AM 106/206: Applied Algebra **Madhu Sudan**[1]

Lecture Notes 11

October 17, 2016

- Reading: Gallian Chapters 9 & 10

1 Normal Subgroups

- Motivation:
  - Recall that the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ $(a + n\mathbb{Z})$ are the same as the congruence classes modulo n $([a]_n)$
  - These form a group under addition, isomorphic to $\mathbb{Z}_n^*$: $[a+b]_n = [a+b \bmod n]_n$ depends only on $[a]_n$ and $[b]_n$ (and not on the particular choice of coset representatives a and b), so we can define $[a]_n + [b]_n = [a+b]_n$.
  - **Q:** under what conditions on $H \leq G$ do the left-cosets of H form a group under the operation of G?
- **Def:** A subgroup H of G is *normal* iff for every $a \in G$, $aH = Ha$. If this holds, we write $H \lhd G$.
- **Proposition:** For $H \leq G$, the following are equivalent:
  - $H \lhd G$
  - for every $a \in G$, $aHa^{-1} = H$
  - for every $a \in G$, $h \in H$, $aha^{-1} \in H$. That is, if $h \in H$, then all *conjugates* of h are also in H.
- **Examples:**
  - Which subgroups of an abelian group are normal?
  - Which subgroups of S_4 are normal?
  - $A_n \lhd S_n$

[1] These notes are copied mostly verbatim from the lecture notes from the Fall 2010 offering, authored by Prof. Salil Vadhan. I will attempt to update them, but apologies if some references to old dates and contents remain.

2 Factor Groups

- **Thm 9.2:** If $H \lhd G$, then the operation $(aH)(bH) = abH$ on the left-cosets of H is well-defined (does not depend on the choice of coset representatives a, b) and forms a group, denoted G/H (called a *factor group*, the *quotient* of G by H, or "G mod H").
- **Proof:**
- **Examples:**
  - $\mathbb{Z}/n\mathbb{Z}$
  - S_n/A_n
  - $(\mathbb{Z}_3 \times \mathbb{Z}_5)/(\mathbb{Z}_3 \times \{0\})$
  - S_4/H where H is the normal subgroup of size 4.
  - $\mathbb{Z}_n/\langle a \rangle$
  - $\mathbb{R}/\mathbb{Z}$

3 Homomorphisms

- **Def:** For groups G, H, and mapping $\varphi : G \to H$ is a *homomorphism* if for all $a, b \in G$, we have $\varphi(ab) = \varphi(a)\varphi(b)$.
  - Note: we don't require that φ is one-to-one or onto!
- **Def:** For a homomorphism $\varphi : G \to H$,
  - the *image* of φ is $\text{Im}(\varphi) = \varphi(G) = \{\varphi(g) : g \in G\} \leq H$.
  - the *kernel* of φ is $\text{Ker}(\varphi) = \{g \in G : \varphi(g) = \varepsilon\} \lhd G$.
- **Thm 10.3:** If $\varphi : G \to H$ is a homomorphism, then $G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$.
  Picture:

- **Examples:**

Domain	Range	Mapping	Homo.?	Image	Kernel
$\mathbb{Z}$	$\mathbb{Z}_n$	$x \mapsto x \bmod n$			
$\mathbb{Z}_n$	$\mathbb{Z}_d$	$x \mapsto x \bmod d$			
$\mathbb{R}^n$	$\mathbb{R}^n$	$x \mapsto Mx$, M a matrix			
$\mathbb{Z} \times \mathbb{Z}$	$\mathbb{Z}$	$(x, y) \mapsto xy$			
S_n	$\{\pm 1\}$	$\sigma \mapsto \text{sign}(\sigma)$			
$\mathbb{R}$	$\mathbb{C}^*$	$x \mapsto e^{2\pi i x}$			
$\mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_3$	$(x, y) \mapsto x$			
G	G/N, where $N \lhd G$	$g \mapsto gN$			

- **Properties of Homomorphisms:**

  1. $\varphi(\varepsilon_G) = \varepsilon_H$.
  2. $\varphi(a^{-1}) = \varphi(a)^{-1}$.
  3. order($\varphi(a)$) divides order(a).

- **Properties of Images:**

  1. $\varphi(G)$ is a subgroup of H.
  2. G cyclic $\Rightarrow$ $\varphi(G)$ cyclic.
  3. G abelian $\Rightarrow$ $\varphi(G)$ abelian.

- **Properties of Kernels:**

  1. Ker(φ) is *normal* subgroup of G.
     - Can prove that K is normal by finding a homomorphism φ s.t. Ker(φ) = K.
  2. $\varphi(a) = \varphi(b) \Leftrightarrow b^{-1}a \in \text{Ker}(\varphi) \Leftrightarrow a\text{Ker}(\varphi) = b\text{Ker}(\varphi)$.
  3. φ injective (one-to-one) if and only if Ker(φ) = $\{\varepsilon\}$.

- **Proof of Thm 10.3 ($G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$):**

4 Appendix: Solvability of Groups and Polynomials

As mentioned in the first lecture groups, historically one of the reasons that led to the study of groups was the connection to solving polynomials "by the method of radicals".

Let us say that a real number is expressible by radicals, or just radical for short, if it is a (1) Rational number, or (2) the sum of two radicals, or (3) the product or ratio of two radicals or (4) the mth-root of a radical for finite m. (A radical should be obtained by a finite number of applications of rules (2)-(4).)

Polynomials over the rationals in one variable, of degree up to 4 have closed form expressions for their roots because their roots are radicals. For example, one of the roots of the polynomial $ax^2 + bx + c$ is $(-b + \sqrt{b^2 - 4ac})/2a$ which is a radical by our definition above.

