Math 250A Lecture 2 Notes

Daniel Raban

August 29, 2017

1 Groups of orders 6 and 8

1.1 Two groups of order 6

- Groups of order 6
  - the cyclic group $\mathbb{Z}/6\mathbb{Z}$
  - the symmetric group S_3

The former is actually a product[1], $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It has nontrivial proper subgroups $A = \{0, 3\}$ and $B = \{0, 2, 4\}$. $G = AB$, $A \cap B = \{0\}$, and A, B commute, so $G \cong A \times B$.

Definition 1.1. The *symmetric group* is $S_n = \{\text{permutations of } n \text{ points } 1, 2, \ldots, n\}$

Notation for permutations: $(a\ b\ c\ d)$ is the function taking $a \mapsto b \mapsto c \mapsto d \mapsto a$. The 6 elements are $\{e, (1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)\}$. The proper subgroups are $\{e, (1\,2\,3), (1\,3\,2)\}, \{e, (1\,2)\}, \{e, (2\,3)\}, \{e, (1\,3)\}$, and $\{e\}$.

1.2 Quotient groups

Fundamental problem: Suppose H is a subgroup of G. We have a set of left cosets aH, the set of such denoted by G/H. Is G/H a group? The most natural attempt is to define the operation as $(aH)(bH) = (ab)H$. The operation we have defined implies that cosets are equivalence classes for the relation $a \equiv b$ iff $aH = bH$ (meaning $a^{-1}b \in H$). Is this well-defined?

Suppose $b_1 \equiv b_2$, so $b_1 = b_2 h$ for some $h \in H$. Then $ab_1 = ab_2h$, so $ab_1 \equiv ab_2$. Suppose $a_1 \equiv a_2$. We want $a_1 b \equiv a_2 b$. We have $a_2hb = a_2b$, so we would be done if the group is commutative. In fact, the condition we need here is $hb = bh'$ for some $h' \in H$; so this operation is well defined if $b^{-1}Hb = H$.

[1] Cayley once made the mistake of thinking these two were different groups, claiming that there were 3 groups of order 6.

Definition 1.2. A subgroup H is *normal* in G if $gH = Hg$ for all $g \in G$.

Example 1.1. Let $G = S_3$ and $H = \{e, (1\,2\,3), (1\,3\,2)\}$. Then H is normal.

Remark 1.1. In fact, any subgroup of index 2 is always normal. H is normal $\iff$ left cosets are the same as right cosets. If H has index 2, left cosets are H and $G \setminus H$; these are also right cosets, so H is normal. So G/H is a group of order 2.

Example 1.2. Let $G = S_3$ and $H = \{e, (1\,2)\}$. H is not normal because $(23)H(23)^{-1} \neq H$; we have $(2\,3)(1\,2)(2\,3)^{-1} = (1\,3)$, which is not in H. In this case, the right cosets are not equal to the left cosets.

1.3 Other groups of order 6

We want to classify the groups of order 6. The first step is to pick an element of order 3. Why does this exist?

Theorem 1.1. *Suppose p is prime and p divides $|G|$. The G has an element of order p.*

Proof. Use induction on the order of the group. Assume this is true for all smaller groups.

First case: G is abelian. Pick some element g of some prime order q; this exists because any element has order dividing G and if g has order mn, g^m has order n. If $q = p$, we are done. If $q \neq p$, then look at group $G/\langle g\rangle$; this has order less than G, so our inductive hypothesis gives us that $G/\langle g\rangle$ has ana elements h or order p. Now lift h to some $a \in G$. $a^p \in \langle g\rangle$, so a has order p or pq. So a or a^q has order p.

Second case: G is not abelian. Look at the adjoint action of G on itself; i.e. $g \cdot s = gsg^{-1}$. Decompose G into orbits under this action. The meaning of a, b being in the same orbit is that $a = gbg^{-1}$ for some $g \in G$. The orbits partition G into equivalence classes. So $|G| = \sum |\text{Orbit}|$. Lagrange's theorem says that $|\text{Orbit}| = |G| / |H|$, where H is the stabilizer of one point of the orbit. So $|G| = \sum_{\text{orbits}} |G| / |H|$. We now have 2 cases:

Case 1: Some H with $|H| < |G|$ has order divisible by p. Then by induction, H has an element of order p, so G does, as well.

Case 2: If $|H| < |G|$ and $|H|$ is not divisible by p, then $|G| / |H|$ is divisible by p. So

$$\underbrace{|G|}_{\text{divisible by } p} = \underbrace{\sum_{\substack{\text{orbits} \\ H \subsetneq G}} \frac{|G|}{|H|}}_{\text{divisible by } p} + \sum_{\substack{\text{orbits} \\ H = G}} \frac{|G|}{|H|} = \underbrace{\sum_{\substack{\text{orbits} \\ H \subsetneq G}} \frac{|G|}{|H|}}_{\text{divisible by } p} + \sum_{\substack{\text{orbits} \\ H = G}} 1.$$

Elements that commute with everything in G, the set of which is called the center of G, is abelian and has order divisible by p because the term on the right is precisely the order of the center of G. By the previous cases, the center of G has an element of order p, so we are done. $\square$

Remark 1.2. This does not need to hold if p is not prime. $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has no element of order 4, but 4 divides $|G|$.

