Math 5111 (Algebra 1)

Lecture #16 of 24 ∼ November 5th, 2020

Abelian Groups, Sylow's Theorems

- Finitely Generated Abelian Groups
- Sylow's Theorems

This material represents §3.4.1-3.4.2 from the course notes.

Abelian Finitely Generated Groups, I

Last time, we proved the following result:

Theorem (Finitely Generated Abelian Groups: Invariant Factors)

If G is a finitely generated abelian group, then there exists a unique nonnegative integer r (the rank of the group G) and a unique list of positive integers $a_1, \dots, a_k$ such that $a_1 | a_2 | \cdots | a_k$ such that $G \cong \mathbb{Z}^r \times (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_k\mathbb{Z})$.

We will now extend this theorem by breaking apart the cyclic factors into prime-power cyclic factors.

The Chinese Remainder Theorem, I

We can also decompose the terms $\mathbb{Z}/n\mathbb{Z}$ into prime powers using the Chinese remainder theorem, as follows:

Proposition (Chinese Remainder Theorem for $\mathbb{Z}$)

If a and b are relatively prime integers, then $\mathbb{Z}/ab\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$. Thus, if n has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$, we have $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})$.

In number theory this result is usually stated as follows: for any relatively prime moduli $m_1, \ldots, m_k$ and any integers $a_1, \ldots, a_k$, there exists a unique solution modulo $m_1 \cdots m_k$ to the system

$$\begin{array}{ccc} x & \equiv & a_1 \bmod m_1 \\ \vdots & \vdots & \vdots \\ x & \equiv & a_k \bmod m_k \end{array}$$

The Chinese Remainder Theorem, II

Proof:

- For the first part, consider the map $\varphi : \mathbb{Z} \to (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ given by $\varphi(n) = (n \bmod a,\ n \bmod b)$.
- This map is easily seen to be a ring homomorphism, and its kernel consists of the elements $n \in \mathbb{Z}$ divisible by both a and b. Since a and b are relatively prime, this means $\ker \varphi = ab\mathbb{Z}$.
- Thus, by the first isomorphism theorem, we obtain an injective ring homomorphism $\tilde{\varphi} : \mathbb{Z}/ab\mathbb{Z} \to (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$.
- But since $\mathbb{Z}/ab\mathbb{Z}$ and $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ both have cardinality ab, the map is also surjective, hence is an isomorphism.
- The second part follows by a trivial induction using the fact that the prime powers $p_i^{a_i}$ in the prime factorization of $n = p_1^{a_1} \cdots p_k^{a_k}$ are relatively prime.

The Chinese Remainder Theorem, III

In fact, the Chinese remainder theorem is quite general and can be formulated in arbitrary commutative rings with 1.

- If we work with general ideals, rather than just principal ideals in a Euclidean domain, the proper condition is not coprimality but rather "comaximality".
- Explicitly, if R is commutative with 1, we say that the ideals I and J are comaximal if $I + J = R$.

Then the statement of the Chinese remainder theorem is as follows:

Theorem (Chinese Remainder Theorem, general)

Let R be a commutative ring with 1 and $I_1, I_2, \ldots, I_n$ be pairwise comaximal ideals of R. Then $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$ and $R/(I_1 I_2 \cdots I_n) \cong (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$ as rings.

Generated Finitely Abelian Groups, II

By decomposing each of the cyclic $\mathbb{Z}/n\mathbb{Z}$ factors from the invariant factor decomposition, we see that any finitely generated abelian group decomposes as a direct product of copies of $\mathbb{Z}$ with $\mathbb{Z}$ modulo prime powers:

Theorem (Finitely Generated Abelian Groups: Elementary Divisors)

If G is a finitely generated abelian group, then there exists a unique nonnegative integer r and a unique list of prime powers $p_i^{a_i}$ such that $G \cong \mathbb{Z}^r \times (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})$.

The terms appearing in the direct product are called the elementary divisors of G.

