Math 5111 (Algebra 1)

Lecture #14 of 24 $\sim$ October 19th, 2020

Group Isomorphism Theorems + Group Actions

- The Isomorphism Theorems for Groups
- Group Actions
- Polynomial Invariants and A_n

This material represents §3.2.3-3.3.2 from the course notes.

Quotients and Homomorphisms, I

Like with rings, we also have various natural connections between normal subgroups and group homomorphisms.

- To begin, observe that if $\varphi : G \to H$ is a group homomorphism, then $\ker \varphi$ is a normal subgroup of G.
- In fact, I proved this fact earlier when I introduced the kernel, but let me remark again: if $g \in \ker \varphi$, then for any $a \in G$, then $\varphi(aga^{-1}) = \varphi(a)\varphi(g)\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = e$. Thus, $aga^{-1} \in \ker \varphi$ as well, and so by our equivalent properties of normality, this means $\ker \varphi$ is a normal subgroup.
- Thus, we can use homomorphisms to construct new normal subgroups.

Quotients and Homomorphisms, II

Equally importantly, we can also do the reverse: we can use normal subgroups to construct homomorphisms.

- The key observation in this direction is that the map $\varphi : G \to G/N$ associating a group element to its residue class / left coset (i.e., with $\varphi(a) = \overline{a}$) is a ring homomorphism.
- Indeed, the homomorphism property is precisely what we arranged for the left cosets of N to satisfy: $\varphi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \varphi(a) \cdot \varphi(b)$.
- Furthermore, the kernel of this map φ is, by definition, the set of elements in G with $\varphi(g) = e$, which is to say, the set of elements $g \in N$.

Thus, kernels of homomorphisms and normal subgroups are precisely the same things.

Quotients and Homomorphisms, III

Let us summarize these observations:

Proposition (Projection Homomorphisms)

If N is a normal subgroup of G, then the map $\varphi : G \to G/N$ defined by $\varphi(a) = \overline{a} = aN$ is a surjective group homomorphism called the projection homomorphism from G to G/N.

Proof:

- We have $\varphi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \varphi(a) \cdot \varphi(b)$, so φ is a homomorphism. Also, φ is surjective, essentially by definition: any residue class in G/N is of the form gN for some $g \in G$, and then $\varphi(g) = gN$.

Quotients and Homomorphisms, IV

We also get the analogous statement of the first isomorphism theorem:

Theorem (First Isomorphism Theorem)

If $\varphi : G \to H$ is a group homomorphism, then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi$ is isomorphic to $\operatorname{im} \varphi$.

Intuitively, φ is a surjective homomorphism $\varphi : G \to \operatorname{im}\varphi$.

- To turn it into an isomorphism, we must "collapse" its kernel to a single element: this is precisely what the quotient group $G/\ker \varphi$ represents.

The proof is the same as for rings: we simply write down the isomorphism and verify it is well-defined and is an isomorphism.

Quotients and Homomorphisms, V

Proof:

- Let $N = \ker \varphi$. We have already shown that N is a normal subgroup of G, so now we will construct a homomorphism $\psi : G/N \to \operatorname{im} \varphi$, and then show that it is injective and surjective.
- The map is defined as follows: for any residue class $gN \in G/N$, we define $\psi(gN) = \varphi(g)$.
- To see ψ is well-defined, suppose that $g' \in gN$ is some other representative of the coset gN. Then $g' = gn$ for some $n \in N$, so $\psi(g'N) = \varphi(g') = \varphi(gn) = \varphi(g)\varphi(n) = \varphi(g) = \psi(gN)$ since $n \in \ker \varphi$, so ψ is well-defined.

Quotients and Homomorphisms, VI

Proof (continued):

- It is then easy to see ψ is a homomorphism, since $\psi(\overline{a} \cdot \overline{b}) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(\overline{a})\psi(\overline{b})$.
- Next, we see that $\psi(\overline{g}) = e$ precisely when $\varphi(g) = e$, which is to say $g \in \ker(\varphi) = N$, so that $\overline{g} = \overline{e}$. Thus, the only element in $\ker \psi$ is $\overline{e}$, so ψ is injective.
- Finally, if h is any element of $\operatorname{im} \varphi$, then by definition there is some $g \in G$ with $\varphi(g) = h$: then $\psi(\overline{g}) = h$, meaning that ψ is surjective.
- Since ψ is a homomorphism that is both injective and surjective, it is an isomorphism.

