Math 5111 (Algebra 1)

Lecture #15 of 24 $\sim$ November 2nd, 2020

Polynomial Invariants, Conjugation Actions, Abelian Groups

- Polynomial Invariants and A_n
- Conjugation Actions
- Finitely-Generated Abelian Groups

This material represents §3.3.3-3.4.1 from the course notes.

Polynomial Invariants and A_n, I

Our primary interest in groups, and in group actions in particular, is to use them to study field extensions. An important action that will be relevant to our work is the action of S_n and its subgroups on polynomials.

The idea is that if we have n variables $x_1, x_2, \ldots, x_n$, then S_n acts on the set of variables by permuting their indices. We can then extend this action to the polynomial ring $F[x_1, x_2, \ldots, x_n]$ in n variables with coefficients from F by having permutations act variable-by-variable in each monomial term.

Polynomial Invariants and A_n, II

Example:

8. (S_n on Polynomials): If F is a field and $x_1, x_2, \ldots, x_n$ are independent variables, then S_n acts on the polynomial ring $F[x_1, x_2, \ldots, x_n]$ via "index permutation" of the variables. Explicitly, given a polynomial $p(x_1, x_2, \ldots, x_n)$ and $\sigma \in S_n$, the action of σ is $\sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$.
   - It is easy to see that this definition yields a group action, since $\sigma_1 \cdot (\sigma_2 \cdot p)) = \sigma_1 \cdot p(x_{\sigma_2(1)}, \ldots, x_{\sigma_2(n)}) = p(x_{\sigma_1\sigma_2(1)}, \ldots, x_{\sigma_1\sigma_2(n)}) = (\sigma_1\sigma_2) \cdot p$, and $1 \cdot p = p(x_1, \ldots, x_n) = p$.
   - As an example, with $n = 4$ and $p(x_1, x_2, x_3, x_4) = (x_1 - 2x_2x_4)(4x_3^3 - x_4^2)$ then for $\sigma = (1\,2\,3\,4)$ we have $\sigma \cdot p = (x_2 - 2x_3x_1)(4x_4^3 - x_1^2)$.

Polynomial Invariants and A_n, III

Example: Let $G = S_3$ act by index permutation on $F[x_1, x_2, x_3]$.

1. Calculate $\sigma \cdot (x_1^2 x_2 x_3 + 3x_1 x_2)$ where $\sigma = (1\,3\,2)$.
2. Find the orbit and stabilizer of the polynomials $x_1 x_2$ and $x_1^2 x_2$ under the action of G.

Polynomial Invariants and A_n, III

Example: Let $G = S_3$ act by index permutation on $F[x_1, x_2, x_3]$.

1. Calculate $\sigma \cdot (x_1^2 x_2 x_3 + 3x_1 x_2)$ where $\sigma = (1\,3\,2)$.
2. Find the orbit and stabilizer of the polynomials $x_1 x_2$ and $x_1^2 x_2$ under the action of G.

- We have $\sigma \cdot (x_1^2 x_2 x_3 + 3x_1 x_2) = x_3^2 x_1 x_2 + 3x_3 x_1$.
- The orbit of $x_1 x_2$ is $\{x_1 x_2, x_1 x_3, x_2 x_3\}$.
- The stabilizer of $x_1 x_2$ is $\{1, (1\,2)\}$.
- The orbit of $x_1^2 x_2$ is $\{x_1^2 x_2, x_1 x_2^2, x_1^2 x_3, x_1 x_3^2, x_2^2 x_3, x_2 x_3^2\}$.
- The stabilizer of $x_1^2 x_2$ is $\{1\}$.
- Note in each case that the size of the orbit times the size of the stabilizer is $6 = \#G$, as dictated by the orbit-stabilizer theorem.

Polynomial Invariants and A_n, IV

We will do much more when we study the roots of degree-3 and degree-4 polynomials. For now, we will use this action to study the alternating group A_n:

- For a fixed n, define the polynomial

$$D = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

- For example, when $n = 3$, $D = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.
- Now consider the action of S_n on D via index permutation, so that for $\sigma \in S_n$ we have $\sigma(D) = \prod_{1 \leq i < j \leq n}(x_{\sigma(i)} - x_{\sigma(j)})$.
- For example, with $n = 3$ and $\sigma = (1\,2\,3)$ we have $\sigma(D) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = -D$.

Polynomial Invariants and A_n, V

We have $D = \prod_{1 \leq i < j \leq n}(x_i - x_j)$.

- As with the example on the last slide, it is in fact true that any permutation $\sigma \in S_n$ will map D either to D or to $-D$.
- This follows by noting that each term in the product for D will appear in $\sigma(D)$, except possibly with the variables in the other order, which is true because σ is an injective map on the set of $\binom{n}{2}$ unordered pairs (a, b) with $a \neq b$, and is therefore a bijection on this set.
- Thus, by collecting all the signs, we see that D and $\sigma(D)$ are the same except up to a product of some number of -1 terms.

