Groups II

Introduction to Model Theory
(Third hour)

October 14, 2021

Section 1

Cosets, normal subgroups, and quotients

Cosets

Let G be a group and H be a subgroup.

- H acts on G via the group operation $h \cdot g$.
- The orbit of $g \in G$ is the set

$$H \cdot g = \{h \cdot g : h \in H\}.$$

- Such sets are called *right cosets* of H. They form a partition of G.
- Similarly, the *left cosets* of H are the sets of the form

$$g \cdot H = \{g \cdot h : h \in H\}.$$

- In an abelian group, left cosets and right cosets are the same thing.

Cosets

- $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.
- The coset of π is the set

$$\mathbb{Z} + \pi = \{n + \pi : n \in \mathbb{Z}\} = \{\dots, \pi - 1, \pi, \pi + 1, \pi + 2, \dots\}.$$

- The coset of 7 is the set

$$\mathbb{Z} + 7 = \{\dots, 7 - 1, 7, 7 + 1, 7 + 2, \dots\} = \mathbb{Z}.$$

Cosets

Let $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\} = \{\ldots, -2, 0, 2, 4, \ldots\}$. Then $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

- If n is even, then the coset of n is $\{\ldots, -2, 0, 2, 4, \ldots\}$.
- If n is odd, then the coset of n is $\{\ldots, -1, 1, 3, 5, \ldots\}$.
- There are two cosets: the set of even numbers and the set of odd numbers.

Left and right quotients

Let G be a group and H be a subgroup.

Definition

G/H is the set of left cosets $\{gH : g \in G\}$.
$H\backslash G$ is the set of right cosets $\{Hg : g \in G\}$.

Fact

There is a bijection between G/H and $H\backslash G$ sending gH to Hg^{-1}.

Order and index

Definition

The *order* of a group G is $|G|$, the size of G.

Definition

If H is a subgroup of G, the *index* of H in G is $|G/H|$, the number of left cosets.

$|G/H| = |H\backslash G|$, so we could also use "right cosets."

Fact

1. $|G| = |G/H| \cdot |H|$.
2. *If K is a subgroup of H, then* $|G/K| = |G/H| \cdot |H/K|$.

Order and index in finite groups:

Corollary

Let G be a finite group and H be a subgroup. Then the order of H divides the order of G.

Example

Suppose the order of G is a prime number p. If H is a subgroup of G, then $|H|$ is 1 or p. So the only subgroups of G are $\{1\}$ and G.

Normal subgroups

Let H be a subgroup of G.

Definition

H is a *normal subgroup* if the following equivalent conditions hold:

- The right cosets of H are the same as the left cosets of H.
- For any $g \in G$, $gH = Hg$.
- For any $g \in G$, $gHg^{-1} = H$.
- For any inner automorphism ϕ_g, we have $\phi_g(H) = H$.

Example

In an abelian group, any subgroup is normal.

Quotient groups

Let G be a group and N be a normal subgroup. G/N is the set of cosets.

Fact

There is a group structure on the set G/N given by

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

Example

$\mathbb{Z}/2\mathbb{Z}$ is the group given by

+	even	odd
even	even	odd
odd	odd	even.

Quotient groups via representatives

- Let G be a group and N be a normal subgroup.
- Let S be a subset of G containing exactly one element from each coset of N.
- For $x, y \in S$, define $x \cdot y$ to be the unique $z \in S$ such that z is in the same coset as $x \cdot y$.
- Then $(S, \cdot)$ is a group, isomorphic to G/N via the map sending x to xN.

Example

For $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$, we can take $S = \{0, 1\}$, and we get $\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0. \end{array}$

Quotient groups via representatives

$\mathbb{Z}/4\mathbb{Z}$ is isomorphic to

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}$$

Quotient groups via representatives

$\mathbb{R}/\mathbb{Z}$ is isomorphic to $[0,1)$ with the group operation

$$x + y = \begin{cases} x + y & \text{if } x + y < 1 \\ x + y - 1 & \text{if } x + y \geq 1. \end{cases}$$

Kernels and images

Let $f : G \to H$ be a homomorphism.

Definition

The *image* of f is the set $\{f(x) : x \in G\}$.
The *kernel* of f is the set $\{x \in G : f(x) = 1_H\}$.

Fact

The image is a subgroup of H. The kernel is a normal subgroup of G.

Example

Consider the homomorphism $(\mathbb{R}, +) \to \mathbb{C}^\times$ given by $\exp(2\pi ix)$.

- The image is the "circle group" $\{z \in \mathbb{C} : |z| = 1\}$.
- The kernel is $(\mathbb{Z}, +)$.