Quotients and Homomorphisms, VII

By using the first isomorphism theorem, we can construct isomorphisms of groups.

- In order to show that G/N is isomorphic to a group H, we search for a surjective homomorphism $\varphi : G \to H$ whose kernel is N.
- As a particular application, we can obtain the other isomorphism theorems using the first isomorphism theorem.

Quotients and Homomorphisms, VIII

Example: Show that $\mathbb{Z}/2020\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/20\mathbb{Z}) \times (\mathbb{Z}/101\mathbb{Z})$ as a group.

Quotients and Homomorphisms, VIII

Example: Show that $\mathbb{Z}/2020\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/20\mathbb{Z}) \times (\mathbb{Z}/101\mathbb{Z})$ as a group.

- We seek a surjective homomorphism $\varphi : \mathbb{Z} \to (\mathbb{Z}/20\mathbb{Z}) \times (\mathbb{Z}/101\mathbb{Z})$ whose kernel is $50\mathbb{Z}$.
- Once this idea is suggested, it is not hard to come up with a candidate, namely, $\varphi(a) = (a \bmod 20, a \bmod 101)$.
- This map is easily seen to be a group homomorphism, and its kernel is $\{k \in \mathbb{Z} : 20|k \text{ and } 101|k\} = 2020\mathbb{Z}$ since 20 and 101 are relatively prime.
- Thus, we get an isomorphism $\tilde{\varphi} : \mathbb{Z}/2020\mathbb{Z} \to \text{im}(\varphi)$. However, since the domain of $\tilde{\varphi}$ has cardinality 2020, the image must also, so in fact $\tilde{\varphi}$ is surjective, hence an isomorphism.

Quotients and Homomorphisms, IX

Theorem (Second Isomorphism Theorem)

If $A \trianglelefteq G$ and B is any subgroup of G, then $AB = \{ab : a \in A, b \in B\}$ is a subgroup of G, $A \cap B$ is a normal subgroup of B, and $(AB)/B$ is isomorphic to $A/(A \cap B)$.

Theorem (Third Isomorphism Theorem)

If H and K are normal subgroups of G with $H \leq K$, then $H \trianglelefteq K$, $(K/H) \trianglelefteq (G/H)$, and $(G/H)/(K/H)$ is isomorphic to G/K.

Theorem (Fourth Isomorphism Theorem)

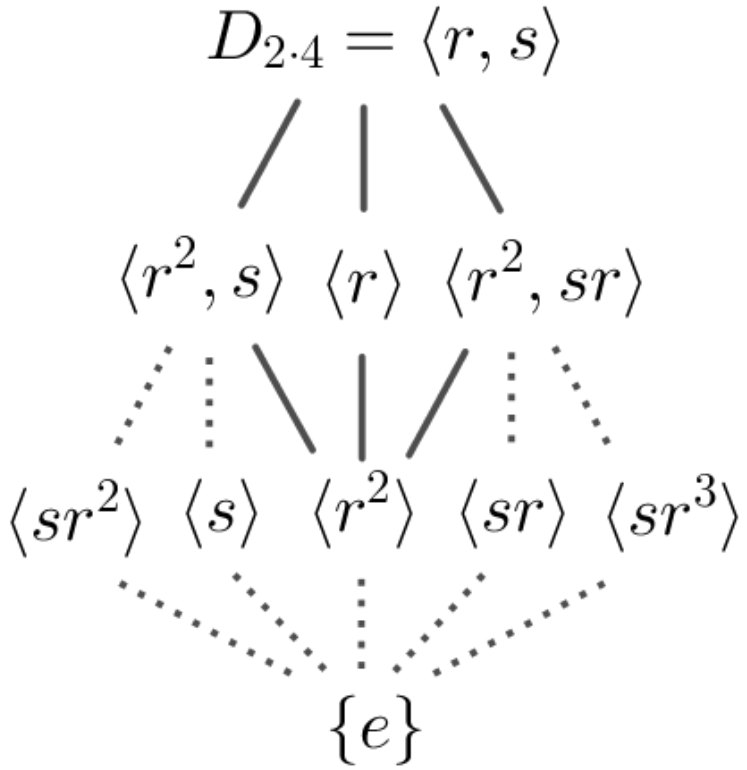
If $N \trianglelefteq G$, there is an inclusion-preserving bijection between the subgroups A of G containing N and the subgroups $\overline{A} = A/N$ of G/N. This bijection preserves the subgroup lattice structure, in the sense that it respects indexes, joins, intersections, and normality.

