Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

November 21, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Quintic Equations

The motivation for Galois work was the problem of the insolubility of the quintic in terms of radials. Able had shown a few years before that the general quintic had no solution but no one had been able to come up with a specific polynomial with rational coefficients which couldn't be solve.

The first thing we have to do though is to define what it means for a number to be expressible as by radicals.

Definition By Radicals

Definition 0.1.0.1. Let $\alpha \in \mathbb{C}$. We say that α is expressible by radicals over F if there is a tower of subfields

of $\mathbb{C}$

$$F = F_0 \subset F_1 \subset \cdots \subset F_r$$

where

(i) $\alpha \in F_r$

(ii) For every $j = 1, \ldots, r, F_j = F_{j-1}(\beta_j)$ where $\beta_j^{n_j} \in F_{j-1}$

Notice the similarity with the definition of those elements which can be constructed with a ruler and a strait edge. Except there the only radicals which were allowed were square roots.

Notice that the nth roots of unity $\zeta_n = e^{2\pi/n}$ are allowed in expressions by radicals. And, if $n = rs$ then $\sqrt[n]{b} = \sqrt[r]{\sqrt[s]{b}}$ and so at the cost of adding more steps we can assume all roots are pth roots for some prime integers p.

Also note that there is a great deal of ambiguity in any expression by roots as there are n different $\sqrt[n]{b}$ for every non-zero b. However as the notation is in and of itself very cumbersome we won't be using the $\sqrt[n]{b}$ often and so we won't bother trying to make it more precise.

One Root Solvable By Radicals, All Are

Theorem 0.1.0.2. *Let $f(x)$ be an irreducible polynomial over a field F. If one root of f in K can be expressed by radical so can any other.*

Proof. Suppose that one root α can be expressed by radicals, say using the tower $F = F_0 \subset \cdots \subset F_r$. Choose a field L which contains F_r and which is a splitting field of some polynomial of the form $f(x)g(x)$ over F. Then L is also the splitting field of fg over $F(\alpha)$. Let α' be a root of f in another field K' and let L' be a splitting field

of fg over $F(\alpha')$. Then we can extend the isomorphism $F(\alpha) \to F(\alpha')$ to an isomorphism $\varphi : L \to L'$. The tower of fields $F = \varphi(F_0) \subset \varphi(F_1) \subset \cdots \subset \varphi(F_r)$ shows that α' is expressible by radicals. □

Galois Groups of Prime Roots of Unity are Cy

Theorem 0.1.0.3. *Let p be a prime integer and let $\zeta_p = e^{2\pi i/p}$. For any subfield F of $\mathbb{C}$ the Galois group of $F(\zeta_p)$ over F is a cyclic group.*

Proof. Let G be the Galois group of $F(\zeta)$ over F. We define a map $v : G \to \mathbb{F}_p^\times$ as follows. Let $\sigma \in G$ be an automorphism. It will carry ζ to another root of the polynomial $x^{p-1} + \cdots + x + 1$, say to ζ^i. The exponent i is determined as an integer modulo p because ζ has multiplicitive order p. Let $v(\sigma) = i$.

Now let $\tau \in G$ be such that $v(\tau) = j$, i.e. $\tau(\zeta) = \zeta^j$. We then have

$$\sigma\tau(\zeta) = \sigma(\zeta^j) = \sigma(\zeta)^j = \zeta^{ij}$$

so $v(\sigma\tau) = v(\sigma) * v(\tau)$. Further $v(id) = 1$ as $id(\zeta) = \zeta^1$.

So, since v commutes with multiplication and is not the zero map we have $v : G \to \mathbb{F}_p^\times$. However it is also injective as ζ generates K over F. □

Galois Definition By Radicals

Theorem 0.1.0.4. *Let α be a complex number which can be expressed by radicals over F. Then a tower of fields $F = F_0 \subset \cdots \subset F_r = K$ can be found which witness this and in addition*

(iii) For each j F_j is a Galois extension of F_{j-1} and the Galois group $G(F_j/F_{j-1})$ is a cyclic group.