The fundamental theorem of homomorphisms

Fact

Let $f : G \to H$ be a homomorphism with kernel K and image $f(G)$. Then $G/K \cong f(G)$. The isomorphism is

$$G/K \xrightarrow{\cong} f(G)$$
$$aK \mapsto f(a).$$

Example

$\mathbb{R}/\mathbb{Z}$ is isomorphic to the circle group $\{z \in \mathbb{C} : |z| = 1\}$. The isomorphism is

$$\mathbb{R}/\mathbb{Z} \xrightarrow{\cong} \{z \in \mathbb{C} : |z| = 1\}$$
$$\mathbb{Z} + a \mapsto \exp(2\pi i a).$$

Motivation for normal subgroups, quotient groups

Let N be a subgroup of G.

- N is normal if and only if N is the kernel of *some* homomorphism $f : G \to H$
- In this case, G/N is isomorphic to the image of f.

Subgroups and quotients of $(\mathbb{Z}, +)$

Fact

The only subgroups of $\mathbb{Z}$ are $\{0\}$ and $n\mathbb{Z}$ for $n = 1, 2, 3, \ldots$.

Quotients of $(\mathbb{Z}, +)$ are called *cyclic groups*. By the above, there are two types:

- $\mathbb{Z}/\{0\} \cong \mathbb{Z}$, the *infinite cyclic group*.
- $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$, the *cyclic group of order n*.

The order of an element

Let G be any group and $g \in G$ be an element. There is a homomorphism

$$\begin{aligned}(\mathbb{Z}, +) &\to G \\ n &\mapsto g^n.\end{aligned}$$

- The image is $\langle g \rangle$, the subgroup generated by g.
- Therefore $\langle g \rangle$ is a quotient of $(\mathbb{Z}, +)$, i.e., a cyclic group.
- The *order* of g is the order of $\langle g \rangle$.
- If g has infinite order, then $\langle g \rangle \cong \mathbb{Z}$.
- If g has order $n < \infty$, then $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Remark

If G is finite, then the order of g is finite and divides $|G|$.

The order of an element

Consider the element -1 in the multiplicative group $\mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot)$.

- The homomorphism $\mathbb{Z} \to \mathbb{R}^\times$ is $n \mapsto (-1)^n$.
- The image is $\langle -1 \rangle = \{+1, -1\}$.
- This is isomorphic to $\mathbb{Z}/2\mathbb{Z}$
- -1 has order 2.

Section 2

Free groups and presentations

The free group on $\{a, b, c\}$

Idea: The free group on $\{a, b, c\}$ is the "most general" group F generated by a, b, c.

- Every element of F will be a product of $a, b, c, a^{-1}, b^{-1}, c^{-1}$.
- The only equations which hold in F are ones which must necessarily hold.

The free group on $\{a, b, c\}$

- Let Σ be the set of strings in the alphabet $\{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$.
- Say that $s, t \in \Sigma$ are "equivalent" if you can get from s to t by inserting and deleting substrings of the form xx^{-1} or $x^{-1}x$, with $x \in \{a, b, c\}$.
  - For example, $abb^{-1}c \sim ac \sim aca^{-1}a \sim aca^{-1}bb^{-1}a$.
- Let F be Σ modulo equivalence. String concatenation defines a group operation on F.
- F is called the *free group* on $\{a, b, c\}$.

The free group on $\{a, b, c\}$

Say that a string $s \in \Sigma$ is "reduced" if s contains no substring of the form xx^{-1} or $x^{-1}x$ for $x \in \{a, b, c\}$.

Fact

Every string in Σ is equivalent to a unique reduced string.

So we could have constructed F as the set of reduced strings, with the group operation

$$s \cdot t = (\text{the unique reduced string equivalent to the concatenation } st).$$

For example, if $s = ab^{-1}$ and $t = bc$, then

$$s \cdot t = ab^{-1}bc = ac.$$

Free groups

The *free group* on a set S is constructed similarly.

- S can be empty or infinite.
- When $S = \{a\}$, the free group is simply $\{a^n : n \in \mathbb{Z}\}$. This is isomorphic to $(\mathbb{Z}, +)$.

Presentations

Idea: notation like

$$\langle a, b, c \mid abc = cba,\; a^2 = b \rangle$$

means

> *The most general group generated by three elements a, b, and c, such that $abc = cba$ and $a^2 = b$.*

Presentations

We can construct $\langle a, b, c \mid abc = cba,\ a^2 = b\rangle$ just like the free group on $\{a, b, c\}$, except that we change "equivalence":

- Two strings s, t are "equivalent" if you can get from s to t by the following operations:
  - Inserting or deleting a substring of the form xx^{-1} or $x^{-1}x$ for some $x \in \{a, b, c\}$ (as before).
  - Replacing a substring abc with cba, or vice versa.
  - Replacing a substring aa with b, or vice versa.