Galois's proof shows that some degree 5 (and higher) polynomials are not solvable by the method of radicals. One such polynomial is $x^5 - 6x + 3$. The proof looks at a finite group arising from polynomials and analyzes their "solvability". Let us describe this group and the definition of solvability.

Suppose we have some polynomial $p(x) = c_n x^n + \cdots + c_0$. Let $\alpha_1, \ldots, \alpha_n$ be the complex roots of this polynomial, so that $p(x) = c_n \cdot \prod_{i=1}^{n}(x - \alpha_i)$. While every permutation of $\alpha_1, \ldots, \alpha_n$ also gives the roots of p, these roots are not all equivalent to each other. For example if we consider the polynomial $x^3 - 1 = 0$, its roots are $a = 1$, $b = (-1 + i\sqrt{3})/2$ and $c = (-1 - i\sqrt{3})/2$. Now while a is very different from b or c (a is real, even rational, while b and c are complex), b and c are really "indistinguishable" in some sense. This is the sense we wish to capture, and it is captured by the following group.

Definition 1 (Automorphism group of a polynomial) *Let p be a polynomial with roots $S = \{\alpha_1, \ldots, \alpha_n\}$. We say that a permutation $\pi : S \to S$ preserves the "algebra" of S if for every univariate polynomial $f(x)$ over $\mathbb{Q}$ and every n-variate polynomial $h(z_1, \ldots, z_n)$ over $\mathbb{Q}$, it is the case that $h(\alpha_1, \ldots, \alpha_n)$ is a root of f if and only if $h(\pi(\alpha_1), \ldots, \pi(\alpha_n))$ is also a root of f. Let $\mathrm{Aut}(p) \leq Sym(S)$ be the set of permutations π such that π preserves the algebra of $\{\alpha_1, \ldots, \alpha_n\}$. (Note that $\mathrm{Aut}(p)$ is closed under composition and so it is indeed a subgroup of $Sym(S)$.)*

For instance $\mathrm{Aut}(x^3 - 1) = \langle (bc) \rangle$ - which explains why b and c are similar to each other but not to a. Another example: If we let $S = \{1, \omega, \omega^2, \omega^3, \omega^4\}$ denote the roots of $x^5 - 1$, then we have $\mathrm{Aut}(x^5 - 1) = \langle (\omega, \omega^2, \omega^4, \omega^3) \rangle$. In both examples above, the automorphism group was very simple - they were abelian, even cyclic. Galois's condition says that if the group gets sufficiently complex, then the polynomial does not have radical roots (or "is not solvable by the method of radicals").

Definition 2 (Solvable groups) *Let G be a group with identity e. We say that G is solvable if there exists a series of groups $G_0, \ldots, G_m$ with $\{e\} = G_0 \lhd G_1 \lhd \cdots G_m = G$ such that for every i, G_i/G_{i-1} is cyclic.*

Theorem 3 *A polynomial $p \in \mathbb{Q}[x]$ has all radical roots if and only if $\mathrm{Aut}(p)$ is solvable.*

We won't prove this theorem since it is well out of scope for us (at least at this stage). But let us explain the intuition. Suppose β is a radical that forms a root of some polynomial p. If β is a radical then we must have proved so by constructing a series of radical elements, slowly building complexity till we reached β. So some β_1 is the first irrational number we build. So β_1 must be of the form r_0^{1/ℓ_1} for some rational number r_0. Then we apply rules (1), (2), (3) for a while till applying rule (4) again. At this stage we get $\beta_2 = r_1(\beta_1)^{1/\ell_2}$ where r_1 is some rational function (ratio of polynomials) of β_1. And so till we get $\beta_m = r_{m-1}(\beta_1, \ldots, \beta_{m-1})^{1/\ell_{m-1}}$. and finally $\beta = r_m(\beta_1, \ldots, \beta_m)$. Roughly, the G_i's correspond to the β_i's and the fact that G_i/G_{i-1} is cyclic corresponds to the fact that β_i is a root of the polynomial $x^{\ell_i} - r_{i-1}(\beta_1, \ldots, \beta_{i-1})$ whose automorphism group would be the cyclic group on $\ell_i - 1$ elements if r_{i-1} were simply a rational number.

Using this theorem it is feasible to argue that concrete polynomials are not solvable. Let us return to our example polynomial $p(x) = x^5 - 6x + 3$. Let S be the set of roots so that $\mathrm{Aut}(p) \leq Sym(S)$.

It turns out that $\mathrm{Aut}(p) = Sym(S)$. This follows from the fact that p does not have any rational factors, and that three of its roots are real, and two complex. The former fact implies that $\mathrm{Aut}(p)$ has an element of order 5 and so must be a five cycle. The latter fact implies that the autmorphism that fixes the three real roots and exchanges the two complex ones is also a permutation in the automorphism group. But now a transposition and a cyclic permutation generate all of $Sym(S)$ leading to the claim above. (Note this is not a proof, but rather a sketch of one.)

Then we argue that $Sym(S) \cong S_5$ is not solvable. It turns out the only normal subgroups of S_5 are A_5 (the alternating group) and the trivial group $\{e\}$, though I do not know of a non-exhaustive proof of this fact. But putting all these ideas together, one can show that the polynomial under consideration is indeed not solvable by the method of radicals!

Source for example and reasoning about it: "Galois Theory and the Insolvability of the Quintic Equation" by Daniel Franz obtained from a web search from `http://documents.kenyon.edu/math/FranzSenEx2010.pdf`. This article in turn attributes the example to page 629 of Dummit, David S., and Richard M. Foote. Abstract Algebra. 3rd ed. Hoboken, NJ: John Wiley and Sons, Inc, 2004.