Suppose G has order 6. Pick element g of order 3. Then $\{e, g, g^3\}$ is a subgroup of order 3. It is normal since it has index 2. Pick an element h of order 2. This gives a subgroup $\{e, h\}$, which is not necessarily normal. Then G is a semidirect product of these subgroups of orders 2 and 3.

Definition 1.3. A *direct product* of groups A and B is $A \times B$ where the operation is $(a_1, b_1)(a_2, b_2) := (a_1 a_2, b_1 b_2)$.

Here, A and B are both normal and commute. In the following definition, A and B will not necessarily commute.

Definition 1.4. Suppose A is normal and B may not be normal. For each element $b \in B$, $a \mapsto bab^{-1}$ is an automorphism of A. Suppose we have a automorphism φ_b of A for each element of B where $\varphi_{b_1 b_2} = \varphi_{b_1}\varphi_{b_2}$ (this means we have a homomorphism from B into $\mathrm{Aut}(A)$). Then a *semidirect product* of groups A and B is $A \rtimes B$ where the operation is $(a_1, b_1)(a_2, b_2) := (a_1 \varphi_{b_2}(a_2), b_1 b_2)$.

So if we have a action of the group B on A, we can define the semidirect product $A \rtimes B$.

Example 1.3. Let $A = \mathbb{Z}/3\mathbb{Z}$, and let $B = \mathbb{Z}/2\mathbb{Z}$. The automorphisms of A are the identity and $a \mapsto -a$. There are 2 ways for B to act on A, the trivial action $\varphi_b(a) = a$, and the nontrivial action $\varphi_b(a) = -a$ if $b \neq e$. These produce the two groups of order 6: $\mathbb{Z}/6\mathbb{Z}$ and S_3, respectively.

There are no other groups of order 6.

1.4 Groups of order 8

Case 1: All elements have order 2. This implies the group is abelian (same argument as last lecture), so it is really a vector space over $\mathbb{F}_2$. So it is $G \cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$.

Case 2: Some element g has order 4. Then $H = \{1, g, g^2, g^3\}$ is a subgroup of index 2, so it is normal. We write what is called an exact sequence:

$$1 \to \underbrace{\mathbb{Z}/4\mathbb{Z}}_{\cong H} \overbrace{\to}^{\text{injective}} G \overbrace{\to}^{\text{surjective}} \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\cong G/H} \to 1.$$

Definition 1.5. An *exact sequence* is a sequence of groups $A \xrightarrow{f} B \xrightarrow{g} C$, where $\mathrm{im}(f) = \ker(g)$. A short exact sequence is an exact sequence of the form $1 \to A \to B \to C \to 1$.

Remark 1.3. A standard blunder is to assume that if we have an exact sequence $1 \to H \to G \to H/G \to 1$, then G is a direct or semidirect product of H and G/H. A counterexample is $G = \mathbb{Z}/4\mathbb{Z}$ and $H = \mathbb{Z}/2Z$.

Remark 1.4. Given $A, B \subseteq G$ with $1 \to A \to G \to B \to 1$ exact, a common problem is to find G. G is called the extension of B by A[2]. This is hard even when A and B are abelian.

Pick some $h \in H$ mapping to a nontrivial element of $\mathbb{Z}/2\mathbb{Z}$. So G contains g, h, $g^4 = e$, $h^2 = e, g$, or g^2, and $\{1, g, g^2, g^3\}$, so $hgh^{-1} = g$ or g^3.

So we get 6 cases. Note that $hgh^{-1} = g$ iff G is abelian. We cannot have $hgh^{-1} = g^3$ and $h^2 = g$, because then g and h commute, so the group is abelian and not abelian. If $h^2 = g$ and $hgh^{-1} = g$, then $G = \mathbb{Z}/8\mathbb{Z}$. Otherwise, if $hgh^{-1} = g$, then $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $hgh^{-1} = g^3$ and $h^2 = e$, we get the dihedral group of order 8. If $h^2 = g^2$ and $hgh^{-1} = g^3$, we have the quaternion group. This covers all the cases.

Remark 1.5. The quaternions[3] $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ form a 4 dimensional division algebra containing $\mathbb{C} = \{a + bi, \in \mathbb{R}\}$.

We then have

- Groups of order 8
  - the cyclic group $\mathbb{Z}/8\mathbb{Z}$
  - the product group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $(\cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2)$
  - the product group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
  - the dihedral group D_8
  - the quaternion group Q_8

[2] This is also sometimes called the extension of A by B.

[3] The word quaternion actually means soldier. Quaternions (not the mathematical kind) are referenced in the New Testament of Christianity.