(\phi^{-1}(x))\phi(g)^{-1} = \phi(g)\,x\,\phi(g)^{-1}.$$

That is,

$$\phi \circ \operatorname{conj}_g \circ \phi^{-1} = \operatorname{conj}_{\phi(g)}.$$

This implies that $\phi \operatorname{Inn}(G)\phi^{-1} \subseteq \operatorname{Inn}(G)$. Replacing ϕ with ϕ^{-1} gives $\phi^{-1}\operatorname{Inn}(G)\phi \subseteq \operatorname{Inn}(G)$, which is equivalent to $\operatorname{Inn}(G) \subseteq \phi \operatorname{Inn}(G)\phi^{-1}$. □

The quotient group is the group

$$\operatorname{Out}(G) := \operatorname{Aut}(G)/\operatorname{Inn}(G)$$

of **outer automorphisms**. Note that elements of $\operatorname{Out}(G)$ are not actually automorphisms, but equivalence classes of automorphisms. **outer automorphisms**

One way to construct non-inner automorphisms is to embed your group as a normal subgroup of a larger group. If $N \trianglelefteq G$, then we get a homomorphism of groups

$$\kappa\colon G \to \operatorname{Aut}(N), \qquad \kappa(g)(x) := gxg^{-1}.$$

The kernel of this is

$$\operatorname{Ker}(\kappa) = C_G(N) := \{\, g \in G \mid gn = ng\ \forall n \in N \,\},$$

the **centralizer** of the subgroup N, which is the collection of all elements of G which commute with elements of N. **centralizer**

Question? Which elements of G does κ send to an inner automorphism of N?

Proposition. *We have that*

$$\kappa^{-1}(\operatorname{Inn}(N)) := \{\, g \in G \mid \kappa(g) \in \operatorname{Inn}(N) \,\} = C_G(N)N,$$

which is a normal subgroup of G.

Proof. That $\kappa^{-1}(\mathrm{Inn}(N))$ is a normal subgroup is straightforward, e.g., by the fourth isomorphism theorem and the fact that $\mathrm{Inn}(N) \trianglelefteq \mathrm{Aut}(N)$.

To prove the equality, first note that if $z \in C_G(N)$, then $\kappa(z) = 1$, so $\kappa(C_G(N)N) \leq \mathrm{Inn}(N)$. Conversely, suppose $g \in G$ is such that $\kappa(g) \in \mathrm{Inn}(N)$. Then $\kappa(g) = \kappa(n)$ for some $n \in N$, and thus $\kappa(gn^{-1}) = 1$, so $gn^{-1} \in C_G(N)$ and thus $g \in C_G(N)n \subseteq C_G(N)N$. □

Therefore κ induces an injective homomorphism

$$\overline{\kappa}\colon G/C_G(N)N \rightarrowtail \mathrm{Out}(N).$$

So any elements of $G \smallsetminus C_G(N)N$ give rise to non-inner automorphisms of N.

Example (An outer automorphism of D_8). Let $G = D_{16} = \langle r, s \mid r^8, s^2, (sr)^2\rangle$. Let $N = \langle r^2, s\rangle \trianglelefteq G$, so that $N = \{e, r^2, r^4, r^6, s, sr^2, sr^4, sr^6\}$. If we set $R = r^2$ and $S = s$, it is straightforward to check that $N \approx \langle R, S \mid R^4, S^2, (RS)^2\rangle \approx D_8$.

Consider $\kappa\colon G \to \mathrm{Aut}(N)$. The kernel of this is $C_G(N) = \{e, r^4\}$, which is the center of G. To see this, note that this must be a subset of $C_G(s) = \{\, g \in G \mid gs = sg \,\}$, which has order $|G|/|\mathrm{Cl}(s)| = 4$, and thus is easily shown to be $\{e, r^4, s, sr^4\}$, and since $r^2 s \neq sr^2$ we see that $s \notin K$.

Clearly $C_G(N) \leq N$ in this example, so $G/C_G(N)N = G/N$ has order 2, generated by the image of r. Thus the automorphism $\psi \in \mathrm{Aut}(N)$ defined by $\psi(x) = rxr^{-1}$, which satisfies

$$\psi(R) = R, \qquad \psi(S) = SR^{-1},$$

is not an inner automorphism of $N \approx D_8$.

Example (Symmetric groups). Fix $n \geq 1$, and consider the conjugation function

$$\mathrm{conj}\colon S_n \to \mathrm{Aut}(S_n).$$

We know $\mathrm{Ker}(\mathrm{conj}) = Z_{S_n}$.

Claim. If $n \geq 3$, $Z_{S_n} = \{e\}$. *Proof.* Suppose $\sigma \in Z_{S_n}$. Then $\sigma g \sigma^{-1} = g$ for all $g \in S_n$. In particular, taking $g = (a\ b)$, we find that

$$(\sigma(a)\ \sigma(b)) = (a\ b),$$

which implies $\sigma(a) \in \{a, b\}$. If there is a $c \notin \{a, b\}$, the same argument gives $\sigma(a) \in \{a, c\}$, so $\sigma(a) = a$. As this works for all $a \in \{1, \dots, n\}$, we see $\sigma = \mathrm{id}$.

Thus for $n \geq 3$, $S_n \approx \mathrm{Inn}(S_n)$. It remains to determine $\mathrm{Out}(S_n)$.

Fact. We have that $\mathrm{Out}(S_n) \approx \{e\}$ for all $n \neq 6$, whereas $\mathrm{Out}(S_6)$ has order 2. (See for instance the wikipedia page on "Automorphisms of the symmetric and alternating groups". I will construct a non-inner automorphism of S_6 later.)

Example (Alternating groups). Let $G = S_n$ and $N = A_n$. If $n \geq 2$ we have $|G : N| = 2$, and you can show that $C_G(N) = \{e\}$ if $n \geq 3$. (For $n \geq 5$, you can use an argument similar to the one that shows $Z_G = \{e\}$, except by using 3-cycles instead of 2-cycles.) Thus $S_n/A_n \rightarrowtail \mathrm{Out}(A_n)$ provides a non-inner automorphism of A_n when $n \geq 3$ (which turns out to be the only one if $n \neq 6$).

28. Automorphisms of cyclic groups

If G is abelian, then $Z_G = G$ so $\mathrm{Inn}(G) = \{1\}$ and thus $\mathrm{Aut}(G) = \mathrm{Out}(G)$.

Example (Infinite cyclic group). Let $G = F(\{a\}) = \langle a \mid \varnothing\rangle$ be the infinite cyclic group, which is also the free group on one generator. There is a bijection

$$\mathbb{Z} \xrightarrow{\sim} \mathrm{End}(G), \qquad k \mapsto \phi_k := \big(a^j \mapsto a^{jk}\big).$$

This is easy to see using the universal property of free groups. Furthermore, we see that $\phi_i \circ \phi_j = \phi_{ij}$, since

$$\phi_i(\phi_j(a)) = \phi_i(a^j) = (a^i)^j = a^{ij} = \phi_{ij}(a).$$

Thus, $(\mathbb{Z}, \cdot) \approx \mathrm{End}(G)$ is an isomorphism of monoids, where the product on $\mathbb{Z}$ is defined by multiplication.

Thus $\phi_k \in \mathrm{End}(G)$ is an isomorphism if and only if k has a multiplicative inverse in $\mathbb{Z}$. Therefore we have an isomorphism of groups

$$\{\pm 1\} \approx \mathrm{Aut}(G).$$

Example (Finite cyclic group). Let $C_n = \langle a \mid a^n \rangle$ for some $n \geq 1$. There is a bijection

$$\mathbb{Z}/n \xrightarrow{\sim} \mathrm{End}(C_n), \qquad k \mapsto \phi_k := \big(a^j \mapsto a^{jk}\big).$$

Again, we can use the univesal property of free groups to prove this. Note that $\phi_k = \phi_{k+n}$ since $a^n = e$.

Furthermore, we have $\phi_i \circ \phi_j = \phi_{ij}$ as in the previous example. Thus, $(\mathbb{Z}/n, \cdot) \approx \mathrm{End}(G)$ is an isomorphism of monoids.

Therefore, we have an isomorphism of groups

$$(\mathbb{Z}/n)^\times \approx \mathrm{Aut}(C_n),$$

where $(\mathbb{Z}/n)^\times$ is the set of congruence classes mod n which has multiplicative inverses mod n, which is a group under multiplication.

$$\begin{aligned}
\mathrm{Aut}(C_2) &\approx (\mathbb{Z}/2)^\times = \{[1]\} \\
\mathrm{Aut}(C_3) &\approx (\mathbb{Z}/3)^\times = \{[1], [2]\} \\
\mathrm{Aut}(C_4) &\approx (\mathbb{Z}/4)^\times = \{[1], [3]\} \\
\mathrm{Aut}(C_5) &\approx (\mathbb{Z}/5)^\times = \{[1], [2], [3], [4]\}.
\end{aligned}$$

We have $|\mathrm{Aut}(C_n)| = \phi(n)$, where ϕ is the **Euler ϕ function**: **Euler ϕ function**

$$\phi(n) = \text{number of integers in } \{1, \dots, n\} \text{ which are relatively prime to } n.$$

Example. Let p be a prime, and let $G = \underbrace{C_p \times \cdots \times C_p}_{n \text{ copies}}$. Written additively, G is an n-dimensional vector space over the finite field $\mathbb{F}_p$ of p elements. You can show that

$$\mathrm{Aut}(G) \approx GL_n(\mathbb{F}_p).$$

A notable special case is the Klein 4-group:

$$\mathrm{Aut}(C_2 \times C_2) \approx GL_2(\mathbb{F}_2) \approx S_3.$$

I'll leave automorphisms of dihedral groups and the quaternion group as exercises.

29. Sylow theorems

Here is a discussion of the Sylow theorems. It is presented a little differently than the book does it (DF 4.5.)

Recall that a p-**group** is a finite group P of order p^k, $k \geq 1$, where p is a prime. **p-group**

A p-**Sylow subgroup** of finite group G is a subgroup $P \leq G$ which is a p-group, and is such that $|G : P|$ is prime to p. Equivalently, if $G = p^a m$ with $(p, m) = 1$ and $a \geq 1$, then a p-Sylow subgroup is a subgroup of order p^a. **p-Sylow subgroup**

Note. With this convention (following DF), the trivial subgroup is not p-Sylow, for any prime p.

Write $\mathrm{Syl}_p(G)$ for the set of p-Sylow subgroups of G, and write $n_p(G) := |\mathrm{Syl}_p(G)|$. Note that G acts on $\mathrm{Syl}_p(G)$ by conjugation: if $P \leq G$ is a p-Sylow subgroup, so is gPg^{-1} for any $g \in G$.

In the following three theorems, p will be a chosen prime, and G will be a finite group of order $p^a m$, where $a \geq 1$ and p does not divide m.

Theorem (Sylow 1)**.** *The group G has a p-Sylow subgroup; i.e.,* $\mathrm{Syl}_p(G) \neq \varnothing$.

Theorem (Sylow 2)**.** *Any two p-Sylow subgroups of G are conjugate; i.e., under the conjugation action, $\mathrm{Syl}_p(G)$ is a single G-orbit. In particular, a Sylow subgroup is normal iff it is the only one.*

Theorem (Sylow 3)**.** *If P is any p-Sylow subgroup of G, then $n_p = |G : N_G(P)|$. Furthermore, $n_p|m$ and $n_p \equiv 1 \mod p$.*

30. Applications of the Sylow theorems

A standard application of the Sylow theorems is to classify all groups of a given order, up to isomorphism. This works especially well if $|G|$ has a factorization into a small number of distinct primes. I'll give some partial results now. **F 9 Sep**

Groups of order pq.

Consider a group G of order pq, where $p < q$ are distinct primes. The Sylow theorems tell us that

$$n_p \mid q, \quad n_p \equiv 1 \pmod p, \qquad n_q \mid p, \quad n_q \equiv 1 \pmod q.$$

Since $q > p$, we must have $n_q = 1$. Furthermore, $n_p \in \{1, q\}$, and $n_p = q$ is only possible if $p \mid q - 1$.