Finitely Generated Groups Abelian, III

Proof:

- The existence follows immediately from decomposing each of the $\mathbb{Z}/n\mathbb{Z}$ terms from the invariant factor decomposition into prime powers.
- For the uniqueness, observe that for any m, the mth-power map φ_m on G is a group homomorphism from G to G since G is abelian. The kernel of φ_m consists of all elements of order dividing m in G.
- The idea is that knowing $\ker \varphi_m$ for all m uniquely characterizes the finite cyclic factors that can show up in the direct product decomposition of G.
- For example, if p is a prime, then $\ker \varphi_p$ picks out all of the terms in the direct product whose prime is p: specifically, a term $\mathbb{Z}/p^n\mathbb{Z}$ contributes the elements $p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$.

Generated Finitely Groups Abelian, IV

Proof (continued):

- More generally, $\ker \varphi_{p^d}$ picks out all of the elements in the copies of $\mathbb{Z}/p\mathbb{Z}$, ... , $\mathbb{Z}/p^{r_d}\mathbb{Z}$, but for higher powers of p we only get the elements of order dividing p^d in those copies.
- Then the quotient $\ker(\varphi_{p^d})/\ker(\varphi_{p^{d+1}})$ is trivial in all components of the direct product except for the terms $\mathbb{Z}/p^k\mathbb{Z}$ with $k \geq d$, where it yields a copy of $\mathbb{Z}/p\mathbb{Z}$.
- Therefore, by computing the order of each quotient $\ker(\varphi_{p^d})/\ker(\varphi_{p^{d+1}})$, we can determine the number of terms $\mathbb{Z}/p^k\mathbb{Z}$ in the direct product with $k \geq d$ for each d.
- This uniquely determines all of the $\mathbb{Z}/p^i\mathbb{Z}$ components in terms of the group structure of G.
- Furthermore, if p is a prime not appearing in any of the prime-power components, we can see that G/pG is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$, so the rank r is also uniquely determined.

Groups Abelian Generated Finitely, V

The argument we gave establishes the uniqueness of the elementary divisors, and (with appropriate minor modification) also gives the uniqueness of the invariant factors.

- Given the invariant factors, it is easy to find the elementary divisors, since we need only find the prime-power factorizations of the invariant factors and then break the terms apart using the Chinese remainder theorem as described above.
- If we have a decomposition into elementary divisor form, we can reconstruct the invariant factor form recursively: the largest invariant factor is the product of the largest power of each prime, then the next largest invariant factor is the product of the largest remaining power of each prime, and so forth.

Finitely Groups Abelian Generated, VI

Example: Find the elementary divisor form of $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/240\mathbb{Z})$.

Finitely Groups Abelian Generated, VI

Example: Find the elementary divisor form of $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/240\mathbb{Z})$.

- We simply break each term into prime powers.
- Note $6 = 2 \cdot 3$ and $240 = 2^4 \cdot 3 \cdot 5$.
- So $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ and $\mathbb{Z}/240\mathbb{Z} \cong (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$.
- Thus, the elementary divisor form of $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/240\mathbb{Z})$ is $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$, or, if we put the terms marginally more in order, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$.

Groups Generated Finitely Abelian, VII

Example: Find the invariant factor form of $(\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/125\mathbb{Z})$.

Groups Generated Finitely Abelian, VII

Example: Find the invariant factor form of $(\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/125\mathbb{Z})$.

- The prime powers are $2^4, 2^4$, then 3, then $5^3, 5, 5$.
- The largest factors are $2^4 \cdot 3 \cdot 5^3 = 6000$. Then the largest remaining factors are $2^4 \cdot 1 \cdot 5 = 80$, and the largest factors after those are $1 \cdot 1 \cdot 5 = 5$.
- Since we have exhausted all factors, we have found all of the invariant factors, and the invariant factor form is $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/80\mathbb{Z}) \times (\mathbb{Z}/6000\mathbb{Z})$.

Groups Finitely Generated Abelian, VIII

Example: Classify the abelian groups of order 36 up to isomorphism, in both elementary divisor and invariant factor form.

Groups Finitely Generated Abelian, VIII

Example: Classify the abelian groups of order 36 up to isomorphism, in both elementary divisor and invariant factor form.

- We first make a list of possible elementary divisors. Since $36 = 2^2 3^2$ we only need to work with the primes 2 and 3.
- The possible cyclic factors for $p = 2$ are $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, while the possible cyclic factors for $p = 3$ are $\mathbb{Z}/9\mathbb{Z}$ and $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.