Polynomial Invariants and A_n, VI

In the language of group actions, the observations on the previous slide amount to noting that the group S_n acts via index permutation on the set $\{+D, -D\}$.

- Our goal now is to prove that A_n is the stabilizer of D.
- Since there is only one orbit of S_n acting on $\{+D, -D\}$ (since there obviously exists a permutation interchanging $+D$ and $-D$), the orbit-stabilizer theorem will then immediately imply that $[S_n : A_n] = 2$, and thus that $\#A_n = n!/2$.

Polynomial Invariants and A_n, VII

Definition

For $\sigma \in S_n$ we define the sign $\operatorname{sgn}(\sigma)$ of σ to be $+1$ if $\sigma(D) = D$ and -1 if $\sigma(D) = -D$. We call a permutation σ even if $\operatorname{sgn}(\sigma) = 1$ and odd if $\operatorname{sgn}(\sigma) = -1$.

Example: In $G = S_4$, find the signs of $\sigma = (1\,2\,4)$ and $\tau = (1\,3)$.

Polynomial Invariants and A_n, VII

Definition

For $\sigma \in S_n$ we define the sign $\operatorname{sgn}(\sigma)$ of σ to be $+1$ if $\sigma(D) = D$ and -1 if $\sigma(D) = -D$. We call a permutation σ even if $\operatorname{sgn}(\sigma) = 1$ and odd if $\operatorname{sgn}(\sigma) = -1$.

Example: In $G = S_4$, find the signs of $\sigma = (1\,2\,4)$ and $\tau = (1\,3)$.

- Here,
  $D = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$.
- Then
  $\sigma \cdot D = (x_2 - x_4)(x_2 - x_3)(x_2 - x_1)(x_4 - x_3)(x_4 - x_1)(x_3 - x_1)$
  $= (-1)^4 D = D$. So $\operatorname{sgn}(\sigma) = 1$.
- Likewise,
  $\tau \cdot D = (x_3 - x_2)(x_3 - x_1)(x_3 - x_4)(x_2 - x_1)(x_2 - x_4)(x_1 - x_4)$
  $= (-1)^3 D = -D$. So $\operatorname{sgn}(\tau) = -1$.

Polynomial Invariants and A_n, VIII

Since S_n acts on the set $A = \{+D, -D\}$, as we just showed, we obtain a group homomorphism from S_n into the permutation group $S_A \cong \{\pm 1\}$. This tells us that the sign map is actually a group homomorphism:

Proposition (Sign Map is a Homomorphism)

The sign map is a group homomorphism $\operatorname{sgn} : S_n \to \{\pm 1\}$. *Equivalently,* $\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)$ *for all* $\sigma, \tau \in S_n$.

Example: In $G = S_4$, verify $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$ for $\sigma = (1\,2\,4)$ and $\tau = (1\,3)$.

Polynomial Invariants and A_n, VIII

Since S_n acts on the set $A = \{+D, -D\}$, as we just showed, we obtain a group homomorphism from S_n into the permutation group $S_A \cong \{\pm 1\}$. This tells us that the sign map is actually a group homomorphism:

Proposition (Sign Map is a Homomorphism)

The sign map is a group homomorphism $\operatorname{sgn} : S_n \to \{\pm 1\}$. *Equivalently,* $\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)$ *for all* $\sigma, \tau \in S_n$.

Example: In $G = S_4$, verify $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$ for $\sigma = (1\,2\,4)$ and $\tau = (1\,3)$.

- We have $\sigma\tau = (1\,2\,4)(1\,3) = (1\,3\,2\,4)$, so $\sigma\tau \cdot D$
  $= (x_3 - x_4)(x_3 - x_2)(x_3 - x_1)(x_4 - x_2)(x_4 - x_1)(x_2 - x_1)$
  $= (-1)^5 D = -D$.
- So $\operatorname{sgn}(\sigma\tau) = -1 = (1)(-1) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$ as claimed.

Polynomial Invariants and A_n, IX

It is possible to give direct proofs that the sign map is a group homomorphism.

- However, these proofs are usually very lengthy and technical.
- One fairly standard approach is to count the number of "inversions", pairs (i, j) with $i < j$ but $\sigma(i) > \sigma(j)$. Each inversion contributes a factor of -1 to the action of σ on D, and so the sign of σ is (-1) to the number of inversions of σ.
- Another approach is to show that the sign map is the same as the determinant of the associated permutation matrix M having a 1 in the entries $(i, \sigma(i))$ for each i and 0s elsewhere.
- Then the fact that the sign map is a group homomorphism follows from the fact that determinants of matrices are multiplicative (which is, of course, another standard fact that is frustratingly difficult to prove from scratch!).

Polynomial Invariants and A_n, X

When I defined A_n last week, I noted that A_n contains all of the even permutations. Using the sign map we can prove that there are no other elements in A_n, and also compute the order of A_n and show that it is a normal subgroup of S_n:

Theorem (Alternating Group)

The alternating group A_n is the kernel of the sign map and is therefore is a normal subgroup of S_n. Explicitly, A_n consists of all even permutations, and has order $n!/2$.