Proposition. *If $p < q$ are primes and $q \not\equiv 1 \pmod p$, then every group of order pq is a cyclic group.*

Proof. Let $Q \trianglelefteq G$ be the unique subgroup of order q, which is a normal subgroup, and write $Q = \langle y \rangle$. Pick any subgroup $P \leq G$ of order p, and write $P = \langle x \rangle$. Consider the homomorphism

$$\kappa\colon P \to \mathrm{Aut}(Q), \qquad \kappa(p)(q) = pqp^{-1}.$$

We know $|\mathrm{Aut}(Q)| = |\mathrm{Aut}(C_q)| = q - 1$, and since $|P| = p$ we see that $\kappa(P) = \{e\}$. Therefore $pq = qp$ for all $p \in P$ and $q \in Q$. In particular $xy = yx$.

Let $z = xy$. If $z^k = e$, then $x^k = y^{-k}$, whence $x^k \in P \cap Q = \{e\}$, so $x^k = e = y^k$. Thus $|z| = pq$, and we see that G is cyclic. □

Example. The above applies to groups of order $15, 33, 35, 51, 65, 69, 77, 85, 87, 91, 95, \dots$, but not to groups of order $2q$ with q odd, or to groups of order $21, 39, 55, 57, 93, \dots$. In each of the cases where it does not apply, there exist non-abelian groups of that order, as we will see later.

Groups of order 30. I claim that if $|G| = 30$, then it contains a normal subgroup isomorphic to C_{15}, and in particular has unique 3- and 5-Sylow subgroups.

In fact, the Sylow theorems tell us that $n_5 \in \{1, 6\}$ and $n_3 \in \{1, 10\}$. If $n_5 = 6$ and $n_3 = 10$, then there must be $4 \cdot 6 = 24$ elements of order 5, and $2 \cdot 10 = 20$ elements of order 3, in G, which is too many. Thus, either $n_5 = 1$ or $n_3 = 1$.

Let P be a 5-Sylow subgroup and Q be a 3-Sylow subgroup. At least one of these is normal in G, and thus $PQ \leq G$. Since $|PQ| = 15$, it has index 2 in G and so $PQ \trianglelefteq G$. The Sylow theorems applied to PQ show that P and Q are the unique 5- and 3-Sylow subgroups in PQ. Therefore $\mathrm{Syl}_5(G) = \{P\}$ and $\mathrm{Syl}_3(G) = \{Q\}$.

Finally, $PQ \approx C_{15}$, as we have already shown that all groups of order 15 are cyclic.

Groups of order 12. Consider 3-Sylow subgroups. We have $n_3|4$ and $n_3 \equiv 1 \mod 3$, so either $n_3 = 1$ or $n_3 = 4$.

I claim that if G does not have a normal 3-Sylow subgroup, then $G \approx A_4$. In this case, $n_3 \neq 1$, so $n_3 = 4$. Remember that G acts on $\mathrm{Syl}_3(G)$ by conjugation, and thus we have a homomorphism

$$\phi\colon G \to \mathrm{Sym}(\mathrm{Syl}_3(G)) \approx S_4.$$

I will show that this is injective, so that G is isomorphic to a subgroup of order 12 of S_4.

If $P \in \mathrm{Syl}_3(G)$, then $|G : N_G(P)| = n_3 = 4$, whence $|N_G(P)| = 3$ so $P = N_G(P)$. The kernel of ϕ consists of elements which normalize *all* 3-Sylow subgroups, and so are in the intersection of all 3-Sylow subgroups. This implies $\mathrm{Ker}\,\phi = \{1\}$, so ϕ is injective, as desired.

It remains to show that $\phi(G) = A_4$, which can be done in a number of ways. For instance, G must contain exactly 8 elements of order 3 (which are the non-identity elements of the four 3-Sylow subgroups), while there are exactly 8 elements of order 3 in S_4, and they generate A_4.

It remains to understand the cases which have a normal 3-Sylow subgroup. We do this later.

Groups of order 60. I claim that if $|G| = 60$ and $n_5 > 1$, then G is simple. This gives another proof that the icosahedral group (and A_5) is simple. (Note that A_5 clearly contains distinct subgroups of order 5.)

By the Sylow theorems, we have $n_5 \in \{1, 6\}$, so the hypothesis implies $n_5 = 6$.

Let H be a non-trivial proper normal subgroup of G; we will show such a thing cannot exist, on a case-by-case basis depending on $|H|$. We will use the fact that since H is normal, if it contains a p-Sylow subgroup, then it contains every p-Sylow subgroup in G.

If $5 \mid |H|$, then H contains a 5-Sylow subgroup; being normal, it must contain every 5-Sylow subgroup of G. Thus $|H| \geq 1 + 4 \cdot 6 = 24$, so $|H| = 30$. But we have shown that any group of order 30 has a unique 5-Sylow, so this is not possible.

If $5 \nmid |H|$, so that $|H| \mid 12$, I claim that G must contain a normal subgroup K of order 2, 3, or 4. If H does not have one of these orders, then $|H| = 6$ or 12, so that H has a normal Sylow subgroup (using the argument given above for $|H| = 12$). This Sylow subgroup K of H must also be a normal subgroup of G, since for all $g \in G$, $gHg^{-1} = H$, and thus $gKg^{-1} \leq H$, so that $gKg^{-1} = K$ since P is the unique subgroup of H of its order. Since $|K|$ must be 2, 3, or 4, this proves the claim.

Now G/K has order 15, 20, or 30. In each case, G/K has a normal 5-Sylow subgroup (the first two cases by the Sylow theorem, the last by the case of groups of order 30 discussed above). The preimage of such a 5-Sylow will be a normal subgroup of G with order divisible by 5, contradicting the above.

31. Proof of Sylow 1

Proof of Sylow 1. This proof is by induction on $|G|$. The base case is $|G| = p$, in which case G is its own p-Sylow subgroup.

Suppose $|G| = p^a m > p$ with $a \geq 1$, and we've proved the theorem for subgroups of smaller order.

Claim. Either

(a) G has a proper subgroup $H \leq G$ of index not divisible by p, or
(b) G has a non-trivial normal subgroup $N \trianglelefteq G$ of order p.

If (a) is true, then by induction H has a p-Sylow subgroup, which is automatically a p-Sylow subgroup of G since p does not divide $|G : H|$. If (b) is true, then either $a = 1$, so that N is the desired p-Sylow subgroup, or $a > 1$ and thus G/N has a p-Sylow subgroup Q by induction. Since $|G/N| = p^{a-1}m$, we see Q has index m in G/N. Let $P = \{\, g \in G \mid gN \in Q \,\}$ be the preimage of P in G. We have that $G/P \approx (G/N)/Q$, so P has index m in G, so is a p-Sylow subgroup.

Proof of Claim. Consider the class equation:

$$p^a m = |G| = |Z(G)| + \sum |G : C_G(g_i)|,$$

where each $[G : C_G(g_i)] > 1$. Thus, if (a) is false, then p divides each $|G : C_G(g_i)|$, and so $|Z(G)|$ is divisible by p. We have shown (Cauchy's theorem) that any group of order divisible by p has an element x of order p, and thus $N = \langle x \rangle \trianglelefteq G$ is desired subgroup, which is normal because it is contained in the center. □

32. Alternate proof of Sylow 1

Here is another proof of the first Sylow theorem.

Alternate proof of Sylow 1. We will show that if $|G| = p^a m$ with $m > 1$, then G admits a *proper* subgroup whose index is not divisible by p; the theorem then follows by an induction on the order of the group. We will accomplish this by producing an action of G on a finite set X such that

(a) $|X|$ is not divisible by p, and
(b) the action of G on X has no fixed points.

Then orbit decomposition then gives

$$|X| = \sum |G : G_{x_i}|$$

where $|G : G_{x_i}| > 1$ since there are no fixed points. Since $|X|$ is not divisible by p, at least one of the $|G : G_{x_i}|$ will not be divisible by p, proving the claim.

Let $X := \{ S \subseteq G \mid |S| = p^a \}$, the set of all subsets of G of order p^a. Note that

$$|X| = \binom{p^a m}{p^a} \equiv m \mod p.$$

(This can proved using the observation that $(x+y)^{p^a m} \equiv (x^{p^a} + y^{p^a})^m$ modulo p.) Thus, $|X|$ is not divisible by p, giving condition (a).

We can make G act on X by left multiplication, so that $gS := \{ gs \mid s \in S \}$. I claim that if $m > 1$ then this action has no fixed point. In fact, if S is a fixed point of the action, choose any $s \in S$ and note that for all $g \in G$ we have that $g = gs^{-1}s \in gs^{-1}S = S$. That is, if S is fixed point then $G \subseteq S$, which is impossible if $m > 1$. This proves condition (b). □

33. Proof of Sylow 2

For Sylow 2, we use the following important fact, which gives us an explicit criterion for a subgroup of a group to have a conjugate contained in another subgroup.

Lemma. *Let G be any group, and let $H, K \leq G$ be subgroups. Then there exists $x \in G$ such that $K \subseteq xHx^{-1}$ if and only if the left action of K on G/H has a fixed point.*

Proof. Suppose xH is a fixed point of the action of K on G/H. This means that for all $k \in K$, we have

$$kxH = xH \qquad \text{whence} \qquad Kx \subseteq KxH = xH.$$

Since $Kx \subseteq xH$ we have $K \subseteq xHx^{-1}$.

Conversely, if $K \subseteq xHx^{-1}$ for some x, then $Kx \subseteq xH$ and hence $k(xH) = xH$ for all $k \in K$. □

Note that we can also write the conclusion as $x^{-1}Kx \subseteq H$, and that if $|H| = |K| < \infty$ it means K and H are conjugate subgroups.

Proof of Sylow 2. Let $P, Q \in \mathrm{Syl}_p(G)$. We have $|G/P| = m$, which is not divisible by p. Consider the left action of Q on G/P; the set G/P must be a disjoint union of orbits of the Q-action, so we have

$$m = |G/P| = c + \sum_{k=1}^{r} |O_k|,$$

where c is the number of fixed points of the action, and each orbit O_k has size bigger than one. Since $|O_k|$ divides $|Q| = p^a$, this means p divides $|O_k|$ for $k = 1, \ldots, r$. Thus $m \equiv c \mod p$, and therefore $c \neq 0$, and by the lemma it follows that Q is conjugate to P. □

This proves more.

Proposition. *If $P \leq G$ is a p-Sylow subgroup, and $Q \leq G$ any subgroup of order a power of p, then Q is conjugate to a subgroup of P. In particular, any p-group of G is contained in a p-Sylow subgroup.*

The proposition is also proved by showing that the action of Q on G/P has a fixed point, in the same way.

As a consequence we get the following.

Corollary. *For a finite group G with $p \mid |G|$, we have*

$$\{\, g \in G \mid \exists k \geq 0,\ \ |g| = p^k \,\} \;=\; \bigcup_{P \in \mathrm{Syl}_p(G)} P.$$

That is, the subset of elements with p-power order is equal to the union of all p-Sylow subgroups.

34. Proof of Sylow 3

Proof of Sylow 3. The group G acts on $\mathrm{Syl}_p(G)$, so that $g \in G$ sends $P \mapsto gPg^{-1}$. By (2), this action transitive, and it is clear that the stabilizer group of $P \in \mathrm{Syl}_p(G)$ is $N_G(P)$. Thus $n_p = |G : N_G(P)|$ for any $P \in \mathrm{Syl}_p(G)$. Since $P \leq N_G(P)$, it follows that $n_p = |G : N_G(P)|$ divides $|G : P| = m$.

For the congruence result, we examine the action of P on the set $\mathrm{Syl}_p(G)$, which is the restriction of the action of G described above. The P-set $\mathrm{Syl}_p(G)$ will be disjoint union of orbits, and we have

$$n_p = |\mathrm{Syl}_p(G)| = c + \sum_{k=1}^{r} |O_k|$$

where the sum is over the P-orbits $O_1, \dots, O_r$ of size bigger than 1, and c is the number of P-fixed points. As above, each $|O_k|$ must be divisible by p, whence $n_p \equiv c \mod p$.

It remains to show that $c = 1$. It is clear that $P \in \mathrm{Syl}_p(G)$ is fixed under the action of conjugation by P, so we only need to show there are no other p-Sylow subgroups fixed by P-conjugation.