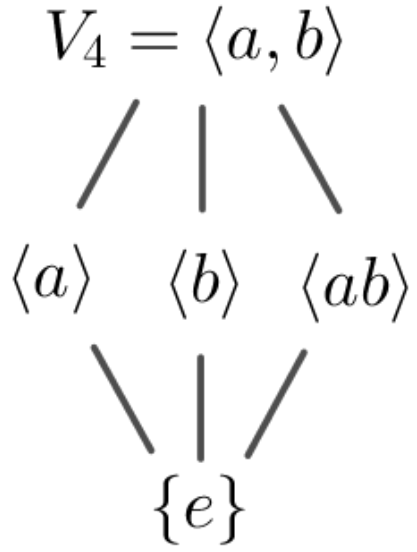
Quotients and Homomorphisms, X

- [2nd isom thm]: Show $(AB)/B$ is isomorphic to $A/(A \cap B)$.
- [3rd isom thm]: Show $(G/H)/(K/H)$ is isomorphic to G/K.
- [4th isom thm]: If $N \leq A$, show that $A \leftrightarrow A/N$ preserves the subgroup lattice structure of G, in the sense that it respects indexes, joins, intersections, and normality.

Quotients and Homomorphisms, XI

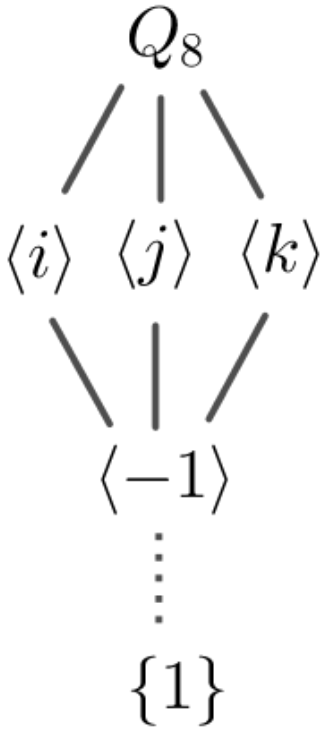
Example: We showed that $N = \langle r^2 \rangle$ is normal in $G = D_{2\cdot 4}$, and that the quotient G/N is isomorphic to the Klein 4-group.

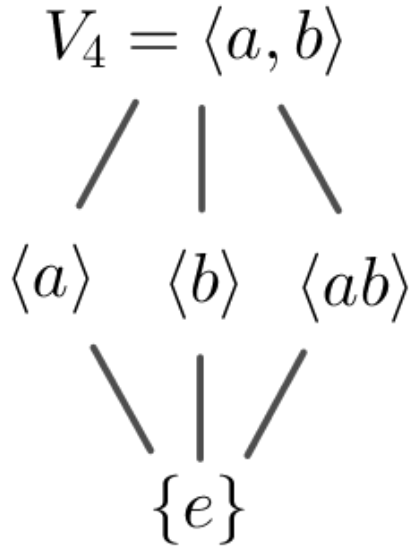




Quotients and Homomorphisms, XII

Example: We showed that $N = \langle -1 \rangle$ is normal in $G = Q_8$, and that the quotient G/N is isomorphic to the Klein 4-group.





Quotients and Homomorphisms, XIII

Example: Identify explicitly the residue classes in $(\mathbb{Z}/20\mathbb{Z})/(5\mathbb{Z}/20\mathbb{Z})$, and identify the quotient group.

Quotients and Homomorphisms, XIII

Example: Identify explicitly the residue classes in $(\mathbb{Z}/20\mathbb{Z})/(5\mathbb{Z}/20\mathbb{Z})$, and identify the quotient group.

