Math 250A Lecture 1 Notes

Daniel Raban

August 24, 2017

1 Groups

1.1 Groups and Actions

Definition 1.1. A *group* is the set of symmetries of something.

Example 1.1. Consider the symmetries of a rectangle. You can:
1: Do nothing
a: Reflect horizontally
b: reflect vertically
c: rotate by π.

Definition 1.2. A *group* is a set G with a binary operation $G \times G \to G$ (usually written $(a, b) \to a + b, a \times b, ab,$ or $a \cdot b$) such that
(1) There is an identity (called e, 1, or 0) such that $ea = a = ae$
(2) Each element has inverse a^{-1} such that $a^{-1}a = aa^{-1} = e$
(3) The operation is associative $(ab)c = a(bc)$.

We must reconcile the two definitions. The first, "concrete" definition can be thought of in the second, "abstract" way by making the operation composition of symmetries. Is the reverse true? Cayley proved that the answer is yes. To show this, we must construct some S with G as the set of its symmetries. G has to act on S. This means we have an action of G on S.

Definition 1.3. An *action* of G on S is a map $G \times S \to S$ such that
(1) $g(h \cdot s) = (gh) \cdot s$ for $s \in S$ and $g, h \in G$
(2) $e \cdot s = s$ for $s \in S$.

Then what is S that satisfies this properties? Well, we can set $S = G$ and make the action on S multiplication by G. This represents G as a subgroup of the symmetries of S; this is not necessarily the group of symmetries of S. But we have shown that G is isomorphic to the set of permutations of a set. Recall:

Definition 1.4. A *subgroup* H of G is a subset of G closed under $\times$ and inverses, containing the identity, e.

Definition 1.5. A *homomorphism* from G to H is a function from G to H preserving $\times$, inverses, and the identity; i.e. $f(ab) = f(a)f(b)$.

Definition 1.6. An *isomorphism* is a homomorphism that is a bijection.

If there is an isomorphism from G to H, then they are essentially the same, up to a relabeling of the elements.

Example 1.2. Let $G = (\mathbb{R}, +)$, and let $H = (\mathbb{R}^*, \times)$ (the nonzero reals). The isomorphism $G \to H$ is the exponential map.

So our new problem is to put some "structure" on $S(= G)$ so that G is the set of all symmetries preserving the structure. The structure is a right action of G on S.

Definition 1.7. A *left* action $G \times S \to S$ is given by $g \cdot s$. A *right* action $S \times G \to S$ is given by $s \cdot g$.

Remark 1.1. The left and right actions of G on S which are different, unless the operation is commutative.

A symmetry $f : S \to S$ preserves a right action of G if $f(s \cdot g) = f(s) \cdot g$. Elements of G acting on left preserve right actions as $(g \cdot s) \cdot h = g \cdot (s \cdot h)$ (which follows from the associative law). The right action commutes with the left action. Moreover, anything commuting with the right action is of the form $s \mapsto g \cdot s$ from some $g \in G$. Suppose $f : S \to S$ commutes with a right action. Then $f(e) = g$ for some g. Then $f(s) = f(es) = f(e) \cdot s = g \cdot s$. So f is "the same" as g. So G is exactly the symmetries of G preserving the right action of G.

Picture G as a graph, where edges between elements are labeled by their right actions. Then the left action of G is the symmetries of the graph.

1.1.1 The 8 actions of a group on itself

Suppose we have left action of G on S $(g, s) \mapsto g \cdot s$. We can get a right action by putting $s \cdot g = g^{-1}s$. Indeed, we have $s(gh) = (gh)^{-1}s = h^{-1}(g^{-1}s) = (sg)h$.

4 left actions of G on G:

1. $g \cdot s = s$, the "trivial" action
2. $g \cdot s = gs$, the standard left action
3. $g \cdot s = sg^{-1}$, a right action "made into" a left action
4. $g \cdot s = gsg^{-1}$, the adjoint action, or conjugation [1]

[1] Some people write conjugation as $g^{-1}sg$.

1.2 Lagrange's theorem and consequences

The way we will approach group theory is to list all groups and to prove theorems when we need to study groups of a particular order (different from the treatment in the Lang textbook).

- Order 1: the "trivial" group
- Order 2, 3 (prime order): There is just one group of any prime order p.

To prove the latter fact, we need Lagrange's theorem.

Theorem 1.1 (Lagrange)**.** *If H is a subgroup of G, and the order (or number of elements) of G, H is finite. Then the order of H divides the order of G.*

Definition 1.8. The left cosets of H in G are sets of the form $gH := \{gh : h \in H\}$. The right cosets of H in G are sets of the form $Hg := \{hg : h \in H\}$.