Suppose $Q \in \mathrm{Syl}_p(G)$ is fixed under conjugation by P; i.e., $pQp^{-1} = Q$ for all $p \in P$, which means that $P \leq N_G(Q)$. The groups P and Q must be p-Sylow subgroups of $N_G(Q)$, since $|N_G(Q)|$ divides $|G|$. But all p-Sylow subgroups of $N_G(Q)$ must be conjugate, and since Q is normal in $N_G(Q)$, it follows that $P = Q$. □

35. An outer automorphism of S_6

I want to describe a construction of a non-inner automorphism of S_6. First, let's figure out how we can tell whether an automorphism $\phi \in \mathrm{Aut}(S_n)$ is inner or not. **M 12 Sep**

For each $k = 1, \dots, n$, we have a subgroup

$$F_k := \{\, g \in S_n \mid g(k) = k \,\} = \mathrm{Stab}(k),$$

the stabilizer subgroup of the element $k \in \{1, \dots, n\}$ for the tautological action of S_n on this set. Note the following.

(1) The subgroups $F_1, \dots, F_n \leq S_n$ are pairwise distinct, as long as $n \geq 3$. (There is always a permutation which fixes k but does not fix any other element.)

(2) There is an isomorphism of groups $F_n \approx S_{n-1}$. This is easy to see: any $\sigma \in F_n$ restricts to a permutation of the subset $\{1, \dots, n-1\}$, and conversely any $\sigma \in S_{n-1}$ can be extended to an element of F_n by setting $\sigma(n) = n$.

(3) The subgroups $F_1, \dots, F_n$ are all conjugate to each other. In fact, we have the following formula:
$$gF_kg^{-1} = F_{g(k)}, \qquad k \in \{1, \dots, n\}, \quad g \in S_n.$$
This is immediate to verify: if $\sigma(k) = k$, then $g\sigma g^{-1}(g(k)) = g(k)$, so $gF_kg^{-1} \subseteq F_{g(k)}$, and the same argument shows $g^{-1}F_{g(k)}g \subseteq F_k$. (Really, it's because $F_k = \mathrm{Stab}(k)$, and $g\,\mathrm{Stab}(k)g^{-1} = \mathrm{Stab}(gk)$.)

(4) Thus, all the F_k are isomorphic to S_{n-1}, so $|S_n : F_k| = n$.

Proposition. *An automorphism $\phi \in \mathrm{Aut}(S_n)$ is inner iff $\phi(F_n) \in \{F_1, \dots, F_n\}$.*

Proof. $\Longrightarrow$: If ϕ is inner then $\phi = \mathrm{conj}_g$ for some $g \in S_n$, and we have already shown $\phi(F_n) = gF_ng^{-1} = F_{g(n)}$.

$\Longleftarrow$: First note that if $H, H' \leq S_n$ are conjugate subgroups, then $\phi(H), \phi(H')$ are conjugate, since $\phi(gHg^{-1}) = \phi(g)\phi(H)\phi(g^{-1})$. Since the F_ks are all conjugate to each other, the hypothesis implies that ϕ actually permutes the set $\{F_1, \dots, F_n\}$ of subgroups.

We can identify the permutation of $\{F_1, \dots, F_n\}$ given by ϕ with a permutation σ of $\{1, \dots, n\}$, by the formula

$$\phi(F_k) = F_{\sigma(k)}, \qquad k \in \{1, \dots, n\}.$$

I now show that $\phi = \mathrm{conj}_\sigma$. It suffices to show that $\psi := \mathrm{conj}_{\sigma^{-1}} \circ \phi$ is the identity automorphism. We have

$$\psi(F_k) = \sigma^{-1} F_{\sigma(k)} \sigma = F_k \qquad \text{for all } k.$$

Since S_n is generated by transpositions, it suffices to show that $\psi((a\ b)) = (a\ b)$ for any transposition $(a\ b) \in S_n$.

Let's show that $\psi((1\ 2)) = (1\ 2)$. Observe that

$$F_3 \cap \dots \cap F_n = \{\, g \in S_n \mid g(k) = k \text{ for all } 3 \leq n \,\} = \{e,\ (1\ 2)\}.$$

Since $\psi(F_k) = F_k$ for all k, ψ must take this intersection to itself, so ψ must fix $(1\ 2)$. Replace the intersection with $\bigcap_{\substack{k=1,\dots,n \\ k \neq a,b}} F_k$ to show ψ fixes $(a\ b)$. □

Proposition. *If $H \leq S_n$ such that $|S_n : H| = n$, then there exists $\phi \in \mathrm{Aut}(S_n)$ such that $\phi(H) = F_n$. If $H \notin \{F_1, \dots, F_n\}$ then ϕ is not an inner homomorphism.*

Proof. Let $x_1H, \dots, x_nH$ denote the n distinct left cosets of H in S_n, with $x_1, \dots, x_n \in S_n$. Assume that $e \in x_nH$. (In fact, we can assume $x_n = e$.)

Any $g \in S_n$ gives a permutation of the set $G/H = \{x_1H, \dots, x_nH\}$ of the set of left-H cosets, where $g \cdot xH = (gx)H$. Thus there exists a unique permutation $\phi(g) \in S_n$ satsifying the formula

$$gx_kH = x_{\phi(g)(k)}H, \qquad k = 1, \dots, n.$$

Thus we have a function $\phi\colon S_n \to S_n$. I claim ϕ is a group homomorphism: if $g, g' \in S_n$, then

$$g(g'x_kH) = g(g'x_kH) = gx_{\phi(g')(k)}H = x_{\phi(g)(\phi(g'))(k)}H,$$

which is also $(gg')x_kH = x_{\phi(gg')(k)}H$, and thus

$$\phi(gg') = \phi(g)\phi(g').$$

The kernel of ϕ is

$$\mathrm{Ker}(\phi) = \{\, g \in S_n \mid gxH = xH \text{ for all } x \in S_n \,\} = \bigcap_{x \in S_n} xHx^{-1}.$$

This is a normal subgroup of S_n, and also a subgroup of H, so $\mathrm{Ker}(\phi) \mid H = (n-1)!$. When $n \neq 4$ the only normal subgroups of S_n are $\{\{e\}, A_n, S_n\}$ so we must have $\mathrm{Ker}(\phi) = \{e\}$. (When $n = 4$ there is also a normal subgroup $V \trianglelefteq S_4$ with $|V| = 4$, but $4 \nmid 3!$ so this doesn't work either.)

Thus ϕ is injective, and therefore is a bijection since it is a self-map of a finite set. Note that $\phi(H) \subseteq F_n$, since if $g \in H$ then $x_nH = gx_nH = x_{\phi(g)(n)}H$ because $x_nH = H$, and so $\phi(g)(n) = n$, i.e., $\phi(g) \in F_n$. Since ϕ is a bijection we have $\phi(H) = F_n$.

If $H \notin \{F_1, \dots, F_n\}$ then clearly ϕ does not permute this collection of subgroups, so is not an inner automorphism of S_n. □

Exercise. The above argument implies the following: the group $\mathrm{Out}(S_n)$ acts freely and transitively on the set X of *conjugacy classes of index n subgroups of S_n*. In particular, $|\mathrm{Out}(S_n)| = |X|$. Prove this.

Now I'm going to produce a subgroup $H \leq S_6$ of index 6 which does not fix any $k \in \{1, \dots, 6\}$, so $H \neq F_k$ for any k.

Consider the 5-Sylow subgroups of S_5. Each 5-Sylow subgroup P has order 5, generated by some 5-cycle permutation. It is not hard to show that there are exactly 6 such 5-Sylow subgroups. (For instance, there are exactly $5!/5 = 24$ 5-cycles in S_5, and there are exactly 4 in each 5-Sylow subgroup, whose pairwise intersections must be the trivial group. Or compute that $|N_{S_5}(P)| = 20$ where $P = \langle (1\ 2\ 3\ 4\ 5) \rangle$, whence $n_5 = 120/20 = 6$.)

Label these 5-Sylow subgroups as $P_1, \dots, P_6$. Conjugation by elements of S_5 permutes the set $\{P_1, \dots, P_6\}$ transitively. Thus for each $h \in S_5$ we get an element $\alpha(h) \in S_6$ by the formula

$$hP_kh^{-1} = P_{\alpha(h)(k)}, \qquad k = 1, \dots, 6.$$

This defines a homomorphism $\alpha\colon S_5 \to S_6$. We have $\mathrm{Ker}(\alpha) = \bigcap_{k=1}^{6} N_{S_5}(P_k)$, which is a normal subgroup of index ≥ 6, and thus is trivial.

Thus we obtain a subgroup $H = \alpha(S_5) \leq S_6$ of index 6. It is not contained in any F_k: we have $\alpha(h) \in F_k$ if and only if $hP_kh^{-1} = P_k$, but we know that S_5 acts *transitively* on the set of Sylow subgroups, so there must exist an $h \in H$ such that $\alpha(h) \notin F_k$.

We have thus constructed a non-inner automorphism ϕ of S_6. Explicitly, we pick:

- a labelling $P_1, \dots, P_6$ of the 5-Sylow subgroups of S_5, which determines a subgroup $H = \alpha(S_5) \leq S_6$, where $\alpha\colon S_5 \rightarrowtail S_6$ is defined by $hP_kh^{-1} = P_{\alpha(h)(k)}$, and
- a labelling $x_1, \dots, x_6H$ of the left-H-cosets in S_6, which determines a function $\phi\colon S_6 \to S_6$ defined by $gx_kH = x_{\phi(g)(k)}$. Then ϕ is a non-inner automorphism of S_6.

36. Finitely generated groups

A group G is **finitely generated** if there exists a finite subset $S \subseteq G$ such that $G = \langle S \rangle$. This implies that every element of G can be written as a word in S. **finitely generated**

Obvious examples.

- Every finite group is finitely generated: take $G = S$.
- If S is a finite set, then the free group $F(S)$ is finitely generated.
- If $G \approx H$, then G is finitely generated iff H is.
- If G is finitely generated, then so is any quotient group G/N.

Warning. If $S \subseteq G$ is an infinite subset, and $G = \langle S \rangle$, it does not follow that G is not finitely generated, since there could be a more efficient generating set. We do have the following.

Proposition. *Let $F = F(S)$ be the free group on a set S. Then F is finitely generated if and only if S is finite.*

Proof. It is immediate that $|S| < \infty$ means $F(S)$ is finitely generated.

For the converse, we make use of the fact that elements of F are precisely the reduced words on the set of symbols S. In particular, because each $x \in F$ is a reduced word of finite length, the symbols which appear in the word are a *finite* subset $S_x \subseteq S$ of all symbols.

Thus if $\{x_1, \dots, x_n\} \subseteq F$ is a finite generating set for F, then every element of F can be written as a product elements from $T \cup T^{-1}$, where $T = S_{x_1} \cup \cdots \cup S_{x_n}$. That is, every element of F can be expressed as a reduced word in symbols from T, which implies $T \leq S$. □

An obvious question: is any subgroup of a finitely generated group also finitely generated? The answer is no.

Example. Let $G = F(a, b)$, the free group on two generators. Write $x_n := a^nba^{-n} \in G$, and let $H = \langle x_n,\ n \in \mathbb{Z} \rangle \leq G$. Then H is not finitely generated. (Remark: H is a normal subgroup of G, and $G/H \approx \langle a, b \mid b \rangle \approx F(a)$.)

To prove this, let S be the set of symbols $\{\, X_n \mid n \in \mathbb{Z} \,\}$, and define the homomorphism

$$\phi\colon F(S) \to G, \qquad X_n \mapsto x_n.$$

I claim ϕ is injective and thus induces an isomorphism $F(S) \approx H$, and therefore H is not finitely generated since $F(S)$ is not.

Here is the idea. An element of $F(S)$ is a reduced word in the X_is:

$$X_{k_1}^{c_1} X_{k_2}^{c_2} \cdots X_{k_r}^{c_r}, \qquad r \geq 0, \quad k_i \in \mathbb{Z}, \quad c_i \in \{\pm 1\}, \quad k_i = k_{i+1} \implies c_i = c_{i+1}.$$

Then ϕ sends this to

$$a^{k_1} b^{c_1} a^{-k_1+k_2} b^{c_2} a^{-k_2+k_3} b^{c_3} \cdots b^{c_{r-1}} a^{-k_{r-1}+k_r} b^{c_r} a^{-k_r} \in G,$$

and this expresses the element as a reduced word in $\{a, b\}$: cancellation can occur only if $k_i = k_{i+1}$ and $c_i = -c_{i+1}$ for some i, but this is excluded by the condition that $X_{k_1}^{c_1} \cdots X_{k_r}^{c_r}$ is a reduced word. (More generally, whenever $k_i = k_{i+1} = \cdots = k_{i+j}$ we have $c_i = \cdots = c_{i+j}$, so $b^{c_i} a^{-k_i+k_{i+1}} \cdots a^{-k_{i+j-1}+k_{i+j}} b^{c_{i+j}}$ reduces to $b^{j c_i}$.)