- By the third isomorphism theorem, the quotient is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.
- We can work this out explicitly by noting that for $G = \mathbb{Z}/20\mathbb{Z}$ and $H = 5\mathbb{Z}/20\mathbb{Z}$, we have elements $G = \{0, 1, \ldots, 19\}$ and $H = \{0, 5, 10, 15\}$.
- So there are indeed five cosets of H, namely $0 + H = \{0, 5, 10, 15\}$, $1 + H = \{1, 6, 11, 16\}$, $2 + H = \{2, 7, 12, 17\}$, $3 + H = \{3, 8, 13, 18\}$, and $4 + H = \{4, 9, 14, 19\}$.
- The arithmetic of these residue classes is exactly the same as the arithmetic in $\mathbb{Z}$ modulo 5.

Group Actions, I

We initially motivated the idea of a group as arising naturally from collections of symmetries of geometric or algebraic objects.

- We can make this interaction more precise using group actions, which formalize the notion of a group "acting on" a set in a way that is compatible with the structure of the group.
- If we think of a group as a collection of symmetries of an object (and we think of the object as a set), each element of the group will behave as a function from the set to itself, and function composition will agree with the group operation.
- Furthermore, the identity element of the group will act as the identity function, and inverses in the group will act as the corresponding inverse function.

Group Actions, II

These requirements lead to the definition of a group action.

Definition

If G is a group and A is a set, a (left) group action of G on A is a function from $G \times A$ to A, written as $g \cdot a$, such that

[A1] *The action is compatible with the group operation:*
$g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ *for any* $g_1, g_2 \in G$ *and* $a \in A$.

[A2] *The identity acts as the identity map:* $e \cdot a = a$ *for all* $a \in A$.

There is also a notion of a right group action, which is a function from $A \times G$ to A whose [A1] statement is $(a \cdot g_2) \cdot g_1 = a \cdot (g_2 g_1)$ and whose [A2] statement is $a \cdot e = a$.

Left and right group actions can be interchanged by observing that if $g \cdot a$ yields a left action, then $a \cdot g^{-1}$ yields a right action.

Group Actions, III

Examples:

1. (S_n): If $A = \{1, 2, \ldots, n\}$, then S_n acts on A via permutation. Explicitly, the action is $\sigma \cdot a = \sigma(a)$.
   - For example, if $n = 5$ we have $(1\,2\,3\,4) \cdot 1 = 2$, $(1\,2\,3)(4\,5) \cdot 4 = 5$, and $(2\,5\,1)(3\,4) \cdot 5 = 1$.
   - For [A1] we have $\sigma \cdot (\tau \cdot a) = \sigma \cdot (\tau(a)) = \sigma(\tau(a)) = (\sigma\tau)(a) = (\sigma\tau) \cdot a$ by the definition of the group action in S_n as function composition.
   - For [A2] we have $1 \cdot a = a$ for all $a \in A$ by the definition of the identity permutation.

Group Actions, IV

Examples:

2. $(D_{2\cdot n})$: If $A = \{V_1, V_2, \ldots, V_n\}$ is the set of vertices of a regular n-gon (labeled counterclockwise), then $D_{2\cdot n}$ acts on A by the geometric interpretation we used to define $D_{2\cdot n}$.
   - For example, we have $r \cdot V_1 = V_2$, $r \cdot V_2 = V_3$, ... , $r \cdot V_{n-1} = V_n$, and $r \cdot V_n = V_1$, and $s \cdot V_1 = V_1$, $s \cdot V_2 = V_n$, $s \cdot V_3 = V_{n-1}$, ... , and $s \cdot V_n = V_2$.
   - The verification that this actually is a group action follows from the analysis we did in originally describing $D_{2\cdot n}$ from its geometric definition.

Group Actions, V

Examples:

3. (Vector Space Multiplication): If $A = V$ is an F-vector space, then we have a group action $G = F^\times$ on V via scalar multiplication.
    - Explicitly, using $\star$ for the group action, we have $\alpha \star v = \alpha v$ for every $v \in A$ and $\alpha \in G$.
    - Axioms [A1] and [A2] follow in this case by the corresponding axioms for vector spaces.
4. (Trivial Action): If G is any group and A is any set, then the trivial group action with $g \cdot a = a$ for all $g \in G$ and $a \in A$ is a group action of G on A.
    - It is easy to see that the trivial action satisfies both [A1] and [A2].

