Lecture 09

Melissa Zhang

MAT 150A

Participation Slip

1. Take a slip from the front of the room.
2. Write your full name on the top left corner.
3. You will write down your answer to some clearly marked "Participation Slip" questions during lecture.
4. Hand in your slip at the end of class, in the pile according to the first letter of your surname.

Index of a Subgroup

Definition

The number of left cosets of a subgroup $H \leq G$ is the **index** of the subgroup, denoted $[G : H]$.

The Counting Formula

For $H \leq G$,

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

Participation Slip

Prove the Counting Formula.

Hint: You'll need a lemma we proved last week.

Counting Formula: For $H \leq G$, $|G| = |H| \cdot [G : H]$.

Corollary

Let G be a finite group.

- (Lagrange's Theorem) If $H \leq G$, then $|H|$ divides $|G|$.
- The order of an element $g \in G$ divides $|G|$.

Participation Slip

Let G be a group of prime order p. Prove that any non-identity element $a \in G$ generates the entire group, i.e. $G = \langle a \rangle$.

The above corollary to the Counting Formula **classifies** groups of prime order p.
They form a single isomorphism class, the class of C_p.

Counting Formula: For $H \leq G$, $|G| = |H| \cdot [G : H]$.

Corollary

Let $\varphi : G \to G'$ be a homomorphism of finite groups.

- $[G : \ker \varphi] = |\operatorname{im} \varphi|$, and hence $|G| = |\ker \varphi||\operatorname{im} \varphi|$
- $|\ker \varphi|$ divides $|G|$
- $|\operatorname{im} \varphi|$ divides both $|G|$ and $|G'|$.

Question

Recall that the alternating group A_n is the kernel of the sign homomorphism

$$\operatorname{sgn} : S_n \to \{\pm 1\}.$$

What is the order of A_n?

Multiplicative Property of the Index

Proposition (Multiplicative Property of the Index)

Suppose we have a chain of subgroups of G

$$K \leq H \leq G.$$

Then

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

The proof of this proposition is quite instructive. If there is some part of it you don't understand, go back and review the section on cosets.

Remark about Right Cosets

- We've been talking about *left cosets*, but could equally well have proven all these theorems for *right cosets*.
- Before Exam 1 (next week!), we will talk about right cosets as a way to review the material.

When are two groups "the same"?

When looking at a specific category of things, we care about (1) the objects themselves and (2) the maps between them, and oftentimes also (3) the notion of *equivalence* between the objects.

Sets

Two sets A and B are ~~basically the same~~ "equivalent" if they are in bijective correspondence,
i.e. there exists a bijection $\varphi : A \to B$.

- Then $\varphi^{-1} : B \to A$ is also a bijection.
- In fact, being "in bijection" is an equivalence relation on (any set of)[a] sets.
- We call the equivalence classes "cardinality".

[a] Russell's paradox + our definition of equivalence relation

Isomorphisms

Definition

An **isomorphism** is a bijective homomorphism.

This is the notion of equivalence among groups.

Examples

- $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$
  - How does this compare with the homomorphism $\exp : \mathbb{R}^+ \to \mathbb{R}^\times$?
- Let $a \in G$ have infinite order. Then $n \mapsto a^n$ is an isomorphism $\mathbb{Z} \to \langle a \rangle$.
- Let $\mathcal{P}$ be the subgroup of $GL_n(\mathbb{R})$ consisting of $n \times n$ permutation matrices. Then there is an isomorphism $S_n \to \mathcal{P}$ sending a permutation to its associated permutation matrix.

Isomorphisms

Lemma 2.6.2

If $\varphi : G \to G'$ is an isomorphism, then the inverse (set) map $\varphi^{-1} : G' \to G$ is also an isomorphism.

Two groups G, G' are **isomorphic** if there exists an isomorphism $\varphi : G \to G'$.

- They are functionally the same group, i.e. you can do your calculations with $a \in G$ or $\varphi(a) \in G'$. The group laws work exactly the same way.
- This **does not** mean that they are literally the same group.
  - In most contexts, the difference between equality ($=$) and equivalence ($\cong$) doesn't really matter, so we will casually say $\mathcal{P}$ "is" S_n.
  - ... But sometimes it does matter!

Conventions, Conventions, Conventions

Conventions change, and differ between mathematical fields, generations of mathematicians, and between individual mathematicians.

- My notation: $G \cong G'$, $g \mapsto g'$
- Artin's notation: $G \approx G'$, $g \rightsquigarrow g'$

Endomorphisms and Automorphisms

Definition

- An **endomorphism** is a *homomorphism* from G to itself.
  - E.g. $2\cdot : \mathbb{Z} \to \mathbb{Z}$
- An **automorphism** is an *isomorphism* from G to itself.
  - E.g. $2\cdot : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$

Another automorphism

Let G be a group, and fix $g \in G$. Then "conjugation by g" is an automorphism:

$$g\bullet : G \to G$$
$$a \mapsto gag^{-1}.$$

Exercises

Q: What are all the automorphisms of a cyclic group C_n?

Hints:

- Let g be a generator.
- What if n is prime?

Q: What are all the automorphisms of the symmetric group S_3?

Hints:

- What are the obvious ones?
- What does an automorphism have to preserve about each element?