Polynomial Invariants and A_n, XI

We will first prove an easy lemma:

Lemma (Transpositions are Odd)

Every transposition in S_n is an odd permutation.

Proof:

- First, observe that $\operatorname{sgn}((1\,2)) = -1$ since the permutation $(1\,2)$ only flips the sign of the single term $x_1 - x_2$ in D.
- Then for any transposition $(i\,j)$, if we set $\sigma = (1\,i)(2\,j)$ then $\sigma(1\,2)\sigma = (i\,j)$.
- Since the sign map is a homomorphism we have $\operatorname{sgn}((i\,j)) = \operatorname{sgn}(\sigma(1\,2)\sigma) = \operatorname{sgn}(\sigma) \cdot (-1) \cdot \operatorname{sgn}(\sigma) = -1$.
- Thus, all transpositions are odd permutations.

Polynomial Invariants and A_n, XII

Theorem (Alternating Group)

The alternating group A_n is the kernel of the sign map and is therefore is a normal subgroup of S_n. Explicitly, A_n consists of all even permutations, and has order $n!/2$.

Proof:

- Since the sign map is a homomorphism, for transpositions $\sigma_1, \ldots, \sigma_k$ we have $\operatorname{sgn}(\sigma_1 \cdots \sigma_k) = (-1)^k$ by the lemma.
- So, $\ker(\operatorname{sgn})$ consists of the permutations that are a product of an even number of transpositions, which is precisely how we defined A_n. Thus, A_n is the kernel of the sign map and consists of all even permutations.
- Furthermore, since sgn is surjective since $\operatorname{sgn}((1\,2)) = -1$, we see $S_n/A_n \cong \operatorname{im}(\operatorname{sgn})$ has order 2, so $|A_n| = |S_n|/2 = n!/2$.

Polynomial Invariants and A_n, XIII

Our argument also gives an easy way to compute the sign of a general permutation from its cycle decomposition.

- Specifically, since a k-cycle can be written as the product of $k-1$ transpositions, the sign of a k-cycle is the opposite of the parity of k.
- Thus for example, 3-cycles are even while 8-cycles are odd.
- Then we see that a permutation is even whenever it has an even number of even-length cycles, and it is odd when it has an odd number of even-length cycles.
- We also see that even permutations are the product of an even number of transpositions, while odd permutations are those that are the product of an odd number of transpositions (whence the terminology), and that no permutation is both even and odd (since the sign map is well-defined).

Conjugation Actions, I

We now study in more detail the conjugation action of a group G on its set of elements.

- As we noted earlier, if G is any group, then G acts on the set $A = G$ via $g \cdot a = gag^{-1}$ for any $g \in G$ and $a \in A$.
- We may generalize this action by noting that G also acts elementwise on the collection of subsets of G, by defining $g \cdot S = \{gs : s \in S\}$ for an arbitrary subset S of G.

Conjugation Actions, II

First, we study the orbits of the conjugation action on elements:

Definition

If G is a group and $a \in G$, we say that b is conjugate to a if there exists some $g \in G$ with $b = gag^{-1}$. The conjugacy class of a in G is the set of elements of G conjugate to a. Explicitly, the conjugacy class of a is the set $\{gag^{-1} : g \in G\}$, which is the orbit of a under conjugation by G.

- In an abelian group, each element is its own conjugacy class, since the condition is simply $b = gag^{-1} = gg^{-1}a = a$.
- More generally, a single element $\{a\}$ is its own conjugacy class precisely when $a \in Z(G)$, which is to say, when a commutes with every element of G.

Conjugation Actions, III

Examples:

1. In $D_{2\cdot 4}$, the conjugacy classes are $\{1\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, sr^2\}$, and $\{sr, sr^3\}$.
   - We can compute that $srs^{-1} = r^3$ and $rsr^{-1} = sr^2$ and $r(sr)r^{-1} = sr^3$.
   - So, the given collections are indeed conjugate.
   - It is not hard to verify that these sets are distinct conjugacy classes.

Conjugation Actions, IV

Examples:

2. In $GL_2(\mathbb{Q})$, the matrices $A = \begin{bmatrix} -3 & 5 \\ 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 0 & -4 \end{bmatrix}$ are conjugate via $M = \begin{bmatrix} 1 & -5 \\ 1 & 1 \end{bmatrix}$, since $MAM^{-1} = B$.
   - Conjugacy of matrices is often studied in linear algebra (where it also has the same name).
   - In 5112, you'll learn the conjugacy classes in $GL_{n\times n}(F)$ for any field F are uniquely represented by matrices in rational canonical form: block-diagonal matrices whose diagonal blocks are companion matrices (1s directly below the diagonal, coefficients of the characteristic polynomial in the last column, 0s elsewhere) for polynomials p_1, p_2, $\ldots$, p_k where $p_1|p_2|\cdots|p_k$.