For example, $cba = abc = aaac = bac$.

Warning

In general, there is no algorithm to tell when two strings are equivalent, unlike the case of free groups.

Presentations

A more abstract construction of $G = \langle a, b, c \mid abc = cba,\ a^2 = b \rangle$ is as follows:

- Let F be the free group on $\{a, b, c\}$.
- Let N be the smallest normal subgroup of F containing $(abc)(cba)^{-1}$ and $(a^2)b^{-1}$.
- Then G is F/N.

An example presentation

- Let S_n be the nth symmetric group, the set of permutations/bijections of $\{1, 2, \ldots, n\}$.
- For $1 \leq i < n$, let σ_i be the transposition which swaps i and $i+1$:

$$\begin{aligned}
\sigma_i(i) &= i+1 \\
\sigma_i(i+1) &= i \\
\sigma_i(x) &= x \text{ if } x \neq i, i+1.
\end{aligned}$$

Fact

S_n has the following presentation:

$$\begin{aligned}
\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \mid & \sigma_1^2 = \sigma_2^2 = \cdots = \sigma_{n-1}^2 = 1, \\
& \sigma_i\sigma_j = \sigma_j\sigma_i \textit{ whenever } |i-j| > 1, \\
& \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \textit{ whenever } |i-j| = 1\rangle.
\end{aligned}$$

Section 3

Around classification

Direct products

Let G, H be groups. The *direct product* is $G \times H$ with the group operation given by

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

Example

The direct product of $(\mathbb{R}, +)$ and $(\mathbb{R}, +)$ is $\mathbb{R}^2$ with the group operation of vector addition

$$(x, y) + (x', y') = (x + x', y + y').$$

Example

The direct product of $(\mathbb{R}, +)$ and $\mathbb{R}^\times$ is the set $\{(x, y) \in \mathbb{R}^2 : y \neq 0\}$, with the group operation given by

$$(x, y) \cdot (x', y') = (x + x', yy').$$

Finite abelian groups

Fact

Every finite abelian group is a direct product of zero or more finite cyclic groups

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

This gives a classification of finite abelian groups.

Remark

Actually, there is some redundancy. For example,

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Finite groups

Can we hope for a classification of finite groups?

- Theoretically, yes.
- Practically, no. (There are too many finite groups.)

Simple groups

Definition

A group G is *simple* if the only normal subgroups of G are $\{1\}$ and G.

Intuition:

- Simple = "prime."
- If G is *not* simple, then G decomposes into smaller groups G/N and N.

Decomposition into simple groups

Fact

Let G be a finite group. Then there is a chain of subgroups

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

such that G_{i-1} is a normal subgroup of G_i and the quotient G_i/G_{i-1} is a simple group.

Fact (Jordan-Hölder)

The length of the chain n is uniquely determined. The quotient groups G_i/G_{i-1} are uniquely determined up to isomorphism and permutation.

Intuition: the G_i/G_{i-1} are the "prime factors" of G.

Strategy for classifying finite groups

To classify finite groups,

1. Classify finite simple groups.
2. Classify the ways to "re-assemble" G from its simple factors.

Finite simple groups

Finite simple groups have been classified, but the classification theorem is VERY hard to prove.

The simplest simple groups

- If p is prime, then the cyclic group $\mathbb{Z}/p\mathbb{Z}$ is simple.
  - These are the only abelian simple groups.
- Let S_n be the nth symmetric group. There is a homomorphism $sgn : S_n \to \{\pm 1\}$ such that $sgn(\tau) = -1$ for any transposition τ. The kernel of sgn is a subgroup $A_n \subseteq S_n$ of index 2, called the *alternating group*. If $n \geq 5$, then A_n is a simple group.

The first few simple groups are

$$\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/7\mathbb{Z}, \ldots, A_5, A_6, A_7, A_8, \ldots$$

The classification of finite simple groups

The finite simple groups are:

1. Cyclic groups of prime order.
2. Alternating groups A_n, for $n \geq 5$.
3. The simple groups of Lie type.
    - Sort of like $GL_n(\mathbb{R})$, if you replace $\mathbb{R}$ with a finite field.
4. 26 other groups, the "*sporadic* groups"
    - The five Mathieu groups, the four Janko groups, the three Conway groups, the three Fischer groups, the Higman-Sims group, the McLaughlin group, the Held group, the Rudvalis group, the Suzuki sporadic group, the O'Nan group, the Harada-Norton group, the Lyons group, the Thompson group, the baby monster group, and the monster group.

Re-assembling groups

If we know $H = G/N$ and N, can we determine G?