Group Actions, VI

Examples:

5. (Left-Multiplication Action): If G is any group, then the left-multiplication action of G on itself is defined via $g \cdot a = ga$ for any $g \in G$ and $a \in G$.
   - The underlying set in this case is $A = G$.
   - For [A1], we have $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a) = g_1(g_2 a) = (g_1 g_2)a = (g_1 g_2) \cdot a$ by associativity in G.
   - For [A2], we have $e \cdot a = ea = a$ by the identity property in G.

Group Actions, VII

Examples:

6. (Conjugation Action): If G is any group, then the conjugation action of G on itself is defined via $g \cdot a = gag^{-1}$ for any $g \in G$ and $a \in G$.
   - Here we also take the underlying set to be $A = G$.
   - For [A1], we have $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1 g_2 (a g_2^{-1}) g_1^{-1} = (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \cdot a$.
   - For [A2], we have $e \cdot a = eae^{-1} = a$.

Group Actions, VIII

Examples:

7. (Automorphisms) For an algebraic object X, which for us will be a group, ring, vector space, or field, the set of automorphisms of X (the isomorphisms of X with itself) act on the set of elements of A.
    - This example, in the category of fields, is really the reason we are discussing groups in the first place.
    - For [A1], we need only observe that function composition is (by definition) the composition operation in the group.
    - For [A2], the identity map (trivially) acts as the identity.
    - Other algebraic(ish) objects whose automorphism one can also fruitfully discuss include sets (yielding symmetric groups, as we discussed), modules, graphs, and algebras.

Group Actions, IX

Notice that we did not include as part of the definition of group action that inverses in the group act as the corresponding inverse function

- In fact, it actually follows from [A1] and [A2].
- Explicitly, by [A1] and [A2], for any $g \in G$ we have $g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = e \cdot a = a$ and also $g \cdot (g^{-1} \cdot a) = (gg^{-1}) \cdot a = e \cdot a = a$: thus, g^{-1} acts as the inverse function of g.
- For each $g \in G$, we obtain a map $\sigma_g : A \to A$ given by $\sigma_g(a) = g \cdot a$; the calculation above shows that σ_g is a bijection with inverse $\sigma_{g^{-1}}$.
- Thus, under the group action, each element $g \in G$ is associated with a bijection σ_g from A to itself, which is an element of the permutation group S_A.

Group Actions, X

In fact, axiom [A1] tells us that the association of an element $g \in G$ with the associated permutation $a \mapsto g \cdot a$ of A is a group homomorphism from G to S_A.

- Explicitly, for any $a \in A$, we have $\sigma_{g_1 g_2}(a) = (g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_2}(a))$, and thus $\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2}$ as functions.
- Conversely, any group homomorphism from G to S_A yields a group action of G on A: [A1] follows by the same calculation performed above, while [A2] follows by the observation that any homomorphism from G to S_A must map the identity of G to the identity of S_A.

Group Actions, XI

Together, our observations show that a group action of G on A is the same as a group homomorphism from G to S_A.

- The idea, in other words, is that each element of G acts by permuting the elements of A in a way that is consistent with the group operation in G.

We can get some additional information by looking at the kernel of this homomorphism.

Definition

The kernel of the group action of G on A is the kernel of the associated homomorphism from G to S_A, namely, the set of $g \in G$ with $g \cdot a = a$ for all $a \in A$. The group action is faithful if its kernel consists of only the identity element.

Group Actions, XII

Examples:

1. The action of $D_{2 \cdot n}$ on the vertices of an n-gon is faithful, as is the action of S_n on $\{1, 2, \ldots, n\}$ and the action of $F^\times$ on an F-vector space V.
2. The kernel of the trivial action of G on A is all of G, and is thus not faithful if G is not the trivial group.
3. The kernel of the left-multiplication action of G on itself is $\{e\}$ (by cancellation), and is therefore faithful.
4. The kernel of the conjugation action of G on itself is its center $Z(G)$. If $Z(G) = \{e\}$ then the action is faithful, and otherwise it is not faithful.