Conjugation Actions, V

Examples:

3. In S_3, the conjugacy classes are $\{1\}$, $\{(1\,2), (1\,3), (2\,3)\}$, and $\{(1\,2\,3), (1\,3\,2)\}$.
   - We can compute that $(1\,3) = g(1\,2)g^{-1}$, $(2\,3) = h(1\,2)h^{-1}$, and $(1\,2\,3) = g(1\,3\,2)g^{-1}$ for $g = (2\,3)$ and $h = (1\,3)$.
   - Thus, the given collections are conjugate to one another.
   - It is also not so hard to verify that these sets are distinct conjugacy classes.

Conjugation Actions, VI

We can in fact generalize the last example to compute the conjugacy classes in S_n:

Proposition (Conjugacy Classes in S_n)

If $\tau \in S_n$, then for any cycle $(a_1 \ldots a_n)$, we have $\tau(a_1 \ldots a_n)\tau^{-1} = (\tau(a_1) \ldots \tau(a_n))$.
Thus, to conjugate a permutation σ by a permutation τ, we simply apply τ to all of the elements in the cycles of σ.
In particular, two elements of S_n are conjugate if and only if they have the same cycle type.

Conjugation Actions, VI

Proof:

- The first statement is a direct calculation: for each i, we have $\tau(a_1 \ldots a_n)\tau^{-1}[\tau(a_i)] = \tau(a_1 \ldots a_n)(a_i) = \tau(a_{i+1})$, where we take $a_{n+1} = a_1$.
- Thus, by the cycle decomposition algorithm, there is a single cycle in $\tau(a_1 \ldots a_n)\tau^{-1}$, consisting of $(\tau(a_1) \ldots \tau(a_n))$.
- The second statement follows from the first one by writing σ as a product of disjoint cycles $\sigma = \sigma_1 \cdots \sigma_d$ and observing that $\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_d\tau^{-1})$.

Conjugation Actions, VII

Proof (continued):

- The last statement follows from the second one: any conjugate of σ has the same cycle type as σ by the calculations on the last slide.
- Conversely, if σ' has the same cycle type as σ, if we align cycles of corresponding lengths together from σ and σ', say so that the lists of all the elements in the cycles are $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, then the permutation τ with $\tau(a_i) = b_i$ for each i will conjugate σ to σ'.

Conjugation Actions, VIII

Let's go through some examples:

Example: For $\sigma = (1\,7\,4\,8\,6)$ and $\tau = (1\,5)(2\,4\,3)(6\,7)$ inside S_8, compute $\sigma\tau\sigma^{-1}$ and $\tau\sigma\tau^{-1}$.

Conjugation Actions, VIII

Let's go through some examples:

Example: For $\sigma = (1\,7\,4\,8\,6)$ and $\tau = (1\,5)(2\,4\,3)(6\,7)$ inside S_8, compute $\sigma\tau\sigma^{-1}$ and $\tau\sigma\tau^{-1}$.

- From the procedure given in the proposition, we have $\sigma\tau\sigma^{-1} = (\sigma(1)\,\sigma(5))(\sigma(2)\,\sigma(4)\,\sigma(3))(\sigma(6)\,\sigma(7)) = (7\,5)(2\,8\,3)(1\,4)$.
- We can confirm this explicitly by multiplying out $\sigma\tau\sigma^{-1} = (1\,7\,4\,8\,6)(1\,5)(2\,4\,3)(6\,7)(1\,6\,8\,4\,7) = (1\,4)(2\,8\,3)(5\,7)(6)$.
- Likewise, $\tau\sigma\tau^{-1} = (\tau(1)\,\tau(7)\,\tau(4)\,\tau(8)\,\tau(6)) = (5\,6\,3\,8\,7)$.

Conjugation Actions, IX

Example: Show that $\sigma_1 = (1\,4\,3\,8)(2\,5\,6)$ and $\sigma_2 = (1\,2\,6)(3\,7\,4\,5)$ are conjugate inside S_8, and find an explicit permutation τ with $\sigma_2 = \tau\sigma_1\tau^{-1}$.

Conjugation Actions, IX

Example: Show that $\sigma_1 = (1\,4\,3\,8)(2\,5\,6)$ and $\sigma_2 = (1\,2\,6)(3\,7\,4\,5)$ are conjugate inside S_8, and find an explicit permutation τ with $\sigma_2 = \tau\sigma_1\tau^{-1}$.

