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.*

Proof. We begin with 2. implies 3.; let A be a non-empty set. Consider

$$\mathcal{C} = \{(B, \leq) \mid B \subseteq A \text{ and } \leq \text{ is a well-order on } B\}. \tag{1.1}$$

We note that $\mathcal{C}$ is non-empty since if we pick $B = \{x\}$ for some $x \in A$, then $x \leq x$ and $(B, \leq) \in \mathcal{C}$. Let $(B, \leq), (C, \leq') \in \mathcal{C}$. We say $(B, \leq) \preceq (C, \leq')$ if there exists $y \in C$ such that

$$B = \{x \in C \mid x \lneq' y\} \; (= I(c, y)) \text{ and } \leq = \leq'|_B, \text{ or } (B, \leq) = (C, \leq') \tag{1.2}$$

Note that $\preceq$ is a partial order on $\mathcal{C}$ and is clearly reflexive.

For transitivity, if we take $B \preceq C$ and $C \preceq D$, then $B = C$ or $B = I(C, y)$ for some $y \in C$, and $C = D$ or $C = I(D, z)$ for some $z \in D$. If equality holds in either case, then clearly $B \preceq D$. If $B = I(C, y)$ and $C = I(D, z)$. Clearly, $B = I(D, y)$.

Now let $T = (\{(B_i, \leq_i) \mid i \in I\})$ be a chain in $\mathcal{C}$. Let $B = \bigcup_{i \in I} B_i$, and $\leq = \bigcup_{i \in I} \leq_i$. Note that this makes sense since if $x \in B_i$ and $y \in B_j$ with $B_i \preceq B_j$, then $x, y \in B_j$. So, we assign $x \leq y$ if $x \leq_j y$. Now let $C \subseteq B$ be non-empty. Also let $x \in C$; then $x \in B_i$ for some $i \in I$. Let $w = \min(B_i \cap C)$. We claim that $w = \min C$. For $y \in C$, if $y \in B_i$ then $w \leq y$. If $y \notin B_i$ then $y \in B_j \in T$. Since T is a chain, either $B_i \preceq B_j$ or $B_j \preceq B_i$; the latter is not possible since $y \notin B_i$. Thus, $B_i = I(B_j, z)$, for some $z \in B_j$, and for any $x \in B_i$, $w \leq x \leq y$.

So $(B, \leq) \in \mathcal{C}$ and it is an upper bound of T; to realize it is an upper bound, we show that $B_i \preceq B$ for all valid i. If $B_i = B$, we are done. Otherwise, let $x = \min(B \setminus B_i)$. Then $B_i = I(B, x)$, and $B_i \preceq B$. Thus, by Zorn's lemma, $\mathcal{C}$ has a maximal element— cal it $(M, \leq)$.

We now claim that $M = A$. If $M \subsetneq A$, then let $a \in A \setminus M$. If we let $\hat{M} = (M \cup \{a\}, \leq')$ where $x \leq' a$ for all $x \in M$, then $M = I(\hat{M}, a)$ but this is a contradiction to the fact that $(M, \leq)$ is a maximal element. Thus, $A = M$.

Next comes 1. implies 3. Let X be a partially ordered set such that every chain has an upper bound. Suppose X has no maximal element; we will utilise the axiom of choice to arise at a contradiction. For every chain T in X, there exists a strict upper bound c_T. Define a function f sending chains T in X to X as $f(T) = c_T \notin T$. Such a function f exists by the axiom of choice. A subset $A \subseteq X$ is called a *conforming subset* if A is well-ordered, with respect to order on X, and for all $x \in A$, $f(I(A, x)) = x$. We claim that if A and B are conforming subsets of X, then $A = B$ or one is the initial segment of the other. For now, let us take this claim to be true. We shall prove it later.

If $f(\emptyset) = x$ then $A = \{x\}$. Note that A is conforming. But $I(A, x) = \emptyset \implies f(I(A, x)) = x$. Let U be the union of all conforming subsets of X. Then U is conforming since if $x \in U$ then $x \in B$ for some B conforming and $x = f(I(B, x)) = f(I(U, x))$. Let $f(U) = w$. Define a new set $\tilde{U} = U \sqcup \{w\}$, which is well-ordered and conforming. Then $U = I(\tilde{U}, w)$, which is a contradiction.

Coming back to the claim, suppose $x \in A \setminus B$. We wish to show that $B = I(A, x)$ for some $x \in A$. Let $x = \min(A \setminus B)$. We claim that this x works. $I(A, x) \subseteq B$ holds since if $y \in A$ and $y < x$ then $y \in B$, or else $x \neq \min(A \setminus B)$. Suppose, now, that the equality does not hold. Take $y = \min(B \setminus I(A, x))$ and $z = \min(A \setminus I(B, y))$. We claim that $I(A, z) = I(B, y)$. Take $v \in I(A, z)$; then $v < z$ implies $v \in I(B, y)$ since $z = \min(A \setminus I(B, y))$. Taking $u \in I(B, y)$, we have $u \in I(A, x) \implies u < x$ since $y = \min(B \setminus I(A, x))$. If $z \leq u$, then $z \in I(A, x) \subseteq B \implies z \in I(B, y)$ contrading the fact that $z = \min(A \setminus I(B, y))$. Thus, $z > u$ and $y \in I(A, z)$. Finally, $z = f(I(A, z)) = f(I(B, y)) = y$ implies $z = x = y$. But this a contradiction since $x \in A \setminus B$ and $y \in B$. ■

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 $a \cdot b = b \cdot a = e$.

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 $n \times n$ matrices.

1.2.1 Some Basic Properties

July 24th.

From the axioms, arise basic properties related to groups.

Proposition 1.20. *Let $(G, \cdot, e)$ be a group.*

1. *Let $a \in G$ be such that $a \cdot b = b$ for all $b \in G$. Then $a = e$; the identity element is unique.*
2. *Each element $a \in G$ has a unique inverse. Thus, the inverse of a is then termed a^{-1}.*
3. *$(a^{-1})^{-1} = a$ holds for all $a \in G$.*
4. *For all $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.*
5. *Let $a \in G$ be such that $a \cdot b = b$ for some $b \in G$. Then $a = e$.*

Proof.

1. Choose b to be e. Then $a \cdot e = e$ by hypothesis, and $a \cdot e = a$ by the property of the identity element. Thus, $a = e$.
2. Let $a \in G$ and $b \in G$ be such that $a \cdot b = b \cdot a = e$. Let $c \in G$ be also such that $c \cdot a = e$. Thus, $(c \cdot a) \cdot b = e \cdot b \Rightarrow c \cdot (a \cdot b) = e \cdot b \Rightarrow c \cdot e = b \Rightarrow c = b$.
3. Easy to see since $a^{-1} \cdot a = a \cdot a^{-1} = e$ which just means that the inverse of a^{-1} is a.
4. Also easy since $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$.
5. Finally, right multiplying b^{-1} leads to $a = a \cdot b \cdot b^{-1} = b \cdot b^{-1} = e$.

■

Index