- This is called the *extension problem*
- One solution is $G = H \times N$, but there are usually other solutions.
- In theory, there is a method to find all the solutions.
- In practice, there are too many solutions.

Fact

If G has order 128, then the simple factors of G must be

$$\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}.$$

But there are more than 2000 possibilities for G.

Section 4

Solvable and nilpotent groups

Characteristic subgroups

Definition

A *characteristic subgroup* of G is a subgroup $H \subseteq G$ such that $\sigma(H) = H$ for any automorphism $\sigma \in G$.

- Any subgroup of G defined in a "natural" way will be a characteristic subgroup.
- Characteristic subgroups are normal subgroups.

The derived subgroup

- The *commutator* of two elements xy is $[x, y] := xyx^{-1}y^{-1}$.
- $[x, y] = 1$ iff $xy = yx$ (x and y commute).
- The *derived subgroup* or *commutator subgroup* G' is the subgroup of G generated by commutators.
  - When G is abelian, $[x, y] = 1$ for all x, y, so $G' = \{1\}$.
- The derived subgroup is a characteristic subgroup.

Fact

The derived subgroup is the smallest normal subgroup N such that G/N is abelian.

The quotient G/G' is called the *abelianization* of G.

Solvable groups

Let G be a group.

- Recursively define $G_0 = G$ and $G_{i+1} = G_i'$ (the derived subgroup).
- If $G_n = \{1\}$ for some finite n, then G is said to be *solvable*.
- The term "solvable" comes from Galois theory.

Solvable groups

- If G is abelian, then G is solvable.
- If G is simple and non-abelian, then G is *not* solvable.
- If G is solvable, then any subgroup or quotient group of G is solvable.
- If N is a normal subgroup of G, then G is solvable if and only if N and G/N are solvable.
- If G, H are solvable, then $G \times H$ is solvable.

Solvable finite groups

Fact

Let G be a finite group. Then G is solvable iff every simple factor is abelian, iff every simple factor is $\mathbb{Z}/p\mathbb{Z}$ for various p.

Fact (Burnside *pq*-theorem)

Let G be a finite group. If $|G|$ is divisible by only two primes, i.e., $|G| = p^k q^j$ for some primes p, q, then G is solvable.

Fact (Feit-Thompson theorem, VERY HARD)

Let G be a finite group. If $|G|$ is odd, then G is solvable.

The Burnside and Feit-Thompson theorems use *representation theory*.

The center

The *center* of G, written $Z(G)$ or $C(G)$, is the subgroup

$$Z(G) = \{g \in G \mid \forall h \in G : gh = hg\}.$$

- $Z(G)$ is a characteristic subgroup of G.
- $Z(G)$ is abelian.
- $Z(G) = G$ if and only if G is abelian.

Nilpotent groups

Let G be a group.

- Recursively define $G_0 = G$, and $G_{i+1} = G_i/Z(G_i)$.
- If $G_n = \{1\}$ for some n, then G is said to be *nilpotent*.
- The term "nilpotent" comes from Lie theory.

Nilpotent groups

- If G is abelian, then G is nilpotent.
- If G is nilpotent, then G is solvable.
- If G is nilpotent, then any subgroup or quotient group of G is nilpotent.
- If G, H are nilpotent, then $G \times H$ is nilpotent.

p-groups

Definition

A *p-group* is a finite group whose order is a power of p.

Fact

Let G be a finite group. Then G is a p-group iff every simple factor of G is $\mathbb{Z}/p\mathbb{Z}$, the cyclic group of order p.

Fact

Every p-group is nilpotent.

Fact

A finite group G is nilpotent if and only if G is a direct product of p-groups for various p.

Sylow subgroups

Let G be a finite group and p be a prime.

Definition

A *p-subgroup of G* is a subgroup that is a p-group.
A *p-Sylow subgroup* of G is a maximal p-subgroup.

Sylow subgroups

Theorem (Sylow)

Let G be a finite group of order n. Write n as $p^k m$ where m is not divisible by p.

1. *Every p-Sylow subgroup has order p^k.*
2. *If H, K are two different p-Sylow subgroups, then H and K are isomorphic and conjugate.*

Example

Let G be any finite group. Let H be a 2-Sylow. Then H is a 2-group, and the index $|G/H|$ is odd.

This can be used to prove the fundamental theorem of algebra.

Sylows and nilpotence

The following are equivalent for a finite group G and a prime p:

- One p-Sylow subgroup of G is normal.
- All p-Sylow subgroups of G are normal.
- There is exactly one p-Sylow subgroup of G.

The following are equivalent for a finite group G:

- G is nilpotent.
- For every prime p, there is a unique p-Sylow.
- Every p-Sylow is a normal subgroup.
- G is a direct product of its Sylow subgroups.