- From the procedure given in the proposition, and making sure to include the 1-cycles, we can write the two permutations with cycles in corresponding order, as $\sigma_1 = (1\,4\,3\,8)(2\,5\,6)(7)$ and $\sigma_2 = (3\,7\,4\,5)(1\,2\,6)(8)$.
- Then, for example, the permutation τ with $\tau(1) = 3$, $\tau(4) = 7$, $\tau(3) = 4$, $\tau(8) = 5$, $\tau(2) = 1$, $\tau(5) = 2$, $\tau(6) = 6$, and $\tau(7) = 8$ will have $\sigma_2 = \tau\sigma_1\tau^{-1}$.
- The cycle decomposition of this τ is $(1\,3\,4\,7\,8\,5\,2)$.
- Note that τ is not unique. Indeed, if we wrote $\sigma_2 = (5\,3\,7\,4)(6\,1\,2)(8)$, which is equivalent, we would get instead $\tau = (1\,5)(2\,6)(3\,7\,8\,4)$.

Conjugation Actions, X

Example: There are 5 conjugacy classes in S_4, since there are 5 possible cycle types: the identity, transpositions, 3-cycles, 4-cycles, and the 2,2-cycles.

- Explicitly, the conjugacy classes are

1. $\{1\}$
2. $\{(1\,2), (1\,3), (1\,4), (2,3), (2\,4), (3,4)\}$
3. $\{(1\,2\,3), (1\,2\,4), (1\,3\,2), (1\,3\,4), (1\,4\,2), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}$
4. $\{(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2)\}$
5. $\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

- In general, the number of conjugacy classes in S_n will be the number of integer partitions of n.

Conjugation Actions, XI

We record some useful general properties of the conjugation action:

Proposition (Properties of Conjugation, I)

Let G be a group acting on its set of elements by conjugation.

1. *For any $g \in G$, the conjugation-by-g map $\varphi_g : G \to G$ is a group isomorphism, with inverse $\varphi_g^{-1} = \varphi_{g^{-1}}$.*
   In particular, all elements in a given conjugacy class have the same order.
2. *If S is any subset of G, then the stabilizer of S under the conjugation action of G is the normalizer*
   $N_G(S) = \{g \in G : gSg^{-1} = S\}$.
   The number of conjugates of S in G is $[G : N_G(S)]$, the index of the normalizer.

Conjugation Actions, XII

We record some useful general properties of the conjugation action:

Proposition (Properties of Conjugation, II)

Let G be a group acting on its set of elements by conjugation.

3. *If a is any element of G, the stabilizer of S under the conjugation action of G is the centralizer $C_G(a) = \{g \in G : gag^{-1} = a\}$, the set of elements of G commuting with a.*
   The number of conjugates of a in G is $[G : C_G(a)]$, the index of the centralizer.
4. *(Class Equation) If G is a finite group and $g_1, \ldots, g_d$ are representatives of the non-central conjugacy classes of G, then $\#P = \#Z(G) + \sum_{i=1}^{d} [P : C_P(g_i)]$.*

Conjugation Actions, XIII

Proofs:

1. For any $g \in G$, the conjugation-by-g map $\varphi_g : G \to G$ is a group isomorphism, with inverse $\varphi_g^{-1} = \varphi_{g^{-1}}$. In particular, all elements in a given conjugacy class have the same order.
   - We have $\varphi_g(ab) = g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) = \varphi_g(a)\varphi_g(b)$ so φ_g is a group homomorphism.
   - Furthermore, since $\varphi_{g^{-1}}(\varphi_g(a)) = g^{-1}[gag^{-1}](g^{-1})^{-1} = g^{-1}gag^{-1}g = a$ we see that $\varphi_{g^{-1}} \circ \varphi_g$ is the identity map; similarly $\varphi_{g^{-1}} \circ \varphi_g$ is also the identity, so φ_g is an isomorphism.
   - The second statement follows from the fact that group isomorphisms preserve orders of elements.

Conjugation Actions, XIV

Proofs:

2. If S is any subset of G, then the stabilizer of S under the conjugation action of G is the normalizer $N_G(S) = \{g \in G : gSg^{-1} = S\}$. The number of conjugates of S in G is $[G : N_G(S)]$, the index of the normalizer.

   - By definition, $g \in G$ stabilizes S under conjugation precisely when $gSg^{-1} = S$.
   - The second statement is an immediate consequence of the orbit-stabilizer theorem.

   Some other facts about normalizers (while we're here):

   - $N_G(S)$ is also equal to the normalizer $N_G(\langle S \rangle)$ of the subgroup generated by S.
   - The normalizer of any subgroup H contains H.
   - H is normal in G if and only if $N_G(H) = G$.

Conjugation Actions, XV

Proofs:

3. If a is any element of G, the stabilizer of S under the conjugation action of G is the centralizer $C_G(a) = \{g \in G : gag^{-1} = a\}$, the set of elements of G commuting with a. The number of conjugates of a in G is $[G : C_G(a)]$, the index of the centralizer.
    - This is simply (2) applied to the set $S = \{a\}$.