Group Actions, XIII

If a group action is faithful, then the associated homomorphism from G to S_A is injective.

- Then, by the first isomorphism theorem, we see that G is isomorphic to its image in S_A.

Applying this observation in particular to the left-multiplication action of G on itself (which is faithful, as we noted on the last slide) yields the following theorem:

Theorem (Cayley's Theorem)

Every group is isomorphic to a subgroup of a symmetric group. Furthermore, if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Group Actions, XIV

Historically, groups were initially conceived as being permutation groups (i.e., subsets of symmetric groups), and it was only later that the axiomatic definition we used was adopted.

- Cayley's theorem, then, indicates that the historical and modern conceptions of a group are equivalent.
- Although the historical definition is more concrete, the axiomatic approach has the advantage of not requiring us to specify a particular symmetric group of which G is a subgroup, and makes many other tasks (e.g., involving homomorphisms and isomorphisms) much easier to handle.

Group Actions, XV

Example: For $G = Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, if we label the elements $\{1, 2, 3, 4, 5, 6, 7, 8\}$ in that order, then i corresponds to the permutation $(1\,3\,2\,4)(5\,7\,6\,8)$ and j corresponds to the permutation $(1\,5\,2\,6)(3\,8\,4\,7)$.

- Thus, since Q_8 is generated by i and j, we see that the subgroup of S_8 generated by $(1\,3\,2\,4)(5\,7\,6\,8)$ and $(1\,5\,2\,6)(3\,8\,4\,7)$ is isomorphic to Q_8.
- If desired, we could write down the corresponding actions for the other elements of Q_8 to identify all 8 permutations in this isomorphic copy of Q_8 inside S_8.

Group Actions, XVI

We will mention that, even though a group G of order n necessarily embeds into S_n, it is certainly possible for G to be isomorphic to a subgroup of a smaller symmetric group.

- For example, since the action of $D_{2\cdot 4}$ on the four vertices of the square is faithful, we see that S_4 contains a subgroup isomorphic to $D_{2\cdot 4}$.
- Explicitly, this subgroup is generated by the images of r and s, which by the original convention we took, would be $(1\,2\,3\,4)$ and $(2\,4)$, respectively.
- If instead we used the left-multiplication of $D_{2\cdot 4}$ on itself, we would instead realize $D_{2\cdot 4}$ as (isomorphic to) a subgroup of S_8.

Group Actions, XVII

If we have a (nontrivial) action of G on A, we can often obtain important structural information about G and about A by studying the group action.

Definition

If G acts on A, then for any $a \in A$ the stabilizer of a is the set $G_a = \{g \in G : g \cdot a = a\}$ of elements of g fixing a.

The stabilizer is a subgroup of G:

- Clearly $e \in G_a$ by [A2], and if $g, h \in G_a$ then $(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a$ by [A1], and also $a = e \cdot a = (g^{-1}g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a$ so $g^{-1} \in G_a$.

Group Actions, XVIII

Examples:

1. For the action of S_n on $\{1, 2, \ldots, n\}$ by permutation, the stabilizer of n is the collection of all permutations that fix n. Since such permutations can permute $\{1, 2, \ldots, n-1\}$ arbitrarily, this stabilizer is isomorphic to S_{n-1}.
2. For the action of $D_{2 \cdot n}$ on the vertices $\{V_1, \ldots, V_n\}$ of a regular n-gon, the stabilizer of any vertex V_i consists of the identity map along with the reflection along the line passing through the center of the n-gon and V_i.
3. For the left-multiplication action of G on itself, the stabilizer of any $a \in G$ consists of only the identity (by cancellation).
4. For the conjugation action of G on itself, the stabilizer of any element $a \in G$ consists of all elements $g \in G$ such that $gag^{-1} = a$, which is to say, all elements $g \in G$ with $ga = ag$ (i.e., all elements of G that commute with a).

Group Actions, XIX

We also have a related notion of the orbit of an element under the action of G:

Definition

If G acts on A, then the orbits of G acting on A are the equivalence classes of the equivalence relation on A given by $a \sim b$ if there exists $g \in G$ with $b = g \cdot a$.
If there is a single orbit (namely, A itself) then we say the action of G on A is transitive.