Groups Generated Abelian Finitely, IX

Example: Classify the abelian groups of order 36 up to isomorphism, in both elementary divisor and invariant factor form.

- Thus, since all combinations are possible and distinct, we see that there are 4 abelian groups of order 36, and their elementary divisor forms are $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z})$, $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z})$, and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.
- To convert these into invariant factor form, we follow the procedure described above to obtain the invariant factor forms $\mathbb{Z}/36\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/18\mathbb{Z})$, and $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$.

Groups Finitely Generated Abelian, X

Example: Find the number of abelian groups, up to isomorphism, of order 7200.

Groups Finitely Generated Abelian, X

Example: Find the number of abelian groups, up to isomorphism, of order 7200.

- We make a list of possible elementary divisors. Since $7200 = 2^5 \cdot 3 \cdot 5^2$ we must work with 2, 3, and 5.
- The possible powers for $p = 2$ are 5, 4-1, 3-2, 3-1-1, 2-2-1, 2-1-1-1, and 1-1-1-1-1, yielding 7 possible combinations of cyclic factors.
- The only possible term for $p = 3$ is $\mathbb{Z}/3\mathbb{Z}$, yielding 1 possibility.
- For $p = 5$ the terms are either 2 or 1-1, yielding 2 possibilities.
- Thus, there are $7 \cdot 1 \cdot 2 = 14$ abelian groups of order 7200, up to isomorphism.

Abelian Generated Groups Finitely, XI

Our arguments in establishing the classification of finitely generated abelian groups also gives us an algorithm for computing a list of generators.

- When the group is infinite, we do essentially need to compute the various relations that hold between a list of generators.
- However, when the group is finite, we do not need to do this explicitly, if we are able to compute the kernels of the various p^nth-power maps for the primes p dividing the order of the group, since as we saw, these kernels uniquely characterize the group structure.
- One may use these observations, for example, to write down the group structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ for each n.

Sylow's Theorems, I

We continue our analysis of the structure of finite groups.

- Suppose the order of G is n. By Lagrange's theorem, the order of any subgroup of G must divide n.
- From the classification of finite(ly generated) abelian groups, it is not hard to see that if G is abelian, then G has a subgroup of order d for every divisor d of n.

Sylow's Theorems, II

However, if G is non-abelian, then it is not the case that there necessarily exists a subgroup of order d for every d dividing n.

- Indeed, A_4, of order 12, has no subgroup of order 6, though it does have subgroups of orders 1, 2, 3, 4, and 12.
- By Cauchy's theorem, if p is a prime dividing n, then G necessarily contains an element of order p, which will then generate a subgroup of G of order p.
- Note that A_4 does contain subgroups of these required prime orders 2 and 3 (along with the obvious subgroups of orders 1 and 12). But it also contains a subgroup of order 4.
- In fact, this is required: we will now show that if p^d is a prime power dividing the order of G, then in fact G must possess a subgroup of order p^d.

Sylow's Theorems, III

Definition

If p is a prime, a p-group is a group whose order is a power of p.

- $\mathbb{Z}/64\mathbb{Z}$, $D_{2\cdot 4}$, and Q_8 are 2-groups while $\mathbb{Z}/25\mathbb{Z}$ is a 5-group.

Definition

If G is a group and p is a prime, a subgroup of G that is a p-group is called a p-subgroup of G. If p^d is the largest power of p dividing $\#G$, then a p-subgroup of G of order p^d is called a Sylow p-subgroup of G.

- If p^d is the largest power of p dividing $\#G$, then p^d is the largest possible order of a p-subgroup of G, by Lagrange's theorem. A Sylow p-subgroup, therefore, is a p-subgroup of G of the maximum possible size.

