Math 110B (Algebra)
University of California, Los Angeles

Aaron Chao

Winter 2022

These are my lecture notes for Math 110B (Algebra), which is the second course in Algebra taught by Nicolle Gonzales. The textbook for this class is *Abstract Algebra: An Introduction, 3rd edition* by Hungerford.

Contents

1 Jan 3, 2022 **2**
1.1 Groups 2

2 Jan 5, 2022 **4**

1 Jan 3, 2022

1.1 Groups

- Algebra $\rightarrow$ study of mathematical structure.
- Rings $\leftrightarrow$ "numbers" e.g. $\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Z}_p$
  2 operations $(+, \cdot)$

Question 1.1: What happens if we have only 1 operation (either $\cdot$ or $+$ but not both)? What kind of structure is this more basic setup?

Answer: Groups! It turns out groups encode the mathematical structures of the symmetries in nature.

Definition 1.2 (Group)
A group $(G, *)$ is a nonempty set with a binary operation $* : G \times G \to G$ that satisfies

1. (Closure): $a * b \in G \quad \forall a, b \in G$
2. (Associativity): $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$
3. (Identity): $\exists e \in G$ such that $e * a = a = a * e \quad \forall a \in G$
4. (Inverse): $\forall a \in G, \exists d \in G$ such that $d * a = e = a * d$

Note:

- If * is addition, we just divide * by the usual + sign. In this case

$$e = 0 \quad \text{and} \quad d = -a$$

- If the operation * is multiplication, we just divide * by the usual $\cdot$ sign. In this case

$$e = 1 \quad \text{and} \quad d = a^{-1}$$

- Be aware that sometimes * is neither.

Definition 1.3 (Abelian)
If the * operation is commutative, i.e. $a * b = b * a$, then we say that G is abelian (named after the mathematician N.H. Abel)

Definition 1.4 (Order, Finite Group vs. Infinite Group)
The order of a group G, denoted $|G|$, is the number of elements it contains (as a set). Thus, G is a finite group if $|G| < \infty$
and G is an infinite group if $|G| = \infty$

Examples 1.5 (Examples of a group)

1. Rings where you "forget" multiplication.
   $\rightarrow (\mathbb{Z}, +)$ integers with $* = +, (\mathbb{R}[X], +)$, etc.
   Note: $(\mathbb{Z}, *)$ with $* = \cdot$ is not a group. Why?

Theorem 1.6
Every ring is an abelian group under addition.

Proof. $e = 0$, inverse $= -a$ for each $a \in R$. □

Fact: If $R \neq 0$ then $(R, \cdot)$ is never a group since 0 has no multiplicative inverse.

Examples 1.7 (More examples of a group)

2. Fields without zero.

Theorem 1.8
Let $\mathbb{F}^*$ denote the nonzero elements of a field $\mathbb{F}$. Then $(\mathbb{F}^*, \cdot)$ is an abelian group.

Recall: A unit in a ring R is an element $a \in R$ with a multiplicative inverse $a^{-1} \in R$ such that $aa^{-1} = 1 = a^{-1}a$.

Theorem 1.9
The set of units $\mathcal{U}$ inside a ring R is a group under multiplication.

Examples 1.10 (More examples of a group cont.)

3. $\mathcal{U}_n = \{m | (m, n) = 1\} \subseteq \mathbb{Z}_n$ is also a group, but under multiplication,

   $\underline{n = 4}$ $\quad \mathbb{Z}_4 = \{0, 1, 2, 3\}, \quad \mathcal{U}_4 = \{1, 3\}$

   $(\mathbb{Z}_4, +)$ and $(\mathcal{U}_4, \cdot)$ are groups with different binary operation!

   $\underline{n = 6}$ $\quad \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}, \quad \mathcal{U}_6 = \{1, 5\}$

   $(\mathcal{U}_6, \cdot)$ is a group

   - $1 \cdot 5 = 5 \pmod 6 \in \mathcal{U}_6$ (closure)
   - $1 = e$ (identity)
   - $1 \cdot 1 = 1, \quad 5 \cdot 5 = 25 \equiv 1 \pmod 6$ (inverse)

2 Jan 5, 2022