Proof. Look at coests of H in G. Any two left cosets have H elements. Also, any two left cosets are either the same or disjoint. If $g_1h_1 = g_2h_2$, then for $h \in H$, $g_1h = g_2(h_2h_1^{-1}h)$, which is in g_2H. So $|G| = |H| \times$ number of left cosets. □

A special case: if $g \in G$, look at the subgroup H of all powers of g; i.e. $H = \{g^n : n \in \mathbb{Z}\}$. The order of g is the smallest $n > 0$ such that $g^n = e$ (if n exists). The order of subgroup H is the order of g. If $|G|$ is finite, $g \in G$, then order of g divides order of G. Suppose G has order p (prime). Pick $g \in G$. Then g has order 1 or p; the first case is $g = e$, and the second is for every other element. So $G = H$.

1.2.1 Applications of Lagrange's theorem

Theorem 1.2 (Fermat)**.** *If $g \in \mathbb{Z}$ and p (prime) does not divide g, then $g^{p-1} = 1 \pmod p$.*

Proof. Look at group $(\mathbb{Z}/p\mathbb{Z})^*$. This is a group of order $p - 1$, so every element has order dividing $p - 1$. □

Theorem 1.3 (Euler)**.** *Suppose $g, m \in \mathbb{Z}$ are coprime. Then $g^{\phi(n)} = 1 \pmod m$, where $\phi(m)$ is the number of irreducible elements of $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Same as the proof of Theorem 1.2. □

1.2.2 Geometric meaning of Lagrange's theorem

Suppose G acts on a set S trasitively. If s, t are in S, then $s = gt$ for some g. FIx some $s \in S$. Put $H = \{h \in G : h \cdot s = s \, \forall s \in S\}$, the elements of G fixing S. Then the points of $S \iff$ cosets of H. $t \to$ elements g such that $gs = t$. Left coset as it $gs = t$, then $(gh)s = t$ as $hs = s$.

Interpret $|G| = |H| \times$ number of left cosets in terms of the action. Then we have that $|G| =$ number of elements fixing $s \times$ number of elements of set S. For example, if G is the group of rotations of an icosahedron, then

$$|G| = \text{number of elements fixing center of a face} \times \text{number of faces.}$$

So in this case, $|G| = 3 \times 20 = 60$.

1.3 Groups of order 4 and product groups

- Groups of order 4: 2 Examples.
  - $(\mathbb{Z}/4\mathbb{Z}, +)$ with elements $\{0, 1, 2, 3\}$
  - Symmetries of a rectangle $\{1, a, b, c\}$

To show that these two are not isomorphic, look a the orders of elements. The orders of elements in the former are 1, 4, 2, and 4; the orders of elements in the latter are 1, 2, 2, and 2. Order does not change under isomorphism, so these groups are not isomorphic.

Are these all the groups of order 4? Well, by Lagrange's theorem, all elements have order 1, 2, or 4. If a group has an element g of order 4, then the elements are $1, g, g^2, g^3$ with the product being $g^a g^b = g^{a+b \pmod 4}$. Then this is isomorphic to $(\mathbb{Z}/4\mathbb{Z}, +)$. If all elements have order 2, G is abelian (commutative). $1 = g^2h^2 = ghgh$, so $hg = h^{-1}g^{-1} = gh$, making G abelian. Writing G additively, G is a vector space over the field $\mathbb{F}_2$ with 2 elements. So G is isomorphic to the unique 2-dimensional vector space over $\mathbb{F}_2$. So, indeed, there are just 2 groups of order 4.

Definition 1.9. The *product* of 2 groups G and H is $G \times H$, where the operation is $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1, h_2)$.

The group $\{1, a, b, c\}$ is isomorphic to a product of 2 subgroups. $\{1, a, b, c\} \cong \{1, a\} \times \{1, b\}$, where $1 \mapsto (1, 1)$, $a \mapsto (a, 1)$, $b \mapsto (1, b)$, and $c \mapsto (a, b)$.

Example 1.3. $\mathbb{R}^* \cong \{1, -1\} \times \mathbb{R}^+$.

Example 1.4. The polar decomposition gives us $\mathbb{C}^* = S^1 \times \mathbb{R}^+$.

Example 1.5. If $\mathbb{F}$ is a field, the vector space $\mathbb{F}^n$ is a product of n copies of $\mathbb{F}$, under addition.

Example 1.6. Let G be the group of all roots of 1 in $\mathbb{C}$ (contains square roots, cube roots, fourth roots, etc). Then $G = \left\{z \in \mathbb{C} : z = e^{2\pi i(m/n)}, m, n \in \mathbb{Z}\right\}$. Define the subgroups $H_1 = \left\{z \in G : \exists n \in \mathbb{Z} \text{ s.t. } z^{2n} = 1\right\}$ and $H_2 = \left\{z \in G : \exists n \in \mathbb{Z} \text{ s.t. } z^{2n+1} = 1\right\}$. Then $G \cong H_1 \times H_2$. In fact, we can separate in this way by any prime, not just by 2.