Sylow's Theorems, IV

Examples:

1. S_4 contains a subgroup $H = \langle (1\,2\,3\,4), (2\,4) \rangle$ isomorphic to the dihedral group $D_{2 \cdot 4}$ of order 8.
   - Since $\# S_4 = 24 = 2^3 \cdot 3$, this subgroup H is a Sylow 2-subgroup of S_4.
   - S_4 also contains several subgroups of order 3, generated by 3-cycles: $\langle (1\,2\,3) \rangle$, $\langle (1\,2\,4) \rangle$, $\langle (1\,3\,4) \rangle$, $\langle (2\,3\,4) \rangle$. These are Sylow 3-subgroups of S_4.
2. The subgroup $\langle 4 \rangle$ of $\mathbb{Z}/36\mathbb{Z}$, which has order 9, is a Sylow 3-subgroup of $\mathbb{Z}/36\mathbb{Z}$.
   - Indeed, this is the unique Sylow 3-subgroup of $\mathbb{Z}/36\mathbb{Z}$.
   - There is also a unique Sylow 2-subgroup of $\mathbb{Z}/36\mathbb{Z}$: the subgroup $\langle 9 \rangle$, which has order 4.

Sylow's Theorems, V

Examples:

3. Identify all of the Sylow subgroups of A_5.

Sylow's Theorems, V

Examples:

3. Identify all of the Sylow subgroups of A_5.

- Note that A_5 has order $5!/2 = 60 = 2^2 \cdot 3 \cdot 5$. Therefore, the Sylow 2-subgroups have order 4, the Sylow 3-subgroups have order 3, and the Sylow 5-subgroups have order 5.
- The Sylow 3-subgroups are cyclic and generated by 3-cycles. Since there are $5 \cdot 4 \cdot 3/3 = 20$ 3-cycles, and each Sylow 3-subgroup contains 2 different ones, there are 10 Sylow 3-subgroups.
- The Sylow 5-subgroups are cyclic and generated by 5-cycles. Since there are $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1/5 = 24$ 5-cycles, and each Sylow 5-subgroup contains 4 different ones, there are 6 Sylow 5-subgroups.

Sylow's Theorems, VI

Examples:

3. Identify all of the Sylow subgroups of A_5.

- It is a bit harder to identify the Sylow 2-subgroups.

Sylow's Theorems, VI

Examples:

3. Identify all of the Sylow subgroups of A_5.

- It is a bit harder to identify the Sylow 2-subgroups.
- Observe that $\langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$ is a subgroup of order 4 inside A_5, isomorphic to the Klein 4-group, so it is a Sylow 2-subgroup.
- In fact, there are 5 of these subgroups inside A_5, obtained by fixing one point and taking the Klein 4-subgroup of the resulting subgroup isomorphic to A_4.
- They are $\langle (1\,2)(3\,5), (1\,3)(2\,5) \rangle$, $\langle (1\,2)(4\,5), (1\,4)(2\,5) \rangle$, $\langle (1\,3)(4\,5), (1\,4)(3\,5) \rangle$, and $\langle (2\,3)(4\,5), (2\,4)(3\,5) \rangle$.
- In fact, these are all of the Sylow 2-subgroups, because the only elements of A_5 with order dividing 4 are the 2,2-cycles, and it is not hard to see that these are the only 2-groups that can be formed from them.

Sylow's Theorems, VII

It is not obvious that Sylow p-subgroups exist. This fact, and substantially more, is the content of the following results of Sylow:

Theorem (Sylow's Theorems)

Suppose that G is a finite group, p is a prime, and p^d is the largest power of p dividing the order of G. Then the following hold:

1. *G contains a Sylow p-subgroup.*
2. *If P is any Sylow p-subgroup of G and Q is any p-subgroup of G, then Q is contained in some conjugate of P (thus, Q is contained in a Sylow p-subgroup of G). Thus, all Sylow p-subgroups of G are conjugate in G and isomorphic.*
3. *The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod{p}$. Furthermore, $n_p = [G : N_G(P)]$ where P is any Sylow p-subgroup of G, and so as a consequence, n_p divides $\#G/p^d$.*

Sylow's Theorems, VIII

We will prove each of the pieces (1)-(3) separately, and the arguments will be a showcase of our results on group actions.

- I will mention that, although the proofs of Sylow's theorems are not actually that complicated, it is not necessary to know them in order to use the results.
- This is in contrast to various other theorems that we have proven, where the ideas in the proof are also important and will show up repeatedly.
- For example, many of our results about the structure of the field extension $F(\alpha)/F$ when α is algebraic rely upon the fact that $F(\alpha)$ is isomorphic to $F[x]/m(x)$, and understanding this fact is crucial for many other things we do.
- With Sylow's theorems, in contrast (at least for "group theory novices") the results and applications are the most important.

