Math 250A Lecture 4 Notes

Daniel Raban

September 5, 2017

1 Groups of Order 12,. . . ,24

1.1 Groups of order 12

Last time we introduced A_4, the symmetries of a tetrahedron, and the binary dihedral group as nonabelian groups of order 12. Recall, that if we have some homomorphism $S^3 \to \mathrm{SO}_3(\mathbb{R})$, then the inverse image has order $2 \times |G|$. If $G = S_3$, then we get A_4.

Look at the rotations of a tetrahedron; what are the conjugacy classes? We have

1. identity
2. rotation by $2\pi/3$ (4 of these)
3. rotation by $4\pi/3$ (4 of these)
4. pick opposite edges and reflect across them (3 of these).

1.1.1 Sylow theorems

Recall that if H is a subgroup of G, the $|H|$ divides $|G|$. Suppose m divides $|G|$. Does G have a subgroup of order m? In general, the answer is no. 6 divides the order of A_4, but there is no subgroup of order 6; this is the smallest counterexample. However, the Sylow theorems provide cases in which this must be true.

Theorem 1.1 (Sylow)**.** *Suppose p is prime, p^n divides $|G|$, and p^{n+1} does not divide $|G|$. Then*

1. *G has a subgroup of order p^n (called a Sylow p-subgroup or p-Sylow subgroup).*
2. *All such subgroups are conjugate.*
3. *There are $1 \pmod p$ such subgroups (and this number divides $|G|$).*
4. *Any subgroup of order p^m with $m \leq n$ is contained in some subgroup of order p^n.*

Proof. To prove part (1), we have 2 cases and proceed by induction on $|G|$. The first case is when some proper subgroup H has index prime to p. Then p^n divides H, so H has a subgroup of order p^n by induction. The second case is when all proper subgroups have index divisible by p. Look at the adjoint action of G on itself. Then any orbit of G has 1 element (stabilizer $= G$) or a multiple of p elements (stabilizer of points $\neq G$). Then, as we showed before, the order of the center is divisible by p. Pick $g \in Z$ of order p. Then $G/\langle g \rangle$ has a subgroup of order p^{n-1} by induction. The inverse image of this subgroup has order p^n.

See Lang for parts (2),(3), and (4), or do them as an exercise. □

Applying this theorem to subgroups of order 3 of groups of order 12, the number of such subgroups is 1 (mod 3) and divides 12. Then the number of is 1 or 4. If it is 1, then the subgroup is normal. Also by the Sylow theorem, G has a subgroup of order $2^2 = 4$. In this case, G is a semidirect product of a normal subgroup of order 3 and a subgroup of order 4. Look at the action of a group of order 4 on it. If $\mathbb{Z}/4\mathbb{Z}$ acts trivially, we get $\mathbb{Z}/12\mathbb{Z}$. If it acts nontrivially, we get the binary dihedral group. If we have $\mathbb{Z}/2\mathbb{Z}$, and it acts trivially, we get $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$; the nontrivial action gives us D_{12}.

If we have 4 subgroups of order 3, label them A_1, A_2, A_3, A_4, where $A_i \cap A_j = \{e\}$ if $i \neq j$. So we get $8 = 4 \times 2$ elements of order 3. This leaves 4 elements not of order 3. We know there is a subgroup of order 4 (by Sylow), so we get 3 elements of order 4, and this subgroup is normal. So G is the semidirect product of the subgroup of order 4 by subgroups $\mathbb{Z}/3\mathbb{Z}$. $\mathbb{Z}/3\mathbb{Z}$ acts nontrivially on the subgroup of order 4. The only possibility is $\mathbb{Z}/3\mathbb{Z}$ acting on $(\mathbb{Z}/3\mathbb{Z})^2$, so there is only 1 possible group. This group is A_4, since it has 4 subgroups of order 3 (fix one of the 4 vertices).

1.2 Solvability

So far we have shown that groups of order ≤ 12 can be split up into products with cyclic groups.

Definition 1.1. A finite group is called *solvable* if either

1. it is cyclic
2. it has a normal subgroup N with N and G/N solvable.

