Math 350, Spring 2025 Professor Rob Benedetto

Optional Handout: Other Group Theory Topics, from Sections 13–15

There are some wonderful topics in Sections 13–15 of Saracino's book that we sadly do not have time for. But here is a brief summary.

The Isomorphism Theorems

The following theorems all appear in Section 13. The first, also known as the Fundamental Theorem on Group Homomorphisms, was covered in detail in class, and you **are** responsible for it (for the final, not the midterms); I'm only including it here for completeness. All four concern homomorphisms and quotient groups.

First Isomorphism Theorem. (Saracino Theorem 13.2)
Let G and H be groups, let $\phi : G \to H$ be an **onto** homomorphism, and let $K = \ker \phi$. Then $G/K \cong H$.

Correspondence Theorem. (Saracino Theorem 13.3)
Let G and H be groups, let $\phi : G \to H$ be an **onto** homomorphism, and let $K = \ker \phi$. Then there is a one-to-one and onto function

$$\big\{\text{subgroups of } G \text{ containing } K\big\} \to \big\{\text{subgroups of } H\big\}$$

given by $G' \mapsto \phi(G')$. Moreover, for each subgroup G' of G containing K, we have $G' \lhd G$ iff $\phi(G') \lhd H$.

Second Isomorphism Theorem. (Saracino Theorem 13.4)
Let G be a group, let $H, K \subseteq G$ be subgroups, and suppose $K \lhd G$. Then $H/(H \cap K) \cong HK/K$

(Here, $HK = \{hk : h \in H \text{ and } k \in K\}$. From various old problem sets, we know, using the fact that $K \lhd G$, that HK is a subgroup of G containing K as a normal subgroup, and that $H \cap K$ is a normal subgroup of H; that is, the statement of the Theorem makes sense.)

Third Isomorphism Theorem. (Saracino Theorem 13.5)
Let G be a group, let $H \lhd K \lhd G$, and suppose in addition that $H \lhd G$. Then $K/H \lhd G/H$, and $(G/H)\big/(K/H) \cong G/K$.

The proof of each of the above theorems requires writing down an appropriate function (between two groups in the case of the three Isomorphism Theorems, or between two sets in the case of the Correspondence Theorem) and then proving that it has whatever properties are relevant. We did the first one in class; see Saracino for the others. For the Correspondence Theorem, the map between the two sets is already given in the statement of the theorem; the rest of the proof is simply to verify that this function between sets is one-to-one and onto, and that the second clause (about normal subgroups) holds. Meanwhile, the proofs of the Second and Third Isomorphism Theorems use the result of the First, by merely constructing an **onto** homomorphism with the appropriate kernel. For example, the map for the Third Isomorphism Theorem goes from G/H to G/K by mapping $Hg \mapsto Kg$. One then proves that this map is a well-defined, onto homomorphism with kernel exactly K/H.

Finitely Generated Abelian Groups

If you think about it, every finite abelian group we have run into has been (isomorphic to) a direct product of finitely many cyclic groups. (For example, the Klein 4-group turned out to be $V_4 \cong C_2 \times C_2$.) Well, that's always true:

Structure Theorem for Finite Abelian Groups (Saracino Theorem 14.2.)
Let G be a finite abelian group, and factor $n = |G|$ as $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, where $k \geq 0$, the numbers $p_1, \ldots, p_k$ are *distinct* primes, and $s_1, \ldots, s_k \geq 1$.
Then there are abelian groups $G_1, \ldots, G_k$ with $|G_i| = p_i^{s_i}$ and $G \cong G_1 \times G_2 \times \cdots \times G_k$, and each G_i is itself of the form

$$G_i \cong C_{q_{i,1}} \times C_{q_{i,2}} \times \cdots \times C_{q_{i,m_i}}$$

where each integer $q_{i,j}$ is of the form $q_{i,j} = p_i^{t_{i,j}}$, with $t_{i,j} \geq 1$, and $s_i = t_{i,1} + \cdots + t_{i,m_i}$.
Furthermore, this factorization is unique up to permuting the order in which the various C_q's are listed.
In other words, **every finite abelian group is isomorphic to a unique direct product of cyclic groups of prime-power order**.

For example, the abelian group C_6 is isomorphic to $C_2 \times C_3$. (See Theorem 6.1(ii).)