Sylow's Theorems, IX: Class Action

1. G contains a Sylow p-subgroup.

Proof:

- We induct on the order n of G. The base case $n = 1$ is trivial.
- For the inductive step, let p be a prime and suppose any group of order strictly less than n has a Sylow p-subgroup.
- Recall that the class equation in G says that $\#G = \#Z(G) + \sum_{i=1}^{e} [G : C_G(g_i)]$, where the $g_1, \dots, g_e$ are representatives of the non-central conjugacy classes of G and $Z(G)$ is the center of G.
- We break into two cases: either p divides $\#Z(G)$, or it doesn't.

Sylow's Theorems, X: Where's The Action?

1. G contains a Sylow p-subgroup.

Proof (case 1):

- If p divides $\#Z(G)$, then by Cauchy's theorem, $Z(G)$ has an element of order p, which then generates a normal subgroup N of G of order p. (The subgroup is normal because it is contained in $Z(G)$.)
- Then G/N is a group of order n/p, so by the inductive hypothesis it has a Sylow p-subgroup $\overline{P}$, which is necessarily of order p^{d-1}.
- Then by the lattice isomorphism theorem, the subgroup P of G containing N with $P/N = \overline{P}$ (i.e., the preimage of $\overline{P}$ under the projection map from G to G/N) has order $\#\overline{P} \cdot \#N = p^{d-1} \cdot p = p^d$ in G.
- Thus, P is a Sylow p-subgroup of G.

Sylow's Theorems, XI: Action Hero

1. G contains a Sylow p-subgroup.

Proof (case 2):

- Now suppose that p does not divide $\#Z(G)$.
- We have $\#G = \#Z(G) + \sum_{i=1}^{e} [G : C_G(g_i)]$.
- Since p divides $\#G$, at least one of the terms $[G : C_G(g_i)]$ must not be divisible by p.
- Let $H = C_G(g_i)$. Since $[G : H]$ is not divisible by p, the order of H is divisible by p^d, and also because g_i is not in the center of G, H is a proper subgroup of G.
- Thus, by the induction hypothesis, H has a Sylow p-subgroup P of order p^d: then P is also a Sylow p-subgroup of G.

G has a Sylow p-subgroup in both cases, so we win.

Sylow's Theorems, XII: Side Action

For the next part of the proof, we first establish a lemma about actions of p-groups:

Lemma (Fixed-Point Congruence for p-Group Actions)

Let p be a prime and suppose P is a p-group acting on a finite set A. Then $\#A \equiv \#\mathrm{Fix}_P(A)$ mod p, where $\mathrm{Fix}_P(A)$ denotes the number of fixed points of P on A (in other words, the number of $a \in A$ such that $g \cdot a = a$ for all $g \in P$).

I will note that the argument we gave to prove Cauchy's theorem is an application of this lemma to the cyclic permutation action of $\mathbb{Z}/p\mathbb{Z}$ on ordered p-tuples $(g_1, \dots, g_p)$ with $g_1 \cdots g_p = 1$.

Sylow's Theorems, XIII: Action Item

Proof:

- By the orbit-stabilizer theorem, the size of the orbit of any $a \in A$ is equal to $[P : P_a]$, the index of the stabilizer P_a of a, which is a divisor of $\#P$ by Lagrange's theorem.
- Therefore, any orbit either has size 1, or has size divisible by p since P is a p-group.
- Note that $a \in A$ has an orbit of size 1 if and only if its stabilizer P_a is all of P, which is equivalent to saying that a is a fixed point of P.
- Since the orbits partition A, this means that $\#A$ is equal to the total number of fixed points (the orbits of size 1) plus a multiple of p (the other orbits).
- Therefore, $\#A \equiv \#\mathrm{Fix}_P(A)$ mod p as desired.

Sylow's Theorems, XIV: All Action, All The Time

2. If P is any Sylow p-subgroup of G and Q is any p-subgroup of G, then Q is contained in some conjugate of P (thus, Q is contained in a Sylow p-subgroup of G). Thus, all Sylow p-subgroups of G are conjugate in G and isomorphic.