Conjugation Actions, XVI

Proofs:

4. (Class Equation) If G is a finite group and $g_1, \ldots, g_d$ are representatives of the non-central conjugacy classes of G, then $\#G = \#Z(G) + \sum_{i=1}^{d} [P : C_G(g_i)]$.
   - The distinct conjugacy classes of G partition G, since they are equivalence classes of an equivalence relation.
   - Also, each element of the center $Z(G)$ is its own conjugacy class.
   - The remaining conjugacy classes, by hypothesis, are represented by the elements $g_1, \ldots, g_d$.
   - By (3), the number of elements in the conjugacy class of g_i is equal to $[G : C_G(g_i)]$.
   - Thus, summing the sizes of all conjugacy classes yields $\#Z(G) + \sum_{i=1}^{d} [G : C_G(g_i)]$, which is also $\#G$.

Conjugation Actions, XVII

The class equation contains valuable combinatorial information about the group G. We will use it later in a more substantial way in our proofs of Sylow's theorems. For now, we will use it to deduce some useful and important facts about p-groups:

Proposition (Centers of p-Groups)

If p is a prime and P is a finite p-group (i.e., a finite group whose order is a power of p), then $\#Z(P) > 1$.

In other words, any p-group (e.g., $D_{2\cdot 4}$ or Q_8 or the Heisenberg groups H_p you saw on homework 7) must contain at least one nonidentity element that commutes with every other element of the group.

Conjugation Actions, XVIII

Proof:

- If $g_1, \ldots, g_d$ represent the non-central conjugacy classes of P, the class equation says $\#P = \#Z(P) + \sum_{i=1}^{d} [P : C_P(g_i)]$.
- Since the centralizer $C_P(g_i)$ is a subgroup of P, by Lagrange's theorem its order and index are both powers of p.
- Furthermore, since each g_i is by hypothesis non-central, this means $C_P(g_i)$ is a proper subgroup of P, and so its index is greater than 1.
- Thus, each term in $\sum_{i=1}^{d} [P : C_P(g_i)]$ is a multiple of p.
- Since $\#P$ is also a multiple of p, this means $\#Z(P) = \#P - \sum_{i=1}^{d} [P : C_P(g_i)]$ is also a multiple of p. Hence it cannot be equal to 1, so $\#Z(P) > 1$.

Conjugation Actions, XIX

The fact that p-groups have a nontrivial center is very useful. One consequence is that groups of order p^2 must be abelian:

Corollary (Groups of Order p^2)

If p is a prime, then every group of order p^2 is abelian. Moreover, there are two such groups, up to isomorphism: $\mathbb{Z}/p^2\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Conjugation Actions, XX

Proof:

- Suppose G has order p^2. Then since $Z(G)$ is not trivial, its order is either p or p^2.
- If $\#Z(G) = p^2$ then $G = Z(G)$ and G is abelian.
- If $\#Z(G) = p$ then $G/Z(G)$ has order p, so it is cyclic. Then by problem 2 from this week's homework, G is again abelian.
- Now, by Lagrange's theorem, every nonidentity element of G must have order p or p^2.
- If there is an element of order p^2, then $G \cong \mathbb{Z}/p^2\mathbb{Z}$.
- Otherwise, every element has order p.
- Pick any g of order p and $h \notin \langle g \rangle$ and note $G = \langle g, h \rangle$.
- Define $\varphi : (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \to G$ that maps $(a, b) \mapsto h^a g^b$.
- It is easy to see that φ is a surjective group homomorphism, so by counting, it is an isomorphism.
- So, G is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or to $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Abelian Groups, I: They're The Nice Ones

That classification was very pleasant. Unfortunately, it turns out to be quite a bit harder to classify p-groups of larger orders.

- However, we can still do quite a bit if we restrict our attention to abelian groups.
- Abelian groups are much nicer, and so we could hope to be able to write them all down in some sort of nice way.

That is what we will do now: give a classification theorem involving abelian groups.

- We might hope to be able to decompose every abelian group as a direct product of "nice" groups (e.g., cyclic groups), like we did with groups of order p^2.
- This is roughly what we will show. But...

Abelian Groups, II: They're Harder Than You Think

... this is harder than it might seem, however, because there are all sorts of unpleasantly large abelian groups, and it can be hard to tell them apart.

- For example, you might reasonably think that $\mathbb{R}$ and $\mathbb{C}$ are different as groups. (They certainly are different as fields.)
- However, in fact $\mathbb{R}$ and $\mathbb{C}$ are isomorphic as additive groups.
- This may seem odd, but in fact, it's because they're isomorphic as $\mathbb{Q}$-vector spaces (they have the same dimension). So, as additive groups, we have $\mathbb{C} \cong \mathbb{R}$.
- But of course, we also know that $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ (geometry!).
- So we obtain the bizarre fact that $\mathbb{R} \cong \mathbb{R} \times \mathbb{R}$ as groups.
- This is a bit of a problem if we are trying to decompose things as direct products.

Abelian Groups, III: Yes, Even The Nice Ones

In fact, even $\mathbb{Q}$, one of the nicest fields there is, has an additive group structure that is worse than you think it is.

