Graduate Algebra, Fall 2014
Lecture 16

Andrei Jorza

2014-10-01

1 Group Theory

1.18 Simpliciy of A_n

Theorem 1. *The group A_n is simple for $n \neq 4$. The group A_4 contains $(\mathbb{Z}/2\mathbb{Z})^2$ as a normal subgroup.*

Proof. We already know that $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ is simple and that $\langle (12)(34), (13)(24) \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2 \subset A_4$ is normal.

We now show by induction that A_n is simple for $n \geq 5$. The base case is that the group A_5 is simple. Indeed, $\mathrm{Syl}_5(A_5)$ contains $\langle (12345) \rangle$ and $\langle (13245) \rangle$. Now let $G = A_n$ and suppose that it has a proper normal subgroup H. Let $G_i = \{\sigma \in A_n | \sigma(i) = i\}$ in which case $G_i \cong A_{n-1}$ is simple by the inductive hupothesis. Thus $G_i \cap H \lhd G_i$ implies either that $H \cap G_i = 1$ or $H \cap G_i = G_i$.

If $G_i \subset H$ for some i then $\sigma G_i \sigma^{-1} = G_{\sigma(i)} \subset \sigma H \sigma^{-1} = H$ and so $G_i \subset H$ for all i. But $G = \langle G_1, \ldots, G_n \rangle$ (indeed, every $\sigma \in A_n$ is a product of an even number of transpositions and if $n \geq 5$ then any product of two transpositions is in some G_i). Thus contradicts that H is proper in G.

Thus $H \cap G_i = 1$ for all i. Thus H acts freely by permutations on $\{1, \ldots, n\}$ since if $\sigma(i) = \tau(i)$ then $\sigma\tau^{-1}(i) = i$ and so $\sigma\tau^{-1} \in H \cap G_i$ so $\sigma = \tau$ in H. Pick $\sigma \in H$ and write it as a product of disjoint permutations $\sigma = c_1 \cdots c_k$. Suppose c_i has length ≥ 3 with $c_i = (a_1, a_2, a_3, \ldots)$. Pick $\tau \in G$ with τ fixing a_1 and a_2 but not a_3 (e.g., a product of two transpositions which include a_3 but not a_1, a_2). Then $\tau\sigma\tau^{-1}$ and σ both take a_1 to a_2 but they take a_2 to different values. This contradicts the normality of H.

Therefore H consists of products of even numbers of disjoint transpositions. If $\sigma = (a_1 a_2)(a_3 a_4)(a_5 a_6) \cdots \in H$ then for $\tau = (a_1 a_2)(a_3 a_5)$ we have both σ and $\tau\sigma\tau^{-1} = (a_1 a_2)(a_5 a_4)(a_3 a_6) \cdots$ take a_1 to a_2 but take a_3 to different values. This contradicts the normality of H.

Finally, H must contain only products of two disjoint transpositions. Pick $(ab)(cd) \in H$ and u, v not among the a, b, c, d ($n \geq 6$). Write $\sigma = (ab)(cd)$ and $\tau = (cu)(dv)$. Then σ and $\tau\sigma\tau^{-1} = (ab)(uv)$ both that a to b but are not the same, thus contradicting the normality of H. $\square$

An alternative means of proving the simplicity of A_n is to use the following explicit generators:

Proposition 2. *Let $n \geq 3$.*

1. $S_n = \langle (i, i+1) | 1 \leq i \leq n-1 \rangle$.
2. $S_n = \langle (12), (12 \ldots n) \rangle$.
3. $A_n = \langle (123), (12 \ldots n) \rangle$.
4. $A_n = \langle (abc) | a \neq b \neq c \neq a \rangle$.

Proof. No proof given, but we will use this statement in Galois theory. $\square$

How to prove the simplicity of A_n using this proposition? Suppose $H \lhd A_n$ is proper normal. With computations one can show that H then contains a 3-cycle. By normality it contains all of them and so cannot be proper.

1.19 Duals

Lemma 3. *Let G, H be groups. Then the set of homomorphisms $\operatorname{Hom}(G, H)$ forms a group under $(fg)(x) = f(x)g(x)$, with unit the identity map $f(x) = 1, \forall x \in G$. If H is abelian, then $\operatorname{Hom}(G, H)$ is also an abelian group, often written additively.*

Definition 4. For a group G write $G^* = \operatorname{Hom}(G, S^1)$ where $S^1 = \{z \in \mathbb{C} \| z| = 1\}$. Write $G^\vee = \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z})$.

Example 5.

1. $\mathbb{Z}^* \cong S^1$ and $\mathbb{Z}^\vee \cong \mathbb{Q}/\mathbb{Z}$.
2. $(\mathbb{Z}/n\mathbb{Z})^\vee \cong \mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^* \cong \mu_n$. Choosing a primitive n-root of unity one has $\mathbb{Z}/n\mathbb{Z} \cong \mu_n$ sending k to the k-th power of the chosen primitive root, but this depends on the choice of primitive root.

Lemma 6. *Let G be a finite group. Then, noncanonically, $G^\vee \cong G^*$.*

Proof. Consider the map $e : \mathbb{Q}/\mathbb{Z} \to S^1$ given by $e(x) = e^{2\pi i x}$, which is a well-defined injective homomorphism. This gives $\operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \operatorname{Hom}(G, \operatorname{Im} e)$. It suffices to show that every homomorphism $G \to S^1$ lands in $\operatorname{Im} e$. Indeed, $f(g^{|G|}) = 1$ and so $f(g)^{|G|} = 1$ which implies that $f(g) \in \mu_{|G|} = e(1/|G|\mathbb{Z}/\mathbb{Z}) \subset \operatorname{Im} e$. $\square$

Definition 7. The **abelianization** of a group G is defined as $G^{\text{ab}} = G/[G, G]$.

Proposition 8. *Let G be a group.*

1. *$[G, G] \lhd G$ and G^{ab} is an abelian group.*
2. *If $f : G \to A$ is a homomorphism to an abelian group then there exists a homomorphism $\overline{f} : G^{\text{ab}} \to A$ such that $G \to G^{\text{ab}} \to A$ commutes.*
3. $\operatorname{Hom}(G, A) \cong \operatorname{Hom}(G^{\text{ab}}, A)$.
4. *If G is finite then $(G^\vee)^\vee \cong G^{\text{ab}}$.*

Proof. The first part follows from $x[a, b]x^{-1} = [xa, b][b, x]$.

Suppose $f : G \to A$ is a homomorphism. Then $[G, G] \subset \ker f$ and by the first isomorphism theorem we deduce the second part.

Third part: The map $f \mapsto \overline{f}$ gives the isomorphism.

Fourth part: By part (3) it suffices to show the statement for G abelian, in this case finite. Consider $G \to (G^\vee)^\vee$ sending g to $\phi_g : f \mapsto f(g)$ for $f \in G^\vee$. This is an injective homomorphism. Indeed, if $\phi_g(f) = 0$ then $f(g) = 0$ for all f. If $g \neq 1$ then consider the natural projection $G \to \langle g \rangle$ and send g to any nonzero element to get $f : G \to A$ such that $f(g) \neq 0$, getting a contradiction. $\square$