Remark. Our subgroup of a free group is also a free group. The Nielsen-Schreier Theorem (which I won't prove) asserts that *every* subgroup of a free group is a free group.

37. The ascending chain condition for groups

It is the case that subgroups of finitely generated *abelian* groups are finitely generated. I will prove this here.

A partially ordered set $(P, \leq)$ has the **ascending chain condition (acc)** if for every countable sequence $\{x_k\}_{k \in \mathbb{N}}$ with $x_k \leq x_{k+1}$, there exists m such that $x_k = x_m$ for all $k \geq m$.

ascending chain condition (acc)

Note that the acc fails for P iff there exists a countable strictly increasing sequence in P, i.e., one of the form $x_1 < x_2 < x_3 < \cdots$.

A group G has the **ascending chain condition for subgroups** if the set of subgroups ordered by $\subseteq$ has the acc.

ascending chain condition for subgroups

Proposition. *The following are equivalent.*

(1) *G has the acc for subgroups.*
(2) *All subgroups are of G are finitely generated.*

Proof. (1) $\implies$ (2). I'll prove the converse. Suppose $H \leq G$ with H not finitely generated. Then we can inductively choose $x_k \in H$ for $k \geq 1$ so that $x_{k+1} \notin H_k := \langle x_1, \ldots, x_{k-1} \rangle$. Then we get a chain of subgroups in G of the form

$$H_1 < H_2 < \cdots$$

whence G does not have the acc for subgroups.

(2) $\implies$ (1). Consider $H_1 \leq H_2 \leq \cdots \leq G$. The union $H := \bigcup_{k=1}^{\infty} H_k$ is also a subgroup of G (since any finite subset of H is actually a subset of some H_k, so H must be closed under products and inverses). By hypothesis $H = \langle x_1, \ldots, x_n \rangle$ for some $x_1, \ldots, x_n \in H$. Since H is a union, each $x_i \in H_{k_i}$ for some k_i. Let $m = \max(k_1, \ldots, k_n)$, whence $x_1, \ldots, x_n \in H_k$ so $H_m = H$, and therefore $H_k = H_m$ for all $k \geq m$. □

We have the following to help prove that a group has the acc for subgroups.

Proposition. *Let $N \trianglelefteq G$. The following are equivalent.*

(1) *G has the acc for subgroups.*
(2) *Both N and G/N have the acc for subgroups.*

Proof. (1) $\implies$ (2). It is immediate that N has the acc for subgroups. If $K_1 \leq K_2 \leq \cdots \leq G/N$ is a chain of subgroups, consider the chain of preimages $\pi^{-1}K_1 \leq \pi^{-1}K_2 \leq \cdots \leq G$ and apply the acc for subgroups of G.

(2) $\implies$ (1). Suppose $H_1 \leq H_2 \leq \cdots \leq G$. We obtain chains of subgroups

$$H_1 \cap N \leq H_2 \cap N \leq \cdots \leq N,$$

and

$$H_1N/N \leq H_2N/N \leq \cdots \leq G/N.$$

The hypothesis implies there exists m such that $H_m \cap N = H_k \cap N$ and $H_mN/N = H_kN/N$ for all $k \geq m$. From this we deduce that $H_m = H_k$ when $k \geq m$. (If $x \in H_k$ for some $k \geq m$, then $H_mN/N = H_kN/N$ implies $x = yn$ for some $y \in H_m$, $n \in N$, whence $y^{-1}x \in H_k \cap N = H_m \cap N$, whence $x = y(y^{-1}x) \in H_m$ as desired.) □

Thus, all subgroups of G are finitely generated iff the same is true for both N and G/N.

38. Subgroups of finitely generated abelian groups

Proposition. *Every finitely generated abelian group has the acc for subgroups. Thus, every subgroup of a finitely generated abelian group is finitely generated.* **W 14 Sep**

Proof. We show that if G is an abelian group which admits a generating set of size n, then G has the acc for subgroups, and we use induction on n.

$n = 0$: Then $G = \{e\}$, and the claim is immediate.

$n = 1$: Then G is a cyclic group. We know that all subgroups of cyclic groups are cyclic, and thus finitely generated, and therefore G has the acc for subgroups.

$n \geq 2$: Suppose $G = \langle x_1, \ldots, x_n\rangle$, and let $H = \langle x_1, \ldots, x_{n-1}\rangle$. Then H has the acc for subgroups by induction, as does G/H since it is cyclic (generated by x_nH). The claim follows from the previous proposition. □

Remark. In the above proof, we needed G to be abelian so that every subgroup is normal.

Remark. A group with the property that every subgroup is normal is called a *Dedekind group*, and a non-abelian one is also called a *Hamiltonian group.* There is a complete classification of these, which you can easily find online.

39. Torsion in abelian groups

Let G be group. I'll say that an element $a \in G$ is **torsion** if it has finite order, and write $G_{\text{tors}} \subseteq G$ for the subset of torsion elements. **torsion**

Proposition. *If G is an abelian group, then G_{tors} is a subgroup of G.*

Proof. Clearly $e \in G_{\text{tors}}$. If x has finite order n, then so does x^{-1}, so $x \in G_{\text{tors}}$ implies $x^{-1} \in G_{\text{tors}}$. Finally, suppose $x, y \in G_{\text{tors}}$ with $|x| = m$ and $|y| = n$. Then

$$(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = e,$$

so xy has finite order (dividing mn). □

Remark. This fails when G is not abelian. For instance, consider $a, b \in \mathrm{Sym}(\mathbb{R})$ defined by $a(x) = -x$, $b(x) = -x + 1$. Then you can easily compute that

$$a \circ a = \mathrm{id}, \qquad b \circ b = \mathrm{id}, \qquad ba(x) = x + 1,$$

whence ba has infinite order. (The subgroup generated by $\{a, b\}$ is the infinite dihedral group.)

A group G is **torsion** if $G_{\text{tors}} = G$, i.e., every element has finite order. Clearly every finite group is torsion, but infinite torsion groups also exist. **torsion**

Remark. The notion of "torsion group" is usually reserved for abelian groups only. Group theorists refer to (possibly nonabelian) groups such that every element is torsion as **periodic groups**. I won't use this terminology however.

periodic groups

Example. Consider the additive group $G := \mathbb{Q}/\mathbb{Z}$. This is a countably infinite group, since we can choose a unique representative of $x + \mathbb{Z}$ for each coset with $x \in \mathbb{Q} \cap [0, 1)$. However, it is a torsion group: if $x \in \mathbb{Q}$ then $x = a/b$ for some $a, b \in \mathbb{Z}$ with $b > 0$, and clearly $bx = 0$, so the order of x divides b.

A group G is **torsion free** if $G_{\text{tors}} = \{e\}$, i.e., if the identity element is the only element of finite order.

torsion free

Proposition. *If G is abelian, then G/G_{tors} is torsion free.*

Proof. Suppose $xG_{\text{tors}} \in G/G_{\text{tors}}$ is an element of finite order n. Then $x^n \in G_{\text{tors}}$, and therefore x^n has some finite order m, whence $x^{mn} = (x^n)^m = e$ in G. But this implies that $x \in G_{\text{tors}}$, and thus $xG_{\text{tors}} = eG_{\text{tors}}$. □

Proposition. *Every finitely generated torsion abelian group is finite.*

Proof. Suppose $G = \langle a_1, \ldots, a_n \rangle$. Since G is torsion, each a_k has finite order $|a_k| = m_k$. Since G is abelian, we have $a_i a_j = a_j a_i$ for all $1 \leq i, j \leq n$. Thus any element of G can be written as $g = a_1^{k_1} \cdots a_n^{k_n}$ with each $k_i \in \{0, \ldots, m_i - 1\}$. □

Proposition. *The additive groups $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are not finitely generated.*

Proof. If $\mathbb{Q}$ is finitely generated, so is the quotient group $\mathbb{Q}/\mathbb{Z}$. Since $\mathbb{Q}/\mathbb{Z}$ is torsion, if it is finitely generated it would therefore be finite, but we know it is not. □

Remark. Here is another proof that $\mathbb{Q}$ is not finitely generated: it doesn't have the acc for subgroups. For instance:

$$\mathbb{Z} \subsetneq \mathbb{Z}\tfrac{1}{2} \subsetneq \mathbb{Z}\tfrac{1}{2^2} \subsetneq \mathbb{Z}\tfrac{1}{2^3} \subsetneq \cdots .$$

Remark. The group $\mathbb{Q}/\mathbb{Z}$ is a union of finite cyclic subgroups $G_n := \mathbb{Z}\frac{1}{n}/\mathbb{Z}$. For any prime p, the union $\bigcup_{k \geq 0} G_{p^k}$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$. It is isomorphic to

$$p^{-1}\mathbb{Z}/\mathbb{Z}, \qquad p^{-1}\mathbb{Z} = \{\, a/p^k \mid a \in \mathbb{Z},\ k \geq 0 \,\}.$$

Note that the exponential map $x \mapsto e^{2\pi i x}$ defines an isomorphism between $\mathbb{Q}/\mathbb{Z}$ and a subgroup of $\mathbb{C}^\times$. The image is in fact the torsion subgroup of $\mathbb{C}^\times$, called the group of *roots of unity* in $\mathbb{C}$.

40. Products of groups

Given groups $G_1, \ldots, G_n$, their **direct product**, or just **product**, is

direct product
product

$$G := G_1 \times \cdots \times G_n = \{\, (g_1, \ldots, g_n) \mid g_i \in G_i \,\},$$

with multiplication defined by

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := (x_1 y_1, \ldots, x_n y_n).$$

It is straightforward to verify the group axioms. The identity element is $e = (e, \ldots, e)$, and inverses are $(x_1, \ldots, x_n)^{-1} = (x_1^{-1}, \ldots, x_n^{-1})$.

This comes with **projection homomorphisms**

projection homomorphisms

$$\pi_k \colon G \to G_k, \qquad \pi_k(x_1, \ldots, x_n) := x_k.$$

There is a straightforward recipe for describing homomorphisms *into* a product.

Proposition. *Let H and $G = G_1 \times \cdots \times G_n$ be groups. There is a bijection*

$$\operatorname{Hom}(H, G) \xrightarrow{\sim} \operatorname{Hom}(H, G_1) \times \cdots \times \operatorname{Hom}(H, G_n),$$

defined by $\phi \mapsto (\pi_1 \circ \phi, \dots, \pi_n \circ \phi)$. The inverse of this bijection sends a tuple $(\phi_k \colon H \to G_k)_{k=1}^n$ to $\phi \colon H \to G$ defined by $\phi(h) = (\phi_1(h), \dots, \phi_n(h))$.

Proof. Straightforward. □

Example. The "Klein 4-group" is isomorphic to $C_2 \times C_2$.

Given such a product $G = G_1 \times \cdots \times G_n$, let

$$G'_k = \{\, (g_1, \dots, g_k, \dots, g_n) \mid g_j = e \text{ if } j \neq k \,\},$$

the kth "coordinate axis" in G. It is straightforword to check that G'_k is a subgroup of the product, and that the function

$$G_k \to G'_k, \qquad x \mapsto (e, \dots, x, \dots, e) \qquad (k\text{th entry}),$$

is an isomorphism of groups. Furthermore, if $x_i \in G'_i$ and $x_j \in G'_j$ with $i \neq j$, then we have $x_i x_j = x_j x_i$. (*Warning:* This is not so if $i = j$. The G_i need not be abelian.)

41. Recognizing products of groups

Proposition. *Let G be a group, and suppose $G_1, \dots, G_n \trianglelefteq G$ are* normal *subgroups such that*

(1) *$G_1 \cdots G_n = G$, and*
(2) *$G_k \cap (G_1 \cdots G_{k-1}) = \{e\}$ for $k = 2, \dots, n$.*

Then the function

$$\phi \colon G_1 \times \cdots \times G_n \to G, \qquad (g_1, \dots, g_n) \mapsto g_1 \cdots g_n$$

is an isomorphism of groups.