Proof:

- Let P, Q be as above and observe that Q acts on the left cosets of P by left multiplication: explicitly, the action is $g \cdot (hP) = (gh)P$ for any $g \in Q$ and left coset hP of P.
- Therefore, since Q is a p-group, by the lemma above, we see that the number of fixed points of this action is congruent to the number of left cosets $[G : P]$ modulo p.
- But since P is a Sylow p-subgroup of G, the index $[G : P]$ is relatively prime to p, so the number of fixed points is nonzero.

Sylow's Theorems, XIV: Action News

2. If P is any Sylow p-subgroup of G and Q is any p-subgroup of G, then Q is contained in some conjugate of P (thus, Q is contained in a Sylow p-subgroup of G). Thus, all Sylow p-subgroups of G are conjugate in G and isomorphic.

Proof (continued):

- So suppose that hP is a fixed point of the action of Q on left cosets of P by left multiplication.
- This means $g \cdot (hP) = hP$ for all $g \in Q$, which is to say, $ghP = hP$. Equivalently, $gh \in hP$ for all $g \in Q$, which is to say, $Q \subseteq hPh^{-1}$.
- Thus, Q is contained in a conjugate of P as claimed.
- For the second part, if Q is now another Sylow p-subgroup, we see $Q \subseteq hPh^{-1}$ as above, but since Q and hPh^{-1} have the same cardinality, they are equal: thus, P and Q are conjugate.

Sylow's Theorems, XV: Lights, Camera, Action

3. The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod p$. Furthermore, $n_p = [G : N_G(P)]$ where P is any Sylow p-subgroup of G, and so as a consequence, n_p divides $\#G/p^d$.

Proof:

- Let P be a Sylow p-subgroup of G and take A to be the set of all Sylow p-subgroups of G.
- Observe that P acts on A by conjugation: explicitly, the action is $g \cdot Q = gQg^{-1}$ for any $g \in P$ and any Sylow p-subgroup Q of G.
- Therefore, since P is a p-group, by the lemma we see that the number of fixed points of this action is congruent modulo p to the number of Sylow p-subgroups of G. We will show that this action has a single fixed point: namely, P.

Sylow's Theorems, XV: Action Comics

3. The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod{p}$. Furthermore, $n_p = [G : N_G(P)]$ where P is any Sylow p-subgroup of G, and so as a consequence, n_p divides $\#G/p^d$.

Proof (part 1):

- So suppose that Q is a fixed point of the conjugation action: then $gQg^{-1} = Q$ for all $g \in P$, meaning that $P \leq N(Q)$. Since Q is a subgroup, $Q \leq N(Q)$ as well.
- Notice that P and Q are then both Sylow p-subgroups of $N(Q)$, and so (2) applied to $N(Q)$ shows that P and Q are conjugate inside $N(Q)$. However, by definition Q is a normal subgroup of $N(Q)$, since all elements of $N(Q)$ normalize Q, and so the only possibility is to have $P = Q$.
- Thus, P is the only fixed point of the conjugation action on A, and so the number n_p of Sylow p-subgroups is congruent to 1 modulo p as claimed.

Sylow's Theorems, XVI: Action Replay

3. The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod{p}$. Furthermore, $n_p = [G : N_G(P)]$ where P is any Sylow p-subgroup of G, and so as a consequence, n_p divides $\#G/p^d$.

Proof (part 2):

- For the second statement, consider the conjugation action of G on the set of its Sylow p-subgroups.
- The stabilizer of P under this action is the set of $g \in G$ such that $gPg^{-1} = P$, which is the normalizer $N_G(P)$ of P in G.
- Therefore, since all Sylow p-subgroups are conjugate by (2), the size of the orbit of P is n_p, which by the orbit-stabilizer theorem is also equal to $[G : N_G(P)]$.
- This is a divisor of $\#G$ by Lagrange's theorem, and since it is relatively prime to p, it must in fact divide $\#G/p^d$.

Sylow Applications, I

Sylow's theorems are very useful for obtaining additional structural information about groups of a given order.

- The first step is to make a list of all of the possible Sylow numbers (i.e., candidates for the numbers n_p of Sylow p-subgroups for each prime p dividing the order of G).
- We can then try to exploit this information to pin down more of the group structure.

Sylow Applications, II

In particular, if we can show that a particular Sylow number n_p must be equal to 1, then we know the resulting Sylow p-subgroup must be normal.