- It is not so hard to see, in fact, that $\mathbb{Q}$ does not decompose as a direct product of two subgroups in a nontrivial way.
- Explicitly: if it did, we would have two nonzero subgroups G and H such that $G \cap H = 0$, since inside $G \times H$ we have $(G \times e) \cap (e \times H) = (e, e)$.
- But any two nonzero subgroups of $\mathbb{Q}$ have a nontrivial intersection: if $p/q \in G$ and $r/s \in H$, then $pr \in G \cap H$.
- So $\mathbb{Q}$ does not decompose as a direct product of subgroups.

Abelian Groups, IV: So What Can We Do?

This may be dispiriting, unless you were paying attention when I said we'd prove a classification theorem.

- The common thread in the examples I gave (namely, $\mathbb{R}$ and $\mathbb{Q}$) is that these groups are not finitely generated.
- The additive group $\mathbb{Z}[i]$ of Gaussian integers, however, is finitely generated (by 1 and i), and in fact $\mathbb{Z}[i] \cong \mathbb{Z} \times \mathbb{Z}$ as a group.
- So perhaps we can still hope that finitely generated abelian groups will behave nicely.
- This turns out to be the case!

Finitely Generated Abelian Groups, I

Our classification, broadly stated, is as follows:

Theorem (Finitely Generated Abelian Groups)

If G is a finitely generated abelian group, then G is isomorphic to a direct product of cyclic groups.

We will in fact give two different, more precise, statements of this theorem. As some illustrations of the general idea:

- $\mathbb{Z}/120\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$
- $(\mathbb{Z}/64\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/16\mathbb{Z})$.
- $\mathbb{Z}[\sqrt[3]{2}] \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

Abelian Groups Finitely Generated, II

The main idea of the proof is essentially row-reduction.

- Specifically, we consider the various relations among the generators, and then use elementary row and column operations in the resulting "relations matrix" to convert the relations into an essentially diagonal form.
- We can then read off the structure of the group as a direct product of cyclic groups.
- The approach we give is really a special case of the general classification of modules over principal ideal domains[1], and essentially the same method can be adapted to prove that more general classification[2].

---

[1] A PID is an integral domain in which every ideal is principal.

[2] The classification of modules over PIDs gives an easy proof of the existence and uniqueness of the rational canonical form (mentioned earlier) and also the Jordan canonical form of a matrix. Take Math 5112 to learn more.

Abelian Finitely Generated Groups, III

First, a lemma:

Lemma

If G is a finitely generated abelian group, then G is finitely presented. In other words, G has a presentation with finitely many generators and finitely many relations.

The content here is that any collection of relations between the generators can always be reduced to a finite set.

We will remark that the result is not true for nonabelian groups.

- Here is a nonabelian finitely generated that is not finitely presented: $\langle a, b, t | tab^i at^{-1} = ba^i b,\ i \in \mathbb{Z} \rangle$. It is of course not easy to establish that this group is not finitely presented.

Abelian Generated Finitely Groups, IV

Proof:

- Induct on number of generators n.
- For the base case $n = 1$, we appeal to our characterization of cyclic groups, which can all be described using ≤ 1 relation.
- For the inductive step, suppose any abelian group with n generators is finitely presented.
- Suppose G is abelian and has $n + 1$ generators $g_1, \ldots, g_n, h$, where we write G as an additive group.
- Since G is abelian, any such relation has the form $ah + b_1 g_1 + \cdots + b_n g_n = 0$ for some $a, b_i \in \mathbb{Z}$.

Abelian Groups Generated Finitely, V

Proof (continued):

- Consider the set of all possible tuples $(a, b_1, \ldots, b_n) \in \mathbb{Z}^{n+1}$ for all possible relations $ah + b_1 g_1 + \cdots + b_n g_n = 0$ between the generators $h, g_1, \ldots, g_n$.
- This set is a subgroup of $\mathbb{Z}^{n+1}$ since it contains the zero vector and is closed under subtraction, since the difference of two relations is also a relation.
- The set of first coordinates of these tuples (i.e., the possible coefficients of h in all possible relations) is a subgroup of $\mathbb{Z}$.
- If the subgroup is the trivial subgroup (0), then h does not appear in any relations: thus, all relations involve elements in the subgroup $\langle g_1, \ldots, g_n \rangle$, and so by the inductive hypothesis we may reduce the collection to a finite set.

Generated Finitely Abelian Groups, VI

Proof (continued more):

- Otherwise, suppose the subgroup is $d\mathbb{Z}$ with $d > 0$. Then there exists a relation (*) of the form $dh + e_1 g_1 + \cdots + e_n g_n = 0$, and the coefficient of h in every other relation is a multiple of d.
- We may then eliminate h from every other relation by subtracting an appropriate multiple of the relation (*).
- Then, just as before, all of the remaining relations lie in the subgroup $\langle g_1, \ldots, g_n \rangle$, so by the inductive hypothesis we may reduce the collection to a finite set.
- Adjoining the relation $dh + e_1 g_1 + \cdots + e_n g_n = 0$ then yields a finite set of relations that generate all relations, as claimed.

