GROUP THEORY

Manish Kumar, notes by Ramdas Singh

Third Semester

List of Symbols

Placeholder

Contents

Chapter 1

INTRODUCTION TO GROUP THEORY

1.1 Set Theory

July 22nd.

We begin with some basic assumptions to introduce set theory. The symbol $\in$ is used to denote membership in a set. A statement using this in set theory may be stated as $x \in y$, which can be either true or false. Once we have developed this language to discuss sets, we can introduce some axioms.

Axiom 1.1. There exists a set with no elements, the *empty set* $\emptyset$.

Formally, the above axiom is $\exists x(\forall y(y \notin x))$.

Axiom 1.2. Two sets are equal if they have the same elements.

From the above two axioms, we can infer a unique empty set. A notion of subsets may also be declared.

Definition 1.3. We say the set A is a *subset* of the set B, denoted $A \subseteq B$, if every element of A is also an element of B.

We also have a bunch of similarity axioms stated below.

Axiom 1.4 (Similarity axioms)**.** We have the following:

1. If x, y are sets, then $\{x, y\} \Rightarrow \{x, \{x, y\}\}$ (not an ordered pair).
2. If A is a set, then $\bigcup A = \{x \mid \exists y \in A,\ x \in y\}$ is a set.
3. There exists a *power set* for every set; given a set A, there exists a set $P(A)$ such that for all $B \subseteq A$, $B \in P(A)$. Formally, $\forall A \exists P(A)(\forall B \subseteq A, B \in P(A))$.
4. The *infinite axiom*: Formally, $\exists I(\emptyset \in I \wedge \forall y \in I(P(y) \in I))$.
5. If A and B are sets, then $A \times B = \{(x, y) \mid x \in A, y \in B\}$ is a set.

Before discussing the last axiom, we define a relation on sets.

Definition 1.5. A *relation* R on a set A is a subset $R \subseteq A \times A$. If $(x, y) \in R$, we write xRy.

Axiom 1.6 (The *axiom of choice*)**.** Let A be a collection of non-empty and disjoint sets. Then there exists a set C consisting of exactly one element from each set in A.

Definition 1.7. A relation R on a set A is said to be:

- *reflexive* if $xRx \forall x \in A$,
- *symmetric* if $xRy \Rightarrow yRx$,
- *transitive* if $xRy \wedge yRz \Rightarrow xRz$,
- *antisymmetric* if $xRy \wedge yRx \Rightarrow x = y$.

Definition 1.8. A *partial order* on a set A is a reflexive, transitive, and antisymmetric relation on A.

Some examples of partially ordered sets include $(R, \leq)$, $(P(\mathbb{R}), \subseteq)$.

Definition 1.9. A *total order* R on a set A is a partial order such that for all $x, y \in A$, either xRy or yRx.

Again, $(R, \leq)$ is a totally ordered set, but not $(P(\mathbb{R}), \subseteq)$.

Definition 1.10. A total order $\leq$ on a set A is said to be a *well-order* if given any non-empty subset $B \subseteq A$, there exists $x \in B$ such that for all $y \in B$, $x \leq y$.

The below theorem may be derived from the above definitions and axioms.

Theorem 1.11 (The *well-ordering principle*)**.** *Every set can be well-ordered.*

We may note that the well-ordering principle and the axiom of choice are equivalent.

Definition 1.12. A *chain* in partially ordered set A, with relation $\prec$, is a subset of A which is totally ordered with respect to $\prec$.

Definition 1.13. Let $C \subseteq A$ be a subset in a partially ordered set $(A, \prec)$. An element $x \in A$ is an upper bound of C if for all $y \in C$, $y \prec x$.

Definition 1.14. An element $x \in A$ is a *maximal element* of a partially ordered set $(A, \prec)$ if for all $y \in A$, $x \prec y \Rightarrow x = y$.

Lemma 1.15 (*Zorn's lemma*)**.** *Let A be a set and let $\prec$ be a partial order on A such that every chain in A has an upper bound. Then A has a maximal element.*

Theorem 1.16. *The following are equialent:*

1. *The axiom of choice,*
2. *The well-ordering principle,*
3. *Zorn's lemma.*

Definition 1.17. A relation R on a set A is said to be an *equivalence relation* if it is reflexive, symmetric, and transitive. Let $x \in A$. Then $[x] = \{yRx \mid y \in A\} \subseteq A$ is called the *equivalence class* of x.

We note that $\bigcup_{x\in A}[x] = A$ and for $x, y \in A$, either $[x] \cap [y] = \emptyset$ or $[x] = [y]$. Thus, we get a partition of A into equivalence classes.

Let I be an indexing set, and let A_i be sets for all $i \in I$. Then the existence of $\mathrm{X}_{i\in I} A_i = \{f : I \to \dot{\bigsqcup} A_i \mid f(i) \in A_i \text{ for all } i \in I\}$ is another way of stating the axiom of choice.

Theorem 1.18 (The *principle of induction*)**.** *Let $S(n)$ be statements about the naturals $n \in \mathbb{N}$. Suppose $S(1)$ holds and for all $k \in \mathbb{N}$, $S(k) \Rightarrow S(k+1)$. Then $S(n)$ holds true for all $n \in \mathbb{N}$.*

Let I be a well-ordered set and let $S(i)$ be statements for all $i \in I$. Suppose that if $S(j)$ holds for all $j < i$, then $S(i)$ holds. Then $S(i)$ holds for all $i \in I$. This is the *principle of transfinite induction*, which is also equivalent to the axiom of choice. We now properly introduce the theory of groups.

1.2 Groups

We first define a group.

Definition 1.19. A *group* is a triple $(G, \cdot, e)$ where G is a set, $\cdot : G \times G \to G$ is a binary operation on G, and $e \in G$ is an element of G satisfying the following axioms:

- The property of *associativity*: For $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- The property of the *identity element*: For all $a \in G$, $a \cdot e = e \cdot a = a$. e is referred to as the identity element.
- The existence and property of the *inverse element*: For all $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = e$. b is referred to as the inverse of a and is denoted by a^{-1}.

In addition, $(G, \cdot, e)$ is also termed an *abelian group* if for all $a, b \in G$, $a \cdot b = b \cdot a$, that is, commutativity holds.

Some examples include $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$. The set $(\mathbb{Q}, \cdot)$ is not a group since 0 does not have an inverse. However, $(\mathbb{Q}^*, \cdot)$ is a group, where $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. All these groups are also abelian. An example of a non-abelian group is S_n, the set of all bijections from $\{1, 2, \ldots, n\}$ to itself, under the binary operation of composition of functions. Another non-abelian group is $(GL_n(\mathbb{R}), \cdot)$, for $n \geq 2$, the set of all invertible real matrices.

Index