- This follows from Sylow (3): if P is the Sylow p-subgroup, then $n_p = [G : N_G(P)]$, so $n_P = 1$ if and only if $N_G(P) = G$, which is to say, when P is a normal subgroup of G.
- Even when n_p is not necessarily equal to 1, it is often still useful to consider $N_G(P)$, since it is another subgroup of G whose order we know if we know n_p.

Sylow Applications, III

Example: If $\#G = 45$, find the possible Sylow numbers of G and identify the possible structures of the Sylow subgroups of G.

Sylow Applications, III

Example: If $\#G = 45$, find the possible Sylow numbers of G and identify the possible structures of the Sylow subgroups of G.

- Since $45 = 3^2 \cdot 5$ we see that n_3 is a divisor of 45 that is congruent to 1 modulo 3. The only divisors not containing a factor of 3 are 1 and 5, and only 1 is congruent to 1 modulo 3. Thus, $n_3 = 1$, so there is a unique Sylow 3-subgroup of G, which has order $3^2 = 9$.
- Since groups of order p^2 are abelian, the Sylow 3-subgroup is isomorphic either to $\mathbb{Z}/9\mathbb{Z}$ or to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.
- Likewise, n_5 is a divisor of 45 that is congruent to 1 modulo 5, hence is actually a divisor of 9. But the only divisor of 9 congruent to 1 modulo 5 is 1. Thus, $n_5 = 1$ also. This means that there is a unique Sylow 5-subgroup, which has order 5 and is thus isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

Sylow Applications, IV

Example: If $\#G = 60$, find the possible Sylow numbers of G and identify the possible structures of the Sylow subgroups of G.

Sylow Applications, IV

Example: If $\#G = 60$, find the possible Sylow numbers of G and identify the possible structures of the Sylow subgroups of G.

- Since $60 = 2^2 \cdot 3 \cdot 5$ we see that n_2 is a divisor of 15 that is odd. Thus, we have $n_2 \in \{1, 3, 5, 15\}$, and since a Sylow 2-subgroup has order 4, it is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
- Likewise, n_3 is a divisor of $2^2 \cdot 5 = 20$ that is congruent to 1 modulo 3. This means $n_3 \in \{1, 10\}$ and since a Sylow 3-subgroup has order 3, it is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.
- Finally, n_5 is a divisor of $2^2 \cdot 3 = 10$ that is congruent to 1 modulo 5. This means $n_5 \in \{1, 6\}$ and since a Sylow 5-subgroup has order 5, it is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

Sylow Applications, V

We do not quite have all the tools necessary to classify groups of most orders yet.

- We will discuss some such tools next class (specifically, how to construct new subgroups by taking products of smaller subgroups).
- However, one thing we can do is use Sylow's theorems to establish that there are no simple groups of a particular order.
- This kind of calculation is useful because it allows us to narrow down the list of possible simple groups, which (as we discussed a few classes ago) are the basic building blocks of finite groups using quotients and group extensions.
- The simplest approach is to show that a Sylow number must equal 1.

Sylow Applications, VI

Example: Show that a group of order 40 cannot be simple.

Sylow Applications, VI

Example: Show that a group of order 40 cannot be simple.

- Since $40 = 2^3 \cdot 5$, we want to compute the possible values of n_2 and n_5.
- The number n_2 of Sylow 2-subgroups is odd and a divisor of 5, so $n_2 \in \{1, 5\}$.
- Also, the number n_5 of Sylow 5-subgroups is congruent to 1 mod 5 and is a divisor of $2^3 = 8$. The only such divisor is 1, so $n_5 = 1$.
- But, by our observation earlier, since there is a unique Sylow 5-subgroup, it is normal.
- Then our group G has a nontrivial proper normal subgroup, so it is not simple.

Sylow Applications, VII

Example: Show that a group G of order 1375 cannot be simple.

Sylow Applications, VII

Example: Show that a group G of order 1375 cannot be simple.

- Notice that $1375 = 5^3 \cdot 11$. Then n_5 is a divisor of 11 congruent to 1 modulo 5, so $n_5 \in \{1, 11\}$.
- Also, n_{11} is a divisor of 5^3 congruent to 1 modulo 11. But the only such divisor is 1, meaning $n_{11} = 1$.
- But then because $n_{11} = 1$, by our results above this means that the unique Sylow 11-subgroup is normal, and thus G cannot be simple.