Proof. First note that if $i < j$ then $G_i \subseteq G_1 \cdots G_{j-1}$, so condition (2) implies that $G_i \cap G_j = \{e\}$ for any $i < j$.

To show that ϕ is a homorphism, we must show that for $x_k, y_k \in G_k$, $k = 1, \dots, n$, we have

$$(x_1 y_1) \cdots (x_n y_n) = (x_1 \cdots x_n) \cdot (y_1 \cdots y_n)$$

This will follow if we can show that elements from distinct factors commute, i.e., if $xy = yx$ whenever $x \in G_i$, $y \in G_j$, and $i \neq j$. Note that

$$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in G_j G_j = G_j \qquad \text{because } G_j \trianglelefteq G,$$

and

$$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in G_i G_i = G_i \qquad \text{because } G_i \trianglelefteq G.$$

Therefore $xyx^{-1}y^{-1} \in G_i \cap G_j = \{e\}$, so $xyx^{-1}y^{-1} = e$, i.e., $xy = yx$. So ϕ is a homomorphism.

Condition (1) means exactly that ϕ is surjective.

Condition (2) implies that ϕ is injective. To see this, we must show that suppose $\phi(x_1, \dots, x_n) = x_1 \cdots x_n = e$ implies all $x_i = e$. We prove this by showing that for each $k = 1, \dots, n$, we have that $x_1 \cdots x_k = e$ implies all $x_i = e$ with $i = 1, \dots, k$. We use induction on k, the case of $k = 1$ being obvious. For the induction step, note that $x_1 \cdots x_k = e$ implies

$$x_k = (x_1 \cdots x_{k-1})^{-1} = x_{k-1}^{-1} \cdots x_1^{-1} = x_1^{-1} \cdots x_{k-1}^{-1} \in G_k \cap G_1 \cdots G_{k-1} = \{e\},$$

where we again use that elements from distinct factors commute. Thus both $x_k = e$ and $x_1 \cdots x_{k-1} = e$, and the claim follows by induction. □

Note: In the special case when $n = 2$, condition (3) becomes

(2) $G_1 \cap G_2 = \{e\}$.

Observe that with more factors, (3) is *not* equivalent to requiring $G_i \cap G_j = \{e\}$ for $i \neq j$. (This is a common error.)

Example. If m is odd, then $D_{4m} \approx D_{2m} \times C_2$. For instance, $D_{12} \approx D_6 \times C_2$. To see this, we use the usual presentation $G = D_{4m} = \langle r, s \mid r^{2m}, s^2, (sr)^2 \rangle$. Let $H = \langle r^2, s \rangle$ and $K = \langle r^m \rangle$. Both $H, K \trianglelefteq G$ are normal, we have $HK = G$, and $H \cap K = \{e\}$. Furthermore, $H \approx D_{2n}$ and $K \approx C_2$.

42. Properties of products of groups

As we noted, $G = G_1 \times \cdots \times G_n$ has coordinate axis subgroups $G'_k \approx G_k$. However, it usually has many other subgroups. (Example: $C_2 \times C_2$ has three subgroups of order 2.)

If $G_k \approx H_k$ for $k = 1, \dots, n$, then $G_1 \times \cdots \times G_n \approx H_1 \times \cdots \times H_n$.

Suppose $G = G_1 \times \cdots \times G_n$, and that G_k is the trivial group. Then there is an obvious isomorphism

$$G \approx G' = G_1 \times \cdots \times G_{k-1} \times G_{k+1} \times \cdots \times G_n,$$

by "omitting the kth component". These are not the *same* group, but it is common to abuse notation by treating them as the same.

Suppose $G = A \times B$, and $A = A_1 \times \cdots \times A_m$, $B = B_1 \times \cdots \times B_n$. Then there is an obvious isomorphism

$$G \approx A_1 \times \cdots \times A_m \times B_1 \times \cdots \times B_n..$$

Again, these are not the *same* group, but it is mostly harmless to treat them as the same.

Proposition. *If $G = G_1 \times \cdots \times G_n$, and $N_k \trianglelefteq G_k$ for all $k = 1, \dots, n$, then $N = N_1 \times \cdots \times N_n$ is a normal subgroup of G, and there is an isomorphism*

$$G/N \approx (G_1/N_1) \times \cdots \times (G_n/N_n).$$

43. Products of finite cyclic groups

Let's compute the order of elements in a product. Recall that for integers $n_1, \dots, n_k$, **F 16 Sep**

$$\operatorname{lcm}(n_1, \dots, n_k) = \text{smallest positive integer } n \text{ such that } n_i \mid n \text{ for all } i = 1, \dots, k.$$

Proposition. *If $G = G_1 \times \cdots \times G_k$, and $g = (g_1, \dots, g_k) \in G$, then $|g| = \operatorname{lcm}(|g_1|, \dots, |g_k|)$, or is infinite if any $|g_i| = \infty$.*

Proof. We have $g^m = (g_1^m, \dots, g_k^m)$. Clearly if some $|g_i| = \infty$ then g^m is the identity element iff $m = 0$. Otherwise, $g^m = e$ iff $|g_i| \mid m$ for $i = 1, \dots, k$, so the smallest positive such m is the least common multiple. □

Let's apply this to elements in a product of finite cyclic groups.

Example. Orders of elements in $C_3 \times C_4 = \langle a \mid a^3 \rangle \times \langle b \mid b^4 \rangle$, $C_4 \times C_4 = \langle a \mid a^4 \rangle \times \langle b \mid b^4 \rangle$, and $C_6 \times C_4 = \langle a \mid a^6 \rangle \times \langle b \mid b^4 \rangle$. The entries in the lower right show the order of $a^i b^j$.

	C_3	1	3	3
C_4		a^0	a^1	a^2
1	b^0	1	3	3
4	b^1	4	12	12
2	b^2	2	6	6
4	b^3	4	12	12

	C_4	1	4	2	4
C_4		a^0	a^1	a^2	a^3
1	b^0	1	4	2	4
4	b^1	4	4	4	4
2	b^2	2	4	2	4
4	b^3	4	4	4	4

	C_6	1	6	3	2	3	6
C_4		a^0	a^1	a^2	a^3	a^4	a^5
1	b^0	1	6	3	2	3	6
4	b^1	4	12	12	4	12	12
2	b^2	2	6	6	2	6	6
4	b^3	4	12	12	4	12	12

Thus $C_3 \times C_4$ is cyclic, while $C_4 \times C_4$ and $C_6 \times C_4$ is not.

Proposition. *Let $G \approx C_{m_1} \times \cdots \times C_{m_k}$ with $C_{m_i} = \langle x_i \mid x_i^{m_i} \rangle$, $i = 1, \dots, k$. For $x = x_1^{a_1} \cdots x_k^{a_k}$, we have*

$$|x| = \operatorname{lcm}\big(\frac{m_1}{d_1}, \dots, \frac{m_k}{d_k}\big), \qquad d_i = \gcd(m_i, a_i).$$

Furthermore, for a given $r \geq 1$, G contains an element of order r if and only if r divides $\operatorname{lcm}(m_1, \dots, m_k)$.

Proof. The first claim is immediate from the previous proposition since $|x_i^{a_i}| = m_i/d_i$ (since the order of $x_i^{a_i}$ is the smallest positive integer r_i such that $m_i \mid a_i r_i$). The second claim is a consequence of the fact that a_i can be chosen so that d_i is any divisor of m_i (e.g., take $a_i = d_i$). □

Corollary. *If $m = m_1 \cdots m_k$ is a product of positive integers, then C_m is isomorphic to $G = C_{m_1} \times \cdots \times C_{m_k}$ if and only if $\gcd(m_i, m_j) = 1$ for all $i \neq j$.*

Proof. By the previous corollary, the largest order of an element of G is $\operatorname{lcm}(m_1, \dots, m_k)$, and this is equal to m if and only if the m_is are pairwise relatively prime. □

Thus, a cyclic group can be isomorphic to a product of cyclic groups, possibly in many ways. But a product of cyclic groups need not be cyclic. One such way is the "primary decomposition".

Corollary. *Let $m = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of m, with $p_i \neq p_j$ if $i \neq j$. Then there is an isomorphism*

$$C_m \approx C_{p^{e_1}} \times \cdots \times C_{p^{e_k}}.$$

Note that if $m = p^e$ is a prime power already, then C_m can not be decomposed further as a product of cyclic groups of smaller order.

44. Classification of finitely generated abelian groups

I'm going to write abelian groups additively here. I am stating the classification theorems, but I will not prove them until later.

Theorem. *Every finitely generated abelian group G is isomorphic to one of the form*

$$G \approx F \times \mathbb{Z}^r, \qquad |F| < \infty, \quad \mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copies}}, \quad r \geq 0.$$

The factors are unique, in the sense that if G admits two such isomorphisms $G \approx F \times \mathbb{Z}^r \approx F' \times \mathbb{Z}^{r'}$, then $F \approx F'$ and $r = r'$.

Remark. The finite group factor F in such a decomposition is always *equal* to the torsion subgroup G_{tors}, and the other factor is isomorphic to G/G_{tors}.

To complete the classification, we need to classify finite abelian groups.

Theorem (Invariant factor decomposition)**.** *Every finite abelian group G is isomorphic to one of the form*

$$G \approx \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_s,$$

where

- $s \geq 0$,
- *each* $n_i \geq 2$,
- $n_{i+1} \mid n_i$ *for all* $i = 1, \dots, s-1$.

Furthermore, the decomposition is unique, in the sense that if G admits another such isomorphism $G \approx \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_t$ with $t \geq 0$, $m_i \geq 2$, $m_{i+1} \mid m_i$, then $s = t$ and $m_i = n_i$ for all i.

So a complete set of invariants for a finitely generated abelian group are

$$G \approx \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_s \times \mathbb{Z}^r :$$

the **free rank** r, and the list $n_1, \dots, n_s$ of **invariant factors**. It is finite iff $r = 0$.

free rank
invariant factors

Example. Here are the possible lists of invariant factors for groups of order $360 = 2^3 \cdot 3^2 \cdot 5$:

$$2^3 \cdot 3^2 \cdot 5; \quad 2^2 \cdot 3^2 \cdot 5,\ 2; \quad 2^2 \cdot 3 \cdot 5,\ 2,\ 2; \quad 2^3 \cdot 3 \cdot 5,\ 3; \quad 2^2 \cdot 3 \cdot 5,\ 2 \cdot 3; \quad 2 \cdot 3 \cdot 5,\ 2 \cdot 3,\ 2.$$

To figure out the possiblities, it may be helpful to write these as pictures, where each row corresponds to an invariant factor.

$$\begin{array}[t]{cccccc} \boxed{2}&\boxed{2}&\boxed{2}&\boxed{3}&\boxed{3}&\boxed{5} \end{array} \quad \begin{array}[t]{ccccc} \boxed{2}&\boxed{2}&\boxed{3}&\boxed{3}&\boxed{5} \\ \boxed{2}&&&& \end{array} \quad \begin{array}[t]{cccc} \boxed{2}&\boxed{3}&\boxed{3}&\boxed{5} \\ \boxed{2}&&& \\ \boxed{2}&&& \end{array} \quad \begin{array}[t]{ccccc} \boxed{2}&\boxed{2}&\boxed{2}&\boxed{3}&\boxed{5} \\ &&&\boxed{3}& \end{array} \quad \begin{array}[t]{cccc} \boxed{2}&\boxed{2}&\boxed{3}&\boxed{5} \\ \boxed{2}&&\boxed{3}& \end{array} \quad \begin{array}[t]{ccc} \boxed{2}&\boxed{3}&\boxed{5} \\ \boxed{2}&\boxed{3}& \\ \boxed{2}&& \end{array}$$

Example. If $|G| = p^a$ for some prime p, then its invariant factors must have the form $n_1 = p^{b_1}, \dots, n_k = p^{b_k}$, with $b_1 \geq \cdots \geq b_k \geq 1$ and $b_1 + \cdots + b_k = a$. Thus, the isomorphism classes of abelian groups of order p^a are in bijective correspondence with integer partitions of a. For instance, every abelian group of order p^5 is isomorphic to exactly one in the following list:

$$\mathbb{Z}/p^5, \quad \mathbb{Z}/p^4 \times \mathbb{Z}/p, \quad \mathbb{Z}/p^3 \times \mathbb{Z}/p^2, \quad \mathbb{Z}/p^3 \times \mathbb{Z}/p \times \mathbb{Z}/p, \quad \mathbb{Z}/p^2 \times \mathbb{Z}/p^2 \times \mathbb{Z}/p$$
$$\mathbb{Z}/p^2 \times \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p, \quad \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p,$$

coresponding to the integer partitions of 5:

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1.$$

The invariant factor decomposition tries to write the group as a product of as few cyclic factors as possible. If instead we try to have as many cyclic factors as possible, we get the **elementary divisor decomposition**.

elementary divisor decomposition

Theorem (Elementary divisor decomposition)**.** *For every finite abelian group G of order $n = p_1^{a_1} \cdots p_k^{a_k}$, where the $p_1 < \cdots < p_k$ are distinct primes, there is*

1. *an isomorphism $G \approx A_1 \times \cdots \times A_k$, with $|A_i| = p_i^{a_i}$ and $a_i \geq 1$, such that*
2. *for each A_i, there is an isomorphism*
$$A_i \approx \mathbb{Z}/p_i^{b_{i1}} \times \cdots \times \mathbb{Z}/p_i^{b_{is_i}},$$
with $b_{i1} \geq \cdots \geq b_{is_i} \geq 1$ and $b_{i1} + \cdots + b_{is_i} = a_i$.