Finitely Abelian Generated Groups, VII

We can now give the proof of one version of the theorem, using a similar idea as that used in the lemma:

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 $a_1, \ldots, a_k$ 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 prove the existence of this decomposition. The uniqueness will follow from the second version, which we do after this one.

The ideas are similar to the ones we used in proving the lemma.

Generated Groups Abelian Finitely, VIII

Proof:

- Suppose G is a finitely generated abelian group, written additively.
- By the lemma, G has a presentation with finitely many generators and finitely many relations: suppose the generators are $g_1, \ldots, g_n$ and the relations are $r_i : a_{1,i}g_1 + \cdots + a_{1,n}g_n = 0$ for each $1 \leq i \leq m$.
- Then we obtain a "relations matrix" $A = \{a_{i,j}\}_{1 \leq i \leq m, 1 \leq j \leq n}$.

Groups Abelian Finitely Generated, IX

Proof (more):

- We may perform various elementary row and column operations on the relations matrix. Specifically:
  1. We may interchange two rows.
  2. We may interchange two columns: this corresponds to changing the order of the generators.
  3. We may negate a row.
  4. We may negate a column: this corresponds to replacing a generator with its inverse.
  5. We may add an integer multiple of one row to another: this does not change the subgroup the relations generate.
  6. We may add an integer multiple of one column to another: this corresponds to a change of variables in the generators $(g, h \mapsto g, h + ag)$.
- None of these operations changes the isomorphism type of G.

Finitely Abelian Groups Generated, X

Proof (more still):

- Now perform the Euclidean algorithm on the upper left entry of A with the other entries in the first row, and then the first column, to obtain a matrix of the form
$$A' = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m,2} & \cdots & b_{m,n} \end{pmatrix}.$$
- Now repeat the procedure on the lower $(m-1) \times (n-1)$ matrix, iteratively, to obtain a "diagonal" matrix
$$D = \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_l \end{pmatrix}.$$ (It is not actually diagonal since m need not equal n.)

Groups Finitely Abelian Generated, XI

Proof (even more still):

- We can then copy $c_2, \ldots, c_l$ into the top row of the matrix and perform the Euclidean algorithm on them, placing the resulting gcd a_1 in the upper-left entry, and then remove the rest of the entries in the top row.
- By construction, we see that a_1 divides all of the entries of the matrix.
- By repeating this procedure, we obtain a relations matrix

$$D' = \begin{pmatrix} a_1 & & & & \\ & \ddots & & & \\ & & a_k & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}, \text{ where } a_1 | a_2 | \cdots | a_k.$$

Generated Abelian Groups Finitely, XII

Proof (even yet more still):

- Now, each step leaves the isomorphism type of G unchanged.
- Therefore, we see that G is isomorphic to the group with presentation $\left\langle h_1, \ldots, h_n \,|\, h_1^{a_1} = e, \ldots, h_k^{a_k} = e \right\rangle$.
- It is easy to see this is a presentation of $(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_k\mathbb{Z}) \times \mathbb{Z}^{n-k}$.
- Thus, G is isomorphic to a direct product of cyclic groups of the claimed form.

Finitely Groups Generated Abelian, XIII

To illustrate, suppose $G = \langle x, y, z | -6x + 3y = 0,\ 10x + 5y = 0 \rangle$.

- Then the relations matrix is $\begin{bmatrix} -6 & 3 & 0 \\ 10 & 5 & 0 \end{bmatrix}$.
- Now if you can do row and column operations:

$$\begin{bmatrix} -6 & 3 & 0 \\ 10 & 5 & 0 \end{bmatrix} \longrightarrow [\text{calculations go here}] \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 60 & 0 \end{bmatrix}.$$

- The relations matrix now has the desired form, so we can read off the presentation: it is $\langle p, q, r | p = 0, 60q = 0 \rangle$.
- This describes the group $(\mathbb{Z}/1\mathbb{Z}) \times (\mathbb{Z}/60\mathbb{Z}) \times \mathbb{Z}$, or equivalently, $\mathbb{Z} \times (\mathbb{Z}/60\mathbb{Z})$.

Generated Abelian Finitely Groups, XIV

The cyclic factors in this decomposition of G are called the invariant factors of G.

- We next describe how we can break each of the cyclic factors in the decomposition into prime powers. (The answer is the Chinese remainder theorem.)
- We will use this observation to establish a different form of the classification theorem (using "elementary divisors"), which is easier to use to establish the uniqueness.
- It is also easier to use the elementary divisor form to classify the abelian groups of a given order.
- We will discuss how to do all of these things next time.

Summary

We discussed groups acting on themselves by conjugation and derived some useful facts from studying this action.

We gave a classification of finitely-generated abelian groups and discussed some related facts.

Next lecture: More abelian groups, Sylow's theorems.