As another example, the Theorem says that any abelian group of order 24 is isomorphic to *exactly one* of

$$C_8 \times C_3, \quad C_2 \times C_4 \times C_3, \quad \text{or} \quad C_2 \times C_2 \times C_2 \times C_3.$$

The proof of the theorem is fairly long, and it takes up most of pages 138–141. (Plus the statement and proof of Theorem 14.1 on pages 133–134; that's an interesting result in its own right, and you should take a look.) But even though the proof is long, it is really just the repeated use of tools we have already learned: quotient groups, orders of elements, and so on.

More generally, recall that a (not necessarily finite) group G is **finitely generated** if there is a finite set $S \subseteq G$ that generates G. (Remember, this means that every element of G can be written as a product of the form $x_1^{e_1} \cdots x_m^{e_m}$, where each x_i is an element of S, and $e_i \in \mathbb{Z}$ are integers; the x_i's **are** allowed to be repeats of each other.) The following theorem is an extension of the one above to finitely generated abelian groups:

Structure Theorem for Finitely Generated Abelian Groups
Let G be a finitely generated abelian group. Then there is an integer $r \geq 0$ and a finite abelian subgroup $G_0 \subseteq G$ such that

$$G \cong \mathbb{Z}^r \times G_0,$$

where $\mathbb{Z}^r$ denotes $\mathbb{Z} \times \cdots \times \mathbb{Z}$. In fact, the subgroup G_0 is precisely the **torsion subgroup**

$$G_0 = \{g \in G : \exists n \geq 1 \text{ such that } g^n = e\}.$$

Moreover, r and G_0 are unique, in the sense that if $G \cong \mathbb{Z}^s \times H$ for some integer $s \geq 0$ and finite abelian group H, then $r = s$ and $H \cong G_0$.

The integer r is called the *rank* of the abelian group G. Note that a finitely generated abelian group G has rank zero if and only if G itself is finite.

Together, then, the two above structure theorems say that any finitely generated abelian group is a finite product of cyclic groups.

Please note, however, that many infinite abelian groups are *not* finitely generated. For example, neither $(\mathbb{Q}, +)$ nor $(\mathbb{Q}^\times, \cdot)$ is finitely generated. (Can you prove that?)

The Sylow Theorems

So what can we say about the structure of finite *non*-abelian groups? Well, far less than we can say about abelian groups, but we can strengthen the result of Cauchy's Theorem (that if p divides the order of G, then G has a subgroup of order p) substantially. The Norwegian mathematician Ludwig Sylow (pronounced "SEE-lō") proved this generalization as a series of three theorems in 1872. To state them, we first need some definitions.

Definition. Let G be a group, and let $H, K \subseteq G$ be subgroups. If there is some element $a \in G$ such that $K = aHa^{-1}$, then we say H and K are *conjugate* (to each other).

A few things to note, most of which we already know:

1. The relation of conjugacy is an equivalence relation on the set of subgroups of G.
2. Two conjugate subgroups are isomorphic to one another. In particular, they each have the same number of elements.
3. A subgroup $H \subseteq G$ is normal in G if and only if its only conjugate is itself.

Definition. Let G be a finite group, p a prime number, and $n \geq 1$ a positive integer. Suppose that p^n divides the order of G but p^{n+1} does not. Then a subgroup $H \subseteq G$ of order p^n is called a *p-Sylow subgroup* of G, or simply a *Sylow subgroup* of G.

For example, if $|G| = 24$, then a 3-Sylow subgroup is any subgroup of order 3, while a 2-Sylow subgroup is any subgroup of order 8. Moreover, G has no p-Sylow subgroups for $p \geq 5$, by Lagrange's Theorem.

The Sylow Theorems Let G be a finite group, let p be a prime number, and let $n \geq 1$. Suppose that $p^n \mid |G|$ but $p^{n+1} \nmid |G|$. Then:

1. G has at least one p-Sylow subgroup. Moreover,
   (a) For any p-Sylow subgroup $H \subseteq G$ and integer k with $1 \leq k \leq n$, H has a subgroup of order p^k.
   (b) For any integer k with $1 \leq k \leq n$ and any subgroup $H' \subseteq G$ with $|H'| = p^k$, there is a p-Sylow subgroup H of G such that $H' \subseteq H \subseteq G$.
2. Any two p-Sylow subgroups are conjugate. That is, for any subgroups $H_1, H_2 \subseteq G$ such that $|H_1| = |H_2| = p^n$, there is some $a \in G$ such that $H_2 = aH_1a^{-1}$.
3. Let m be the number of p-Sylow subgroups of G.