Furthermore, this decomposition is unique, in the sense that if G admits isomorphisms $G \approx B_1 \times \cdots \times B_\ell$ with $|B_i| = q_i^{a_i}$ with q_i prime and $a_j \geq 1$, then $k = \ell$, $p_i = q_i$, and $A_i \approx B_i$.

The decomposition described in (1) is called the **primary decomposition** of G. Part (2) is just giving the invariant factor decomposition of each A_i.

primary decomposition

The list of numbers $p_1^{b_{11}}, \dots, p_k^{b_{ks_k}}$ are the **elementary divisors** of the group G. The list of elementary divisors is a complete isomorphism invariant of a finite abelian group G.

elementary divisors

Example. Here are the possible lists of elementary divisors for groups of order $360 = 2^3 \cdot 3^2 \cdot 5$:

$$2^3, 3^2, 5; \qquad 2^2, 2, 3^2, 5; \qquad 2, 2, 2, 3^2, 5; \qquad 2^3, 3, 3, 5; \qquad 2^2, 2, 3, 3, 5; \qquad 2, 2, 2, 3, 3, 5.$$

You can get these by factoring the invariant factors into products of distinct primes.

Remark. Although I will not prove either classification theorem right now, we can say the following.

1. G admits an invariant factor decomposition if and only if it admits an elementary divisor decomposition. Given an IVD, split apart each cyclic factor to get an EDD, and conversely given an EDD draw the factors in a table as above, and use this to group them together into cyclic factors.
2. The list of invariant factors for G is unique if and only if the list of elementary divisors for G is unique (up to reordering). The recipe described in (1) describes a particular bijective correspondence between sets of invariant factors and sets of elementary divisors. If a G admits two diffferent sets of invariant factors, then it admits two different sets of elementary divisors and vice versa.

45. Extensions of groups

Let H, K, G be groups. We say that G is an **extension** of K by H if there exists a normal subgroup $H' \trianglelefteq G$ and isomorphsims

extension

$$H \approx H', \qquad K \approx G/H'.$$

Typically when discussing such extensions I will silently identify H with the subgroup H'.

A **split extension** is such an extension, together with a subgroup $K' \leq G$ such that $K' \to G/H'$, $x \mapsto xH'$, is an isomorphism.

split extension

You can represent an extension by describing a sequence of homomorphisms

$$\begin{tikzcd} H \arrow[r, tail, "j"] & G \arrow[r, two heads, "p"] & K \arrow[l, dotted, bend left, "s"] \end{tikzcd}$$

where j is injective, p is surjective, and $j(H) = \mathrm{Ker}(p)$. This implies that $H' := j(H)$ is a subgroup isomorphic to H, and $G/H' \approx K$. It is split if there exists a homomorphism s such that $ps = \mathrm{id}_K$. This gives a subgroup $K' := s(K)$ such that $K' \approx G/H'$ by $x \mapsto xH'$.

Example. You can always extend K by H via the **trivial extension**, defined by

trivial extension

$$G := H \times K, \qquad H' = H \times \{e\}.$$

The trivial extension is always split, by $K' = \{e\} \times K$.

Example. Let $H = K = C_2$. Then both $G_1 = C_2 \times C_2$ and $G_2 = C_4$ are extensions of K by H:

$$H' = \{e, a\} \trianglelefteq G_1 = C_2 \times C_2 = \langle a \mid a^2 \rangle \times \langle b \mid b^2 \rangle = \{e, a, b, ab\}, \quad G_1/H' = \{\bar{e}, \bar{b}\},$$

and

$$H' = \{e, c^2\} \trianglelefteq G_2 = C_4 = \langle c \mid c^4 \rangle = \{e, c, c^2, c^3\}, \quad G_2/H' = \{\bar{e}, \bar{c}\}.$$

The first extension is split, using $K' = \{e, b\} \leq G_1$, but the second extension is not split.

Example. Let $H = C_3$ and $K = C_2$. Then both $G_1 = C_6$ and $G_2 = D_6$ are extensions of K by H:

$$H' = \{e, a^2, a^4\} \trianglelefteq G_1 = C_6 = \langle a \rangle a^6, \quad G_1/H' = \{\bar{e}, \bar{a}\},$$

and

$$H' = \{e, r, r^2\} \trianglelefteq G_2 = D_6 = \langle r, s \rangle r^3, s^2, (sr)^2, \quad G_2/H' = \{\bar{e}, \bar{s}\}.$$

These are both split extensions, using $K' = \{e, a^3\} \leq G_1$ and $K' = \{e, s\} \leq G_2$.

The **extension problem** for groups is to classify, for given H and K, all possible extensions up to isomorphism. There is a complete solution in terms of group cohomology (sometimes called *Schreier theory*), but it is difficult to compute this in practice.

extension problem

46. Semi-direct products

There is a good classification of *split* extensions: they are isomorphic to semi-direct products.

M 19 Sep

First, note that identifying G as a split extension amounts to specifying subgroups $H, K \leq G$ such that

(1) H is normal in G,
(2) $G = HK$, and
(3) $H \cap K = \{e\}$.

Condition (1) implies that you have a homomorphism $x \mapsto xH \colon K \to G/H$, and conditions (2) and (3) are exactly what you need to ensure that $x \mapsto xH \colon K \to G/H$ is an isomorphism. (Exercise: use the diamond isomorphism theorem.) Note that K is not assumed to be normal in G, and in fact K is normal iff G is a product of the subgroups H and K.

In particular, note that any $g \in G$ can be written *uniquely* as

$$g = hk, \qquad h \in H, \quad k \in K.$$

In this situation we get a homomorphism

$$\alpha\colon K \to \operatorname{Aut}(H), \qquad k \mapsto \operatorname{conj}_k |H = \big(h \mapsto khk^{-1}\big).$$

Note: I'm going to write $\alpha_k \in \operatorname{Aut}(H)$ instead of $\alpha(k)$, since something like "$\alpha_k(h)$" is easier to parse.

It turns out we can completely reconstruct the group structure on G knowing H and K and the homomorphism α. In fact, if

$$g_1 = h_1k_1, \quad g_2 = h_2k_2, \qquad h_1, h_2 \in H, \quad k_1, k_2 \in K,$$

then

$$\begin{aligned} g_1g_2 &= h_1k_1\, h_2k_2 \\ &= h_1k_1h_2\, k_1^{-1}k_1\, k_2 \\ &= h_1(k_1h_2k_1^{-1})\, k_1k_2 \\ &= h_1\alpha_{k_1}(h_2)\, k_1k_2 \end{aligned}$$

where $h_1\alpha_{k_1}(h_2) \in H$ and $k_1k_2 \in K$.

Remark. The book introduces the notation $k \cdot h := khk^{-1}$ for the conjugation $\alpha(k)(h)$. This is ok but can lead to confusion with multiplication in G. Another notation you will sometimes see for such a conjugation is

$$h^k := khk^{-1}.$$

This is a somewhat better notation, especially because you have then formulas

$$(h_1h_2)^k = h_1^kh_2^k, \qquad h^{k_1k_2} = (h^{k_2})^{k_1}.$$

(The order of the k_is in the second formula is not ideal, but is the correct one.)

Note that G is the *internal product* of H and K iff $hk = kh$ for all $h \in H$, $k \in K$, i.e., iff $\alpha\colon K \to \operatorname{Aut}(H)$ is the *trivial* homomorphism, or equivalently, if K is *also* a normal subgroup of G.

Exercise. Show that $\alpha\colon K \to \operatorname{Aut}(H)$ is the trivial homomorphism iff K is normal in G.

Theorem. *Let H, K be groups, and $\alpha\colon K \to \operatorname{Aut}(H)$ a homomorphism. Let G be the set $H \times K$, and define a product on G by the rule*

$$(h_1, k_1)(h_2, k_2) := (h_1\, \alpha_{k_1}(h_2),\, k_1k_2).$$

Then we have the following.

1. *G is a group, with identity element (e, e) and inverses $(h, k)^{-1} = (\alpha_{k^{-1}}(h^{-1}), k^{-1})$.*
2. *The subsets $H' = H \times \{e\}$ and $K' = \{e\} \times K$ are subgroups of G, and there are isomorphisms $H \xrightarrow{\sim} H'$ and $K \xrightarrow{\sim} K'$ defined by $h \mapsto (h, e)$ and $k \mapsto (e, k)$ respectively.*

We now identify H with H' and K with K' via these isomorphisms in the following.

3. *$H \trianglelefteq G$.*
4. *$H \cap K = \{e\}$ and $G = HK$.*
5. *We have $khk^{-1} = \alpha_k(h)$ for all $h \in H$ and $k \in K$.*

The theorem constructs a new group G. A standard notation for a semi-direct product is $G = H \rtimes K$. However, be careful: the semi-direct product depends not only on the groups H and K, but also the homomorphisms α. It is better to write $H \rtimes_\alpha K$.

Example. Let $H = F(a)$ and $K = \langle b \mid b^2 \rangle$. Let $\alpha\colon K \to \operatorname{Aut}(H)$ be the homomorphism defined by $\alpha(b)(a) = a^{-1}$. We obtain a semi-direct product $G = H \rtimes K$. If we identify H and K with the obvious subgroups of G, this means that

$$G = \{\, a^n \mid n \in \mathbb{Z} \,\} \amalg \{\, a^n b \mid n \in \mathbb{Z} \,\}, \qquad bab^{-1} = a^{-1}.$$

In fact, G is the infinite dihedral group.

Example. Let $H = \langle a \mid a^m \rangle$ and $K = \langle b \mid b^2 \rangle$, and $\alpha\colon K \to \operatorname{Aut}(H)$ by $\alpha(b)(a) = a^{-1}$. Then $G = H \rtimes_\alpha H$ is isomorphic to the dihedral group D_{2m}.

Proof. (1) is a straightforward verification. It is easy to see that (e,e) is an identity element.

Here is associativity. We have

$$\begin{aligned}\big((h_1,k_1)(h_2,k_2)\big)(h_3,k_3) &= (h_1\alpha_{k_1}(h_2),\ k_1k_2)(h_3,k_3) \\ &= (h_1\alpha_{k_1}(h_2)\alpha_{k_1k_2}(h_3),\ k_1k_2k_3)\end{aligned}$$

and

$$\begin{aligned}(h_1,k_1)\big((h_2,k_2)(h_3,k_3)\big) &= (h_1,k_1)(h_2\alpha_{k_2}(h_3),\ k_2k_3) \\ &= (h_1\alpha_{k_1}(h_2\alpha_{k_2}(h_3)),\ k_1k_2k_3).\end{aligned}$$

These are equal because

$$\alpha_{k_1}(h_2\alpha_{k_2}(h_3)) = \alpha_{k_1}(h_2)\alpha_{k_1}(\alpha_{k_2}(h_3)) = \alpha_{k_1}(h_2)\alpha_{k_1k_2}(h_3),$$

since both $\alpha(k_1)\colon H \to H$ and $\alpha\colon K \to \operatorname{Aut}(H)$ are homomorphisms.