Sylow Applications, VIII

Frequently, the congruence conditions do not immediately force the existence of a normal Sylow subgroup.

- But sometimes we can count elements in these various Sylow subgroups and show that having all of the Sylow numbers be large would force the group to have too many elements.
- The general idea is that a group of order p must have $p - 1$ elements of order p, and they are all generators.
- Therefore, distinct subgroups of order p in G cannot share any of their elements of order p.

Sylow Applications, VIII

Example: Show that a group G of order 105 cannot be simple.

Sylow Applications, VIII

Example: Show that a group G of order 105 cannot be simple.

- Notice that $105 = 3 \cdot 5 \cdot 7$. Thus, $n_3 \equiv 1 \bmod 3$ and divides $5 \cdot 7$, so must be among $\{1, 5, 7, 35\}$. The only possibilities are $n_3 \in \{1, 7\}$.
- Likewise, $n_5 \equiv 1 \bmod 5$ and divides $3 \cdot 7$, so must be among $\{1, 3, 7, 21\}$. The only possibilities are $n_5 \in \{1, 21\}$.
- Finally, $n_7 \equiv 1 \bmod 7$ and divides $3 \cdot 5$, so must be among $\{1, 3, 5, 15\}$. The only possibilities are $n_7 \in \{1, 15\}$.
- If any of n_3, n_5, and n_7 equals 1, then the corresponding Sylow subgroup is normal and then G is not simple.

Sylow Applications, IX

Example: Show that a group G of order 105 cannot be simple.

- A priori, it may seem that we could have $n_3 = 7$, $n_5 = 21$, and $n_7 = 15$. However, this is not actually possible.

Sylow Applications, IX

Example: Show that a group G of order 105 cannot be simple.

- A priori, it may seem that we could have $n_3 = 7$, $n_5 = 21$, and $n_7 = 15$. However, this is not actually possible.
- Each Sylow 3-subgroup is cyclic and thus has $3 - 1 = 2$ elements of order 3.
- Each of these elements of order 3 generates the group, so all $7 \cdot (3 - 1) = 14$ of these elements must be distinct.
- Likewise, there would have to be $21 \cdot (5 - 1) = 84$ elements of order 5, and $15 \cdot (7 - 1) = 90$ elements of order 7.
- Along with the identity, we have now identified $1 + 14 + 84 + 90 = 189$ different elements of G, but G cannot actually have this many elements.
- Therefore, we cannot have $n_3 = 7$, $n_5 = 21$, and $n_7 = 15$, so one of them must equal 1: thus G is not simple.

Sylow Applications, X

Example: Show that a group G of order 132 cannot be simple.

Sylow Applications, X

Example: Show that a group G of order 132 cannot be simple.

- Notice that $132 = 2^2 \cdot 3 \cdot 11$. Then n_2 is odd and divides $3 \cdot 11$, so $n_2 \in \{1, 3, 11, 33\}$. Likewise, $n_3 \equiv 1 \pmod 3$ and divides $2^2 \cdot 11$, so $n_3 \in \{1, 4, 22\}$, and $n_{11} \equiv 1 \pmod{11}$ and divides $2^2 \cdot 3$, so $n_{11} \in \{1, 12\}$.
- If n_3 or n_{11} equals 1, then the corresponding Sylow subgroup is normal.
- Otherwise, we would have $n_{11} = 12$ and $n_3 \geq 4$: in this case we would obtain $12 \cdot (11 - 1) = 120$ elements of order 11 along with an additional $4 \cdot (3 - 1) = 8$ elements of order 3.
- There are only $132 - 120 - 8 = 4$ elements remaining in the group, so since there is a Sylow 2-subgroup and it has order 4, all of the remaining elements must lie in this Sylow 2-subgroup, and there can be only one of them.
- Thus, n_2, n_3, or n_{11} must equal 1, and so G cannot be simple.

Summary

We discussed more about the classification of finitely-generated abelian groups and gave examples.

We stated and proved Sylow's theorems.

We gave some applications of Sylow's theorems.

Next lecture: Products of subgroups.