Math 322 Notes

Henry Xia

September 13, 2018

Contents

1 Introduction

Definition 1.1. A *quotient set is a set $S/\sim$ whose elements are in one to one correspondence with equivalence classes of S. We also write $\overline{S} = S/\sim$.*

Definition 1.2. A *natural map $S \to S/\sim$ is a surjective map to the equivalence classes of S.*

Definition 1.3. A *semigroup is a set S that is closed under multiplication. That is $\forall a, b \in S$, we have $ab \in S$.*

Definition 1.4. A *monoid is a semigroup that has an identity element. That is $\exists 1 \in S$ such that $1a = a1 = a$ for all $a \in S$.*

Definition 1.5. A *group is a monoid where every element has an inverse. That is $\forall a \in S$, there exists some a^{-1} such that $aa^{-1} = 1$.*

Definition 1.6. A *subgroup is a subset of a group that is also a group.*

Definition 1.7. An *Abelian group is a group whose multiplication is commutative.*

Definition 1.8. The *symmetric group on n elements is the set of all permutations of n elements. We denote this as S_n.*

Definition 1.9. A *cyclic group is a group that can be generated by one of its elements. That is $G = \left\{a, a^2, \ldots, a^{n-1}, a^n = 1\right\}$. We say that a generates G.*

Definition 1.10. The *order of a group is the number of elements in the cardinality of the group. The order of an element a is the smallest m such that $a^m = 1$. If no such m exists, we say a has infinite order. This is equivalently the order of the group generated by a.*

Definition 1.11. The *direct product is the cartesian product of the groups, where the group action is defined componentwise.*

Definition 1.12. We say a group G is isomorphic to a group H, or $G \simeq H$, if there exists a bijection from G to H that preserves the group action. That is there exists some bijection $f : G \to H$ such that $f(xy) = f(x)f(y)$.

Example 1.1. The group $\mathbb{R}$ with addition is isomorphic to $\mathbb{R}^*_+$ with multiplication. We can take $f(x) = e^x$, then $f(x + y) = e^{x+y} = e^x e^y = f(x)f(y)$.

Theorem 1.1 (Cayley's Theorem)**.** *Any finite group G is isomorphic to a subgroup of the symmetric group acting on G.*

Proof. Let $G = \{x_1, x_2, \ldots, x_n\}$ have order n. Then for each $a \in G$, define $f_a : G \to G$ where $f_a(x) = ax$. We claim that f_a is a bijection. It suffices to show that f_a is an injection. Suppose that $f_a(x) = f_a(y)$, then $ax = ay \implies a^{-1}ax = a^{-1}ay \implies x = y$.
Let $\phi : G \to S_n$ map each element $a \in G$ to the element of S_n that corresponds to f_a. Now we need to check that ϕ is injective. Indeed, if $\phi(a) = \phi(b)$, then $ax = f_a(x) = f_b(x) = bx \implies a = b$. We also need to check that $\phi(ab) = \phi(a)\phi(b)$. Indeed, $\phi(ab)$ maps x to abx, $\phi(b)$ maps x to bx, and $\phi(a)$ maps bx to abx. □

Example 1.2. Is $(\mathbb{Q}, +)$ isomorphic to $(\mathbb{Q}^*_+, \times)$?
No. Consider $2x = a$, where $a \in \mathbb{Q}$. There exists some $x \in \mathbb{Q}$ for all a. This equation becomes $f(x)^2 = f(a)$ should the two groups be isomorphic, however, it is clear that $f(x)$ does not exist for all $f(a)$.

Example 1.3. Fix $a \in G$, then let $C = \{b \in G : ab = ba\}$. We call a the centralizer. Observe that C is a subgroup of G.
It is obvious that $1 \in C$.
Let $x, y \in C$, then $xya = xay = axy$ by associativity, hence $xy \in C$.
Let $x \in C$, then $x^{-1}a = x^{-1}axx^{-1} = x^{-1}xax^{-1} = ax^{-1}$ by associativity, hence $x^{-1} \in C$.

Definition 1.13. The *center* of a group G is the subgroup $\{a : ax = xa \;\; \forall x \in G\}$.

Remark 1.1. The intersection of subgroups is also a subgroup.