Here are inverses:

$$\begin{aligned}(h,k)(\alpha_{k^{-1}}(h^{-1}),\ k^{-1}) &= (h\alpha_k(\alpha_{k^{-1}}(h^{-1})),\ kk^{-1}) \\ &= (h\alpha_{kk^{-1}}(h^{-1})\, e) = (e,e), \\ (\alpha_{k^{-1}}(h^{-1}), k^{-1})(h,k) &= (\alpha_{k^{-1}}(h^{-1})\alpha_{k^{-1}}(h),\ k^{-1}k) \\ &= (\alpha_{k^{-1}}(h^{-1}h),\ e) = (e,e).\end{aligned}$$

(2) is a straightforward verification: restricted to H' and K', products are given by

$$(h_1,e)(h_2,e) = (h_1\alpha_e(h_2), ee) = (h_1h_2, e), \qquad (e,k_1)(e,k_2) = (e\alpha_{k_1}(e), k_1k_2) = (e, k_1k_2).$$

(3) is clear, since

$$\begin{aligned}(h,k)(h',e)(h,k)^{-1} &= (h\alpha_k(h'), k)(\alpha_{k^{-1}}(h^{-1}), k^{-1}) \\ &= (h\alpha_k(h')\alpha_k(\alpha_{k^{-1}}(h^{-1})), kk^{-1}) \\ &= (h\alpha_k(h')\alpha_{kk^{-1}}(h^{-1}), e) = (h\alpha_k(h')h^{-1}, e).\end{aligned}$$

(4) is immediate, and (5) is just the easily verifed formula

$$(e,k)(h,e)(e,k)^{-1} = (\alpha_k(h), e).$$

□

Example (Groups of order pq). Suppose $p < q$ are primes, and that $p \mid q-1$. Since $|\operatorname{Aut}(C_q)| = q-1$, by Cauchy's theorem there is a subgroup $P \leq \operatorname{Aut}(C_q)$ of order p. Let $\alpha\colon P \to \operatorname{Aut}(C_q)$ be the inclusion homomorphism. Then $G = C_q \rtimes_\alpha P$ is a non-abelian group of order pq.

Example (Affine groups). Let $G \subseteq \operatorname{Sym}(\mathbb{R}^n)$ be the set of all functions $\phi\colon \mathbb{R}^n \to \mathbb{R}^n$ of the form

$$\phi(x) = Ax + b, \qquad A \in GL_n(\mathbb{R}), \quad b \in \mathbb{R}^n.$$

This can be shown to be a subgroup. It is a semi-direct product of its subgroups

$$H = \{\, \phi \mid \phi(x) = x + b,\ b \in \mathbb{R}^n \,\}, \qquad K = \{\, \phi \mid \phi(x) = Ax,\ A \in GL_n(\mathbb{R}) \,\}.$$

47. Composition series

A group G is **simple** if it has exactly two normal subgroups, which are necessarily $\{e\}$ and G. **simple** Note: the trivial group is *not* simple, much in the same way that 1 is not a prime number. Note that a simple group cannot arise an extension of two smaller groups.

Example. An abelian group is simple if and only if it is cyclic of prime order.

Example. Let $G \leq SO(3)$ be the symmetry group of a regular icosahedron centered at the origin. This is a group of order 60. It is a simple group.

Example. As we have shown, every alternating group A_n with $n \geq 5$ is simple.

A **composition series** for a group G is a finite chain of subgroups **composition series**

$$\{e\} = M_0 \leq M_1 \leq \cdots \leq M_{r-1} \leq M_r = G, \qquad r \geq 0,$$

such that

(1) M_{k-1} is a normal subgroup of M_k, for each $k = 1, \dots, r$, and
(2) the quotient M_k/M_{k-1} is a simple group.

The list of groups $(M_1/M_0, \dots, M_r/M_{r-1})$ are called the **composition factors** of the composition series. **composition factors**

Example. A simple group has a simple composition series: $1 \leq G$.

Example. A composition series of A_4:

$$1 \leq \langle (12)(34) \rangle \leq \langle (12)(34), (13)(24) \rangle \leq A_4.$$

The composition factors are (C_2, C_2, C_3).

Note that "is a normal subgroup of" is not a transitive relation.

Example. Two composition series of D_{12}:

$$1 \leq \langle s \rangle \leq \langle s, r^3 \rangle \leq D_{12} \qquad \text{and} \qquad 1 \leq \langle r^3 \rangle \leq \langle r \rangle \leq D_{12}.$$

The sequences of composition factors are (C_2, C_3, C_2) and (C_3, C_2, C_2) respectively. In the first example $\langle s \rangle$ is not normal in D_{12}.

Proposition. *Every finite group has a composition series.*

Proof. Use induction on order. If $|G| = 1$, it has a composition series of length 0. If $|G| > 1$, then either (i) G is simple, so $\{e\} \leq G$ is a composition series, or (ii) G is not simple, so G has non-trivial proper normal subgroups. Choose a maximal proper normal subgroup $N \trianglelefteq G$. Since $N \neq G$ the quotient G/N is simple (since normal subgroups of G/N correspond to normal subgroups of G containing N). By induction, N has a composition series $\{e\} \leq M_0 \leq \cdots \leq M_{r-1} = N$, and therefore extends to a composition series for G of length r, with $M_r = G$. □

48. Jordan-Hölder theorem

Theorem (Jordan-Hölder)**.** *Suppose G is a group with a composition series. Then the composition factors of a composition series are unique up to change of permutation. That is, if*

$$\{e\} = M_0 \leq \cdots \leq M_r = G, \qquad \{e\} = N_0 \leq \cdots \leq N_s = G$$

are two composition series, then $r = s$ and there exists $\sigma \in S_r$ such that $M_k/M_{k-1} \approx N_{\sigma(k)}/N_{\sigma(k)-1}$ for all $k = 1, \dots, n$.

Thus, the unordered list of composition factors of a finite group G is an invariant of the group up to isomorphism.

The proof will be based on the following argument. Fix a composition series $\{e\} = M_0 \leq \cdots \leq M_r = G$, and suppose $N \trianglelefteq G$ such that G/N is simple. We obtain the following diagram of subgroups.

$$\begin{tikzcd}
\{e\} = M_0 \arrow[r, tail] & M_1 \arrow[r, tail] & M_2 \arrow[r, tail] & \cdots \arrow[r, tail] & M_{r-1} \arrow[r, tail] & M_r = G \\
\{e\} = M_0 \cap N \arrow[u, tail] \arrow[r, tail] & M_1 \cap N \arrow[u, tail] \arrow[r, tail] & M_2 \cap N \arrow[u, tail] \arrow[r, tail] & \cdots \arrow[r, tail] & M_{r-1} \cap N \arrow[u, tail] \arrow[r, tail] & M_r \cap N = N \arrow[u, tail]
\end{tikzcd}$$

Each arrow in the diagram represents the inclusion of a *normal* subgroup. That is, we have that:

$$M_{k-1} \trianglelefteq M_k, \qquad M_{k-1} \cap N \trianglelefteq M_k \cap N, \qquad M_k \cap N \trianglelefteq N.$$

Next note that since $M_{j-1} \cap (M_j \cap N) = M_{j-1} \cap N$, we have inclusions of subgroups

$$M_{j-1}/M_{j-1} \cap N \to M_j/M_j \cap N,$$

each of which is the inclusion of a normal subgroup since $M_{j-1} \trianglelefteq M_j$. Thus we also have a diagram of subgroups

$$\{e\} = M_0/M_0 \cap N \rightarrowtail M_1/M_1 \cap N \rightarrowtail M_2/M_2 \cap N \rightarrowtail \cdots \rightarrowtail M_{r-1}/M_{r-1} \cap N \rightarrowtail M_r/M_r \cap N = G/N$$

each of which is normal in the next. But remember that G/N is assumed to be simple. Thus if $k \in \{1, \dots, r\}$ is such that $M_{k-1} \leq N$ but $M_k \not\leq N$, then we have

$$\{e\} = M_0/M_0 \cap N = \cdots = M_{k-1}/M_{k-1} \cap N \rightarrowtail M_k/M_k \cap N = M_{k+1}/M_{k+1} \cap N = \cdots M_r/M_r \cap N = G/N.$$

Also note that since $M_k \not\leq N$ we must have $M_k \cap N < M_k$, but since M_k/M_{k-1} is simple and $M_{k-1} = M_{k-1} \cap N$, we must have $M_{k-1} \cap N = M_k \cap N$.

Putting these observations together, and using the diamond isomorphism theorem, we have the following:

(a) For $j < k$ we have $M_j \cap N = M_j$.
(b) We have $M_{k-1} \cap N = M_k \cap N$.
(c) For $j > k$ we have $M_j = M_{j-1}(M_j \cap N)$, and isomorphisms $M_j/M_j \cap N \xrightarrow{\sim} G/N$.
(d) We have $M_k/M_{k-1} \approx M_k/M_k \cap N \approx G/N$.
(e) For $j \neq k$ we have isomorphisms

$$M_j \cap N/M_{j-1} \cap N \xrightarrow{\sim} M_j/M_{j-1}.$$

$$\begin{tikzcd}
\cdots \arrow[r, tail] & M_{k-2} \arrow[r, tail] & M_{k-1} \arrow[r, tail] & M_k \arrow[r, tail] \arrow[dr, phantom, "\diamondsuit"] & M_{k+1} \arrow[r, tail] \arrow[dr, phantom, "\diamondsuit"] & \cdots \arrow[r, tail] \arrow[dr, phantom, "\diamondsuit"] & G \\
\cdots \arrow[r, tail] & M_{k-2} \cap N \arrow[u, equal] \arrow[r, tail] & M_{k-1} \cap N \arrow[u, equal] \arrow[r, equal] & M_k \cap N \arrow[u, tail] \arrow[r, tail] & M_{k+1} \cap N \arrow[u, tail] \arrow[r, tail] & \cdots \arrow[r, tail] & N \arrow[u, tail]
\end{tikzcd}$$

As a consequence, we see that if we omit $M_k \cap N$, we obtain a composition series for N:

$$\{e\} = M_0 \cap N \rightarrowtail \cdots \rightarrowtail M_{k-1} \cap N \rightarrowtail M_{k+1} \cap N \rightarrowtail \cdots \rightarrowtail M_r \cap N = N.$$

This series has length $r - 1$, with composition factors isomorphic to

$$(M_1/M_0, \dots, M_{k-1}/M_{k-2}, M_{k+1}/M_k, \dots, M_r/M_{r-1}).$$

The "missing factor" M_k/M_{k-1} is isomorphic to G/N.

Proof of Jordan-Hölder. We work by induction on the length of the shortest composition series. WLOG assume $r \geq s$. Let $N = N_{s-1}$, so that N has a composition series of length $s-1$, with factors $(N_1/N_0, \dots, N_{s-1}/N_{s-2})$. The above argument produces a composition series for N of length $r-1$, with factors $(M_1/M_0, \dots, M_{k-1}/M_{k-2}, M_{k+1}/M_k, \dots, M_0/M_{r-1})$. Thus by induction $s-1 = r-1$ and these lists have the same factors, up to isomorphisms and permutation. Finally note that $N_s/N_{s-1} = G/N \approx M_k/M_{k-1}$, so the two series for G have the same factors up to isomorphism and permutation. □

49. Solvable groups

W 21 Sep

A group G is **solvable** if it admits a finite chain of subgroups

solvable

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G,$$

with each $G_k \trianglelefteq G_{k+1}$, such that each quotient G_k/G_{k-1} is abelian.

In particular, a finite group G is solvable if its composition factors are abelian, i.e., all cyclic of prime order.

Examples:

- If $N \trianglelefteq G$ and both N and G/N are solvable, then G is solvable.
- Abelian groups are solvable.
- Dihedral groups are solvable, since $C_n \leq D_{2n}$ with $D_{2n}/C_n \approx C_2$.
- The quaternion group Q_8 is solvable: it has a composition series $\{\pm 1\} < \langle i \rangle < Q_8$.
- S_4 is solvable, since $N = \langle (1\ 2)(3\ 4),\ (1\ 3)(2\ 4) \rangle \trianglelefteq S_4$ and $S_4/N \approx S_3 \approx D_6$.
- If G admits a composition series such that every composition factor is abelian, then G is solvable. (Warning: the converse is not true, since some abelian groups have no composition series.)