- It is straightforward to verify that $\sim$ is indeed an equivalence relation, so it makes sense to speak of its equivalence classes.

Group Actions, XX

Explicitly, the orbits are the sets $G \cdot a = \mathcal{O}_a = \{g \cdot a : g \in G\}$ for the various elements $a \in A$.

- The set $G \cdot a$ is the orbit of a under G, and (per the definition) is the subset of A that can be obtained by starting at a and applying an element of G.
- The term "orbit" is intended to connote the idea that the action of G sends a to various different places, and the orbit of a is the collection of all the places that a can go.

Group Actions, XXI

Examples:

1. For the action of S_n on $\{1, 2, \ldots, n\}$ by permutation, for $\sigma = (1\,2\,3\,\ldots\,n)$ we have $\sigma \cdot 1 = 2$, $\sigma \cdot 2 = 3$, ... , and $\sigma \cdot n = 1$, so there is a single orbit consisting of the entire set $\{1, 2, \ldots, n\}$. This means the action is transitive.
2. The left-multiplication action of G on itself is transitive, since for any $g, h \in G$ we have $(hg^{-1}) \cdot g = h$.
3. For the conjugation action of $G = S_3$ on itself, there are three orbits: $\{e\}$, $\{(1\,2), (1\,3), (2\,3)\}$, and $\{(1\,2\,3), (1\,3\,2)\}$.

Group Actions, XXII

There is an incredibly important combinatorial relation between orbits and stabilizers:

Proposition (Orbit-Stabilizer Theorem)

If G acts on the set A, then the number of elements in the orbit $\mathcal{O}_a$ is equal to $[G : G_a]$, the index of the stabilizer of a.

This result is very intuitive:

- The orbit counts how many different places that G can send the element a. The stabilizer measures how many elements of g must send a to itself.
- The idea is then that if G moves a to many different places, then few elements of G can send a to itself.
- It is analogous to the nullity-rank theorem: if T has a large image, then few elements can be mapped to zero.

Group Actions, XXIII

Proof:

- We will show that there is a bijection between elements $b \in \mathcal{O}_a$ and the left cosets bG_a of the stabilizer G_a.
- Consider the map $f : G \to A$ with $f(g) = g \cdot a$.
- Then for any $g, h \in G$, we see that $f(g) = f(h)$ iff $g \cdot a = h \cdot a$ iff $a = g^{-1} \cdot (h \cdot a) = (g^{-1}h) \cdot a$ iff $g^{-1}h \in G_a$ iff $gG_a = hG_a$.
- Therefore, for any $b \in \mathcal{O}_a$ with $b = g \cdot a$, we see that the fiber $f^{-1}(b)$ of the map f is precisely the left coset gG_a.
- This means that f yields a bijection between the left cosets of G_a with the elements of the orbit $\mathcal{O}_a$ of a.
- The claimed result then follows immediately because the number of left cosets of G_a equals $[G : G_a]$, as we showed previously.

Group Actions, XXIV

The orbit-stabilizer theorem has a number of important applications in enumerative combinatorics, since it provides a way to enumerate orbits under group actions in a convenient way.

- We will also make use of the orbit-stabilizer theorem in our analysis of groups – in particular, we will obtain a number of useful consequences by analyzing the orbits and stabilizers of the conjugation action of G on itself.

To illustrate, we reinterpret the proof of Cauchy's theorem using the orbit-stabilizer theorem:

- The idea was to look at the cycling action of $\mathbb{Z}/p\mathbb{Z}$ on ordered p-tuples of elements $(g_1, g_2, \ldots, g_p)$ such that $g_1 \cdots g_p = e$.
- The possible sizes of an orbit, by the orbit-stabilizer theorem, are the possible indices of the stabilizer, which are 1 and p.
- We then immediately obtain Cauchy's theorem by counting the total number of tuples, grouped together in orbits.

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, VIII

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, IX

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, X

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, XI

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, XII

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).

Summary

We discussed the isomorphism theorems for groups.

We introduced the notion of a group action and discussed some basic properties of group actions.

We introduced the action of S_n on polynomials by index permutation and used it to establish some properties of A_n.

Next lecture: Conjugation actions, finitely-generated abelian groups.