   Then $m \equiv 1 \pmod{p}$, **and** m divides $|G|/p^n$.

   That is, $m \mid |G|$, $p \nmid m$, and there is an integer $j \geq 1$ such that $m = 1 + jp$.

   In fact, if H is a p-Sylow subgroup, then $m = [G : N(H)]$, where $N(H)$ is the normalizer of H in G.

The Sylow Theorems appear in Section 15, specifically as Theorems 15.1–15.3 on page 144. The proofs are quite involved, but they use techniques we are familiar with: counting certain sets by constructing cleverly chosen one-to-one and onto maps between sets, using results like the Class Equation, Lagrange's Theorem, and Cauchy's Theorem. In particular, although statement 1(a) above is a generalization of Cauchy's Theorem, the proof requires the use of Cauchy's Theorem, so we were not wasting our time when we proved Cauchy's Theorem.

Here is an example of the power of the Sylow Theorems.

Corollary. Let p and q be prime numbers with $p < q$ and $p \nmid (q-1)$. Then every group of order pq is abelian, and in fact cyclic.

(So for example, the only group of order $15 = 3 \cdot 5$ is C_{15}, up to isomorphism. However, this doesn't apply to numbers like $10 = 2 \cdot 5$ or more generally $2q$, where q is an odd prime, since $2|(q-1)$. And good thing it doesn't apply in that case, since there *are* nonabelian groups of those orders, namely the dihedral group D_q of order $2q$. It also doesn't apply to groups of order $21 = 3 \cdot 7$, since $3|(7-1)$. And sure enough, there *is* a nonabelian group of order 21; see if you can find it.)

Proof of Corollary. Given a group G of order pq, let $H \subseteq G$ be a p-Sylow subgroup, and let $K \subseteq G$ be a q-Sylow subgroup; they exist by the First Sylow Theorem. So $|H| = p$ and $|K| = q$.

But how many p-Sylow subgroups are there? Well, call this number m. By the Third Sylow Theorem, we have $m|q$ (i.e., $m = 1$ or $m = q$, since q is prime) but also $m \equiv 1 \pmod{p}$; so $m = 1$, since $q \not\equiv 1 \pmod{p}$ by hypothesis. That is, H is the *only* p-Sylow subgroup. Since aHa^{-1} is also a p-Sylow subgroup for any $a \in G$, we must have $aHa^{-1} = H$ for all $a \in G$, and hence $H \lhd G$.

By a similar argument, $K \lhd G$. (This time we use the hypothesis that $q > p$ to show that $p \not\equiv 1 \pmod{q}$, and hence the number of q-Sylow subgroups is not p.)

Consider the subgroup $H \cap K$. By Lagrange's Theorem, the number of elements of this subgroup must divide both p and q, and therefore this number must be 1. That is, $H \cap K = \{e\}$. Using that fact, one can easily show that the set $HK = \{hk : h \in H, k \in K\}$ has exactly pq distinct elements, and therefore $HK = G$. That is, *every* element of G may be written as hk for some $h \in H$ and $k \in K$.

Meanwhile, using the three facts that $H \lhd G$, $K \lhd G$, and $H \cap K = \{e\}$, one can show that $hk = kh$ for all $h \in H$ and $k \in K$; see Exercise 11.7. However, H is abelian (since it is order p and hence cyclic), and so is K. Thus, given $g_1, g_2 \in G$, we may write $g_1 = h_1k_1$ and $g_2 = h_2k_2$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$, and therefore

$$g_1g_2 = h_1k_1h_2k_2 = h_1h_2k_1k_2 = h_2h_1k_2k_1 = h_2k_2h_1k_1 = g_2g_1.$$

That is, G is abelian. It then follows immediate from the Structure Theorem for Finite Abelian Groups that $G \cong C_p \times C_q$, which is cyclic by Theorem 6.1(ii). QED

You can find more applications of the Sylow Theorems in Chapter 15, especially on pages 146–147 and in the exercises of that section.