On the other hand, any group which has a composition series containing a non-abelian simple group is not solvable.

Given elements $x, y \in G$, we write

$$[x, y] := xyx^{-1}y^{-1} \in G$$

for the **commutator** of x and y. For subsets $S, T \subseteq G$, we write

commutator

$$[S, T] := \langle [x, y],\ x \in S,\ y \in T \rangle$$

for the subgroup generated by such commutators. In particular, the **commutator subgroup** of G is the subgroup $[G, G]$ generated by all commutators. ("Generated" is important here: the subset of commutators is not usually a subgroup.)

commutator subgroup

Note that $[G, G] \trianglelefteq G$, since $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$. The quotient group $G/[G, G]$ is abelian, and is called the **abelianization** of G, since it is the "largest abelian quotient" of G, in the following sense.

abelianization

Proposition. *If $H \trianglelefteq G$, then G/H is abelian if and only if $[G, G] \leq H$.*

Proof. Clear. □

The **derived series** of G is the sequence of subgroups $G^{(k)}$ defined by

derived series

- $G^{(0)} = G$,
- $G^{(1)} = [G, G]$,
- $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$, $k \geq 2$.

We obtain a descending chain of subgroups, each of which is normal in the previous:

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots.$$

Note that there is no reason for the sequence to terminate.

Example. Let $G = D_{2n}$ with $n \geq 3$. We have $[r^i, r^j] = e$, $[r^i, sr^j] = r^{2i}$, $[sr^i, sr^j] = r^{-2j}$, $[sr^i, sr^j] = r^{2(j-i)}$. Thus:

(1) If n is even, the derived series is $D_{2n} > \langle r^2 \rangle > \{e\}$.
(2) If n is odd, the derived series is $D_{2n} > \langle r \rangle > \{e\}$.

Proposition. *G is solvable if and only if $G^{(s)} = \{e\}$ for some s.*

Proof. If $G^{(s)} = \{e\}$, then the derived series is a finite chain of subgroups with abelian quotients, so G is solvable.

For the converse, suppose $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$ with H_k/H_{k-1} abelian. Then

$$H_{s-1} \supseteq [H_s, H_s] = [G, G] = G^{(1)},$$
$$H_{s-2} \supseteq [H_{s-1}, H_{s-1}] \supseteq [G^{(1)}, G^{(1)}] = G^{(2)},$$

etc., so $\{e\} = H_0 \supseteq G^{(s)}$, whence $G^{(s)} = \{e\}$. □

We have the following consequence.

Corollary. *If G is solvable, then so is any subgroup or quotient group of G.*

Proof. Suppose $H \leq G$. Then clearly $[H, H] \leq [G, G]$, and using this it is easy to show that $H^{(k)} \subseteq G^{(k)}$ for all k. Thus if $G^{(s)} = \{e\}$ then $H^{(s)} = \{e\}$.

Suppose $N \trianglelefteq G$. Then

$$[G/N, G/N] = [G, G]N/N.$$

This is easy to prove using the fact that, for $x, y \in G$, we have $[xN, yN] = [x, y]N$ (where $[xN, yN]$ is the commutator in G/N, and $[x, y]$ the commutator in G). Using this it is easy to show that $(G/N)^{(k)} = G^{(k)}N/N$. Thus if $G^{(s)} = \{e\}$ then $(G/N)^{(s)} = \{eN\}$. □

Remark. I should mention a famous result about finite solvable groups, called the *Feit-Thompson theorem* or the *odd order theorem*: every finite group of odd order is solvable. This immediately implies that every non-abelian simple group must has even order, since the only solvable simple groups are abelian.

The proof is complex: although it was first proved almost 60 years ago, it still takes a full length book to give the proof.

50. Upper central series and nilpotent groups

Given a group G, we write $Z(G) = \{\, g \in G \mid gx = xg \ \forall x \in G \,\}$ for the center of G, which is a normal subgroup of G.

We inductively define a series of normal subgroups $Z_k(G) \leq G$, called the **upper central series**, as follows. **upper central series**

- $Z_0(G) = \{e\}$.
- $Z_1(G) = Z(G)$.
- For any $k \geq 1$, $Z_{k+1}(G)$ is the preimage under the quotient map $\pi\colon G \to G/Z_k(G)$ of $Z(G/Z_k(G))$. (The preimage will be normal in G, by the lattice isomorphism theorem.)

We obtain a possibly infinite sequence of subgroups

$$\{e\} = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq G,$$

all of which are normal in G.

Remark. To make the definition explicit, $Z_{k+1}(G)$ consists of elements $g \in G$ such that $gxg^{-1}x^{-1} \in Z_k(G)$ for all $x \in G$.

Note that $Z_k(G) = Z_{k+1}(G)$ iff $Z(G/Z_k(G)) = \{e\}$. If this happens for some k, then the sequence stabilizes at this point: $Z_j(G) = Z_k(G)$ for all $j \geq k$.

A group G is **nilpotent** if there exists a c such that $Z_c(G) = G$. The smallest such c is called the **nilpotence class** of G. **nilpotent** **nilpotence class**

Remark. Observe that for each k

$$Z_k(G)/Z_{k-1}(G) \approx Z(G/Z_{k-1}(G))$$

is an abelian group. In particular, if G is nilpotent, then taking $G_k = Z_k(G)$ gives $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$ so that each G_k/G_{k-1} is abelian. That is, every nilpotent group is solvable. The converse is not true, as we will see. (And as you should expect, since $Z_k(G) \trianglelefteq G$ for all k, and the terms in a composition series for G need not be normal in G.)

Example. G is abelian iff $Z(G) = G$, iff G has nilpotence class 0 or 1. (The trivial group has nilpotence class 0.)

Example. Consider $G = D_8 = \langle r, s \mid r^4, s^2, (sr)^2 \rangle$. We have

$$Z_1(G) = \langle r^2 \rangle, \qquad Z_2(G) = G,$$

so G is nilpotent, of nilpotence class 2.

Consider $G = D_{12} = \langle r, s \mid r^6, s^2, (sr)^2 \rangle$. We have

$$Z_1(G) = \langle r^3 \rangle = Z_2(G).$$

This is because $D_{12}/\langle r^2 \rangle \approx D_6$, which has trivial center. Thus D_{12} is not nilpotent. This gives an example of a solvable group which is not nilpotent.

Proposition. *If G is nilpotent, so is any quotient group G/N, and the nilpotence class of G is $\geq$ the nilpotence class of G/N.*

Proof. Let $\pi\colon G \to G/N$ be the quotient homomorphism. We show that $\pi(Z_k(G)) \subseteq Z_k(G/N)$, so $Z_c(G) = G$ implies $Z_c(G/N) = G/N$. Prove this by induction on k: if $g \in Z_{k+1}(G)$, then $gxg^{-1}x \in Z_k(G)$, so $(gN)(xN)(gN)^{-1}(xN)^{-1} = gxg^{-1}x^{-1}N \in Z_k(G/N)$ for all $x \in G$, so $gN \in Z_{k+1}(G/N)$. □

Proposition. *If $G_1, \ldots, G_s$ are nilpotent, then $G = G_1 \times \cdots \times G_s$ is nilpotent.*

Proof. Prove that $Z_k(G) = Z_k(G_1) \times \cdots \times Z_k(G_s)$, using induction on k. □

Proposition. *Let p be a prime and G a p-group of order p^a, $a \geq 1$. Then G is nilpotent, and if $a \geq 2$ it has nilpotence class $\leq a - 1$.*

Note: this is stated slightly incorrectly in DF (at least in my edition, where it is §6.1 Proposition 2).

Proof. We have already observed, using the class equation, that every non-trivial p-group has non-trivial center. Therefore, if for some k we have $Z_k(G) \neq G$, the quotient $G/Z_k(G)$ is also a p-group and so has non-trivial center $Z(G/Z_k(G))$, and thus $Z_k(G) \subsetneq Z_{k+1}(G)$. Since p must therefore divide the index $|Z_{k+1}(G) : Z_k(G)|$, we must have $|Z_k(G)| \geq p^k$, so $Z_a(G) = G$ and thus G has nilpotence class $\leq a$.

In remains to show a cannot be the nilpotence class if $a \geq 2$. It is clear that $|Z_k(G)| \geq p^k$ when $0 \leq k \leq a$. Thus $|G/Z_{a-2}(G)| \in \{1, p, p^2\}$, but we have shown that all groups of such orders are abelian, so $Z_{a-1}(G) = G$, whence the nilpotence class is $\leq a - 1$. □

51. Finite nilpotent groups

The following characterizes finite nilpotent groups: they are exactly the *products* of p-groups for various primes p.

Theorem. *Let G be a finite group with $p_1, \dots, p_s$ the distinct primes dividing its order. Then the following are equivalent:*

1. *G is nilpotent.*
2. *If $H < G$ then $H < N_G(H)$ (i.e., every proper subgroup of G is proper in its normalizer, or equivalently, G is the only subgroup which is its own normalizer).*
3. *$|\mathrm{Syl}_{p_i}(G)| = 1$ for all $i = 1, \dots, s$ (or equivalently, G has a normal p_i-Sylow subgroup for all $i = 1, \dots, s$).*
4. *$G \approx P_1 \times \cdots \times P_s$, where $P_i \in \mathrm{Syl}_{p_i}(G)$.*

Proof. (1) $\implies$ (2). Use induction on $|G|$, where the case of $|G| = 1$ is trivial.

Assuming $|G| > 1$, there are two cases:

(a) $Z(G) \not\subseteq H$. Since $Z(G) \leq N_G(H)$, we see that $H \neq N_G(H)$.

(b) $Z(G) \leq H$. Write $Z := Z(G)$, and note that $|Z| > 1$ since G is non-trivial and nilpotent. Since $Z \trianglelefteq G$ we can form the quotients

$$H/Z \leq N_G(H)/Z \leq G/Z,$$

where: G/Z is nilpotent, $H/Z < G/Z$, and $|G/Z| < |G|$. Thus by induction $H/Z < N_{G/Z}(H/Z)$. But it is straightforward to check that $N_{G/Z}(H/Z) = N_G(H)/Z$, so $H/Z < N_G(H)/Z$ and thus $H < N_G(H)$ as desired.

(2) $\implies$ (3). Let P_i be a p_i-Sylow subgroup of G, and let $N_i = N_G(P_i)$. The Sylow theorems applied to N_i imply that P_i is the only p_i-Sylow subgroup of N_i. If $g \in N_G(N_i)$ we have $gP_ig^{-1} \leq gN_ig^{-1} = N_i$ and so $g_iP_ig_i^{-1} = P_i$. This shows that $N_G(N_i) = N_i$.

By (2), $N_G(N_i) = N_i$ implies $N_i = G$, so $P_i \trianglelefteq G$ and $\mathrm{Syl}_{p_i}(G) = \{P_i\}$ by the Sylow theorems.

(3) $\implies$ (4). Let $H_0 = \{e\}$ and $H_k = P_1 \cdots P_k$ for $k = 1, \dots, s$. Since each $P_k \trianglelefteq G$, each $H_k = H_{k-1}P_k$ is a subgroup of G.

We show by induction on k that $H_{k-1} \cap P_k = \{e\}$, and thus H_k is an internal product of H_{k-1} and P_k, and therefore that $|H_k| = |P_1| \cdots |P_s|$. For $k = 1$ this is clear. If $k \geq 2$, by induction we have that $|H_{k-1}| = |P_1| \cdots |P_{k-1}|$, which is relatively prime to $|P_k|$. Since the order of elements of $H_{k-1} \cap P_k$ must divide both, we have $H_{k-1} \cap P_k = \{e\}$.

Thus $|H_s| = |G|$, so $G = H_s$, and therefore $G \approx H_s \approx H_{s-1} \times P_s \approx \cdots P_1 \times \cdots \times P_s$ as desired.

(4) $\implies$ (1). All p-groups are nilpotent, and products of nilpotent groups are nilpotent.

□

This gives the "primary decomposition" of finite abelian groups.

Corollary. *Any finite abelian group is a product of its Sylow subgroups.*

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL
Email address: rezk@illinois.edu