Definition 1.2. G is callled *simple* if has no normal subgroup other than $\{e\}$ and itself.

Example 1.1. The rotations of an icosahedron is a non-cyclic simple group. Look at the conjugacy classes:

1. identity (order 1)
2. rotation by $2\pi/3$ (order 3, 20 of them, each corresponding to a face)

3. rotation by $2\pi/5$ (order 5, 12 of them, each corresponding to a vertex)

4. rotation by $4\pi/5$ (order 5, 12 of them, each corresponding to a vertex)

5. rotation by π (order 2, 15 of them, (number of edges)/2).

Any normal subgroup must be a union of conjugacy classes. Suppose n is the order of a normal subgroup. Then $n = 1+$ some of $\{12, 12, 15, 20\}$, and $n = 1, 2, 3, 5, 6, 10, 12, 15, 20, 30, 60$. Then the only solutions are $n = 1$ or $n = 60$, which shows that this group is simple.

Every finite group can be split up into simple groups.

Theorem 1.2 (Jordan-Holder)**.** *The set of simple groups we get does not depend on the choice of splitting.*

Proof. See Lang.[1] □

Finite simple groups have been classified as 18 types in infinite series and 26 others (sporadic).

Example 1.2. $\mathrm{GL}_n(\mathbb{F}_p)$ gives rise to $\mathrm{SL}_n(\mathbb{F}_p)$ by quotienting out by the kernel of the determinant map, and $\mathrm{SL}_n(\mathbb{F}_p)$ gives rise to $\mathrm{PSL}_n(\mathbb{F}_p)$ by quotienting out by the center.

1.3 Groups of order 13, 14, and 15

13 is prime, and 14 is of order $2p$, so our previous results give us:

- Groups of order 13
  - $\mathbb{Z}/13\mathbb{Z}$
- Groups of order 14
  - $\mathbb{Z}/14\mathbb{Z}$
  - the dihedral group D_{14}

For groups of order 15, we prove general results for groups of order p, q for primes $p < q$.

The Sylow theorems give us that G has a subgroup of order q. The number of conjugates is 1 (mod q) and divides pq. So the only possibility is 1. So G has a normal subgroup $\mathbb{Z}/q\mathbb{Z}$. SO G is a semidirect product of $\mathbb{Z}/q\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$. How can $\mathbb{Z}/p\mathbb{Z}$ act on $\mathbb{Z}/q\mathbb{Z}$? $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/q\mathbb{Z})^*$, which has order $q - 1$. This is cyclic (will prove later when we cover fields), so it has 1 subgroup of order p if p divides $q - 1$. So either p does not divide $q - 1$ or p divides $q - 1$. In the first case, the only subgroup of order pq is cyclic, so we get 1 group of order 15. In the second case, there are 2 groups: the first is the cyclic group (comes from the trivial action), and the second is $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. We summarize this as

[1] Professor Borcherds couldn't really make sense of the proof in Lang, and he has never actually used the Jordan-Holder theorem, which is why proof here has been omitted.

- Groups of order pq ($p < q$)
  - If p divides $q - 1$
    - $\mathbb{Z}/pq\mathbb{Z}$
  - If p does not divide $q - 1$
    - $\mathbb{Z}/pq\mathbb{Z}$
    - $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Example 1.3. Let $p = 2$. 2 divides $q - 1$, so we get the cyclic and dihedral groups.

Example 1.4. Let $p = 3$ and $q = 7$. 3 divides $7 - 1$, so we get a nonabelian group. This is the smallest non-abelian group of odd order.

1.4 Groups of order 16

Groups of order 16 are a mess (same is true for p^n, where $n \geq 4$). We just list them and not prove anything.

