Math 250A: Graduate Abstract Algebra

Tyler Zhu

August 27, 2020

> *"A good stock of examples, as large as possible, is indispensable for a thorough understanding of any concept, and when I want to learn something new, I make it my first job to build one."*
>
> – *Paul Halmos.*

These are course notes for the Fall 2020 rendition of Math 250A, Graduate Abstract Algebra, taught by Professor Ken Ribet.

Contents

1 Thursday, August 27

1.1 Groups

A *group* is a set G together with a binary product mapping from $G \times G \mapsto G$ which satisfies the following axioms:

- G is associative, i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c)$ for all $a, b, c \in G$,
- G has an identity element e for which $ge = eg = g$ for all $g \in G$, and
- each $g \in G$ has a two-sided inverse, i.e. an element $a \in G$ such that $ag = ga = e$.

Sometimes closure is mentioned here, but that's inherent when we defined the binary product as one which maps to G.

We can easily show that this identiy must be unique, for if we had two identities e, e', then $e = ee' = e'$.

An *Abelian* group is one which is also commutative, i.e. for all $a, b \in G$, $ab = ba$.

Example 1.1 (Examples of abelian groups)**.** Here are some simple examples of abelian groups.

- The trivial group $G = \{e\}$ is abelian.
- The set of rational numbers under addition, $\mathbb{Q}$.
- The second is the group of nonzero rational numbers under multiplication, $\mathbb{Q}^\times$, i.e. the multiplicative group. The group action is denoted by $x, y \mapsto xy$ or $x \cdot y$.

A group G is *cyclic* if there is $g \in G$ so that $G = \{g^n | n \in \mathbb{Z}\}$, where $g^n = g \cdot g \ldots g$ (n times) if $n > 0$ and $g^n = (g^{-1})^n$ when $n < 0$, and $g^0 = e$ by definition. The element g is called the *generator* of the group.

If we wrote this additively, we would write this as $G = \{n \cdot g | n \in \mathbb{Z}\}$.

Example 1.2 (Examples of Cyclic Groups)**.** Some examples of cyclic groups.

- The set of integers, $\mathbb{Z}$, itself. $1 \in \mathbb{Z}$ is one of the two generators (-1 being the other).
- The set of integers mod n is also a cyclic group under addition, noted as $\mathbb{Z}/n\mathbb{Z}$.
- The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, defined as
$$\{a \in \mathbb{Z}/n\mathbb{Z} | \gcd(a, n) = 1\},$$
when n is a prime number, which we will prove later in this course.

The last example above lends itself to a broader generalization. Here's a taste of what's to come...

Theorem 1. Let $F^\times$ be the group of nonzero elements of a field F (under multiplication). If $G \subseteq F^\times$ is a finite subgroup, then G is cyclic.

For example, the nth roots of unity are finite subgroups of $\mathbb{C}^\times$, and hence are also cyclic. We knew that already though, since they're generated by $e^{2\pi i/n}$.

Example 1.3. If V is a vector space over K, the set of invertible linear maps $T : V \to V$ forms a group under composition, called the *general linear* group $\mathrm{GL}(V)$.

If $V = K^n$, then $\mathrm{GL}(V) = \mathrm{GL}(n, K)$, the group of invertible $n \times n$ matrices with coefficients in K. The *special linear* group $\mathrm{SL}(n, K)$ is the subgroup with determinant 1.

Suppose we wanted to construct an element of $\mathrm{GL}(n, K)$ using this matrix interpretation. We can approach it by building it column by column, keeping in mind to make the columns linearly independent so that the determinant is not 0. In other words, if this matrix is $[C_1\ C_2 \dots C_n]$ where the C_i are the columns, then we want $C_i \notin \mathrm{Span}(C_1, \dots, C_{i-1})$ for $i > 1$ and that C_1 is not the zero vector.

Let K be a finite field now, with order $q = |K|$, like $\mathbb{Z}/q\mathbb{Z}$. What is $|\mathrm{GL}(n, K)|$?

We can count by counting the choices we have for each column. For $C_1 \in K^n$, it just needs to be non-empty, so we have $q^n - 1$ choices. For C_2, we need $C_2 \notin \mathrm{Span}(C_1) = \{\text{multiples of } C_1\}$. There are q multiples, so we have $q^n - q$ choices for C_2.

In general, the number of possibilities for C_i is $q^n - q^{i-1}$ since the span of $i-1$ linearly independent vectors in K is isomorphic to K^{i-1}, which has q^{i-1} elements. Multiplying everything up gives the total order of the group as

$$\mathrm{GL}(n, K) = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}).$$

If $\sum$ is a set, the set of invertible maps $f : \sum \to \sum$ forms a group under composition called the *symmetric* group on the set $\sum$. Notation is S_Σ, but Lang calls it $\mathrm{Perm}(\sum)$. Borrowing notation from combinatorics, we let $[n] = \{1, 2, \dots, n\}$, so that the symmetric group on n elements is $\mathrm{Perm}([n]) = S_{[n]}$.

Remark. The examples $\mathrm{GL}(V)$ and $\mathrm{Perm}(\Sigma)$ are special examples of a construction where the set of automorphisms is a group (category theory makes this precise).

Remark. When Lang was alive, he'd yell at Berkeley undergrads who'd tell him that a morphism $X \to Y$ is invertible iff it is 1-1 and onto. Mostly true, but false in simple example. For example, the map x^3 from $(-1, 1) \mapsto (-1, 1)$ in the category of differentiable maps has a set-theoretic inverse $x^{1/3}$, which is nondifferentiable at $x = 0$.

We can form subgroups of groups. Some special ones are the cosets of G. If $H < G$, the set G/H is the set of subsets of G of the form gH (for g in G). These are called the *left cosets* of H in G.

Similarly, $H \setminus G$ is the set of *right* cosets Hg with $g \in G$.

Left cosets are the equivalence classes for the equivalence relation $x \sim y \iff x^{-1}y \in H$, while right cosets are equivialence classes for $x \sim y \iff xy^{-1} \in H$.

The cosets gH all have the same cardinality, i.e. the map $h \mapsto gh$ is a bijection. The group G is the disjoint union of the distinct cosets gH since they're all equivalence classes. Thus,

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = [G : H] \cdot |H|.$$

In particular, when G is a finite group, the order of every subgroup $H < G$ divides the order of G, which is Lagrange's theorem.

1.2 Homomorphisms

Note: homomorphisms are the morphisms in the category of groups!

If X and Y are groups, the *trivial* homomorphism $X \to Y$ is the map that takes everything to the identity of Y.

The floor (or greatest integer map)

$$\lfloor \cdot \rfloor : \mathbb{Q} \to \mathbb{Z}, x \mapsto \lfloor x \rfloor$$

is *not* a homomorphism since $\lfloor \frac{3}{4} \rfloor + \lfloor \frac{3}{4} \rfloor \neq \lfloor \frac{3}{2} \rfloor = 1$.

The identity map on X is a homomorphism $X \to X$.

If A is abelian and n is an integer, the nth power map $a \mapsto a^n$ is an endomorphism of A (i.e. a homomorphism from a group to itself, especially when the group is abelian).

The determinant map is a homomorphism $\mathrm{GL}(n, K) \to K^{\times}$ when $n > 0$ and K is a field.

A subgroup N of G is normal if for all $g \in G$, $gNg^{-1} \subseteq N$. As we've learned before, the kernel of a homomorphism is normal. In this case, the "canonical" quotient map

$$\pi : G \to G/N, g \mapsto gN$$

is a homomorphism with kernel N.