- Groups of order 16
  - Abelian
    - $\mathbb{Z}/16\mathbb{Z}$
    - $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
    - $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
    - $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$
    - $(\mathbb{Z}/2\mathbb{Z})^4$
  - Nonabelian, with an element of order 8
    - Generalized quaternion: $g^8 = 1$, $aga^{-1} = g^{-1}$, $a^2 = g^4$
    - Dihedral: $g^8 = 1$, $aga^{-1} = g^{-1}$, $a^2 = 1$
    - Semidihedral: $g^8 = 1$, $aga^{-1} = g^3$, $a^2 = 1$
    - (Nameless): $g^8 = 1$, $aga^{-1} = g^5$, $a^2 = 1$
  - Products
    - $Q_8 \times \mathbb{Z}/2\mathbb{Z}$
    - $D_8 \times \mathbb{Z}/2\mathbb{Z}$
  - Semidirect products
    - $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
    - $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/4\mathbb{Z}$
  - Miscellaneous
    - Pauli matrices, generated by the matrices

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm i & 0 \\ 0 & \pm i \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}.$$

1.5 Finitely generated abelian groups

So far, the finitely generated abelian groups we know about are finite products of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$. These are actually all the examples.

Theorem 1.3. *Let G be a finitely generated abelian group. Then G is a finite product of groups of the form $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$.*

Proof. Suppose G is abelian (written additively), generated by $g_1, \ldots, g_n$. We have the relations $m_{1,1}g_1 + m_{1,2}g_2 + \cdots + m_{1,n}g_n = 0$, etc, which give us a (possibly infinite) matrix of the coefficients. We can simplify the matrix by adding k times any column to any other; this is a change of generators $g_i \mapsto g_i + kg_j$. We can add k times any row to any other row; if rows $R = S = 0$, this is equivalent to $R = 0$ and $kR + S = 0$. We can apply these operations to make $m_{1,1}$ as small as possible. Subtract multiples of column 1 from other columns to make row 1 have only 1 nonzero entry ($m_{1,1}$). This is possible because $m_{1,1}$ divides $m_{1,2}$; otherwise $m_{1,2} = km_{1,1} + r$ for $|r| < m_1$, and we could subtract $km_{1,1}$ from $m_{1,2}$ and then subtract $r = m_{1,2}$ from $m_{1,1}$ to make $m_{1,1}$ smaller. We can kill off the first column in the same way, leaving $m_{1,1}$ as the only nonzero entry in the first column. Repeat this whole process with $m_{2,2}$ and so on to get a matrix where only $m_{i,i}$ is nonzero for $1 \leq i \leq n$. So our group is now generated by $g_1, \ldots, g_n$ with the relations $m_{1,1}g_1 = 0$, $m_{2,2}g_2 = 0, \ldots$. So $G \cong \mathbb{Z}/m_{1,1}\mathbb{Z} \times \mathbb{Z}/m_{2,2}\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{n,n}\mathbb{Z}$, where if $m_{i,i} = 0$, we just have $\mathbb{Z}$ in the product. □

Remark 1.1. This decomposition is unique if we insist that $m_{i,i}$ divides $m_{j,j}$ for $i < j$ or if we insist that all $m_{i,i}$ are prime powers or 0, and order does not matter.

1.6 Groups of order 17,. . . ,24

17 is prime, so we have

- Groups of order 17
  - $\mathbb{Z}/17\mathbb{Z}$

Groups of order 18 have a normal subgroup of order 3^2. We can then classify the groups by semidirect products to get 5 groups.

- Groups of order 18
  - 5 semidirect product groups
- Groups of order 19
  - $\mathbb{Z}/19\mathbb{Z}$

Groups of order 20 have a normal subgroup of order 5. We can then classify the groups by semidirect products to get 5 groups, as in the case of order 18.

- Groups of order 20
  - 5 semidirect product groups

$21 = pq$ for $p = 3$ and $7 = q$ (and 3 divides $7 - 1$), so we have

- Groups of order 21
  - $\mathbb{Z}/pq\mathbb{Z}$

$22 = 2p$, so we have

- Groups of order 22
  - $\mathbb{Z}/22\mathbb{Z}$

23 is prime, so we have

- Groups of order 23
  - $\mathbb{Z}/23\mathbb{Z}$
- Groups of order 24
  - the symmetric group S_4
  - Binary dihedral group (inverse image of A_4 under $S^3 \to \mathrm{SO}_3$)
  - a dozen or so others...