Proof. Suppose we have a tower $F = F_0 \subset \cdots \subset F_r$ in which $F_r = F(\beta_1, \ldots, \beta_r)$. As we have remarked we may assume that $\beta_j^{p_j} \in F_{j-1}$ for some prime p_j. Let $\zeta_{p_j} = e^{2\pi i/p_j}$ be a p_jth root of 1. We can then form a new chain of fields adjoining $(\zeta_{p_1}, \ldots, \zeta_{p_r}, \beta_1, \ldots, \beta_r)$ in that order. We then know that each of these extensions is Galois (the first by the previous theorem and the later by what we proved about Kummer extensions). □

Lets consider the Galois group of a product of polynomials $f(x)g(x)$ over F. Let K' be a splitting field of fg. Then K' contains a splitting field of K of f and F' of g. So we have the following diagram.

$$\begin{array}{ccc} & K' & \\ \cup & & \cup \\ K & & F' \\ \cup & & \cup \end{array}$$

Splitting Fields of $f(x)g(x)$

Theorem 0.1.0.5. *With the above notation, let* $G = G(K/F)$ *and* $H = G(F'/F)$ *and* $\mathcal{G} = G(K'/F)$.

(i) G *and* H *are quotients of* $\mathcal{G}$

(ii) $\mathcal{G}$ *is isomorphic to a subgroup of the product* $G \times H$.

Proof. The first assertion follows from the fact that K and F' are intermediate fields which are Galois extensions of F. Let us denote the canonical homomorphism $\mathcal{G} \to G, \mathcal{G} \to H$ by subscripts $\sigma \rightsquigarrow \sigma_f$ and $\sigma \rightsquigarrow \sigma_g$. Then σ_f describes the way that σ operates on the roots of f and σ_g describes the way it operates on the roots of g. We then get a map $\mathcal{G} \to G \times H$ by $\sigma \rightsquigarrow (\sigma_f, \sigma_g)$. If σ_f, σ_g are both the identity then σ operates trivially on the roots of fg and hence $\sigma = 1$. This shows that $\mathcal{G} \to G \times H$ is injective and so it is isomorphic to a

subgroup of $G \times H$. □

Definition Simple Group

Definition 0.1.0.6. Recall that a group is called Simple if it is not the trivial group and if it contains no proper normal subgroups.

Simple and Abelian Groups and Solvability by

Theorem 0.1.0.7. *Let f be a polynomial over F whose Galois group G is a simple non-Abelian group. Let F' be a Galois extension of F with Abelian Galois group. Let K' be a splitting field of f over F'. Then the Galois group of $G(K'/F')$ is isomorphic to G.*

Proof. We first reduce ourselves to the case that $[F' : F]$ is a prime number. To do this we suppose that the lemma has been proved in that case and we choose a cyclic quotient group H of $G(F'/F)$ of prime order. Such a quo-

tient exists because $G(F'/F)$ is abelian. This quotient determines an intermediate field $F_1 \subset F'$ which is a Galois extension of F and such that $G(F_1/F) = H$. Let K_1 be the splitting field of f over F_1. Then since $[F_1 : F]$ is a prime $G(K_1/F_1) = G$. So we may replace F by F_1 and K by K_1. Induction on $[F' : F]$ will complete the proof.

So we may assume $[F' : F] = p$ is prime and that $H = G(F'/F)$ is a cyclic group of order p. The splitting field K' will contain a splitting field of f over F, call it K. We are then in the situation of the previous theorem. So the Galois group $\mathcal{G}$ of K' over F is a subgroup of $G \times H$ and it maps surjectively to G. It follows that $|G|$ divides $|\mathcal{G}|$ and that $|\mathcal{G}|$ divides $|G \times H| = p|G|$. If $|G| = |\mathcal{G}|$ then counting degrees shows $K = K'$. In this case K contains the Galois extension F' and hence H is

a quotient of G. Since G is a nonabelian simple group this is impossible. The only remaining possibility is that $\mathcal{G} = G \times H$. Applying the main theory to the chain of field $F \subset F' \subset K'$ we conclude that $G(K'/F') = G$ as required. □

This proposition is key because it tells us that if the Galois group of f is a simple non-Abelian group then we will not make any progress towards solving for its roots if we replace F by an abelian extension.

S_5 Not Solvable By Radicals

Theorem 0.1.0.8. *The roots of a quintic polynomial $f(x)$ whose Galois group is S_5 or A_5 can not be expressed by radicals over F.*

Proof. Let K be a splitting field of f. If $G = S_5$ then the discriminant of f is not a square in F. In this case we replace F by $F(\delta)$ where δ is a square root of the

discriminant in K. The Galois group of $G(K/F(\delta))$ is A_5

It is obviously enough to show that the roots can't be expressed by radicals over $F(\delta)$ and so this reduces the case of S_5 to that of A_5

Suppose that the Galois group o f is A_5 but that some root α of f is expressible by radicals over F. Say that $\alpha \in F_r$ where $F = F_0 \subset \cdots \subset F_r$ and each extension in the chain is Galois with cyclic Galois group. Now since the Galois group of f over F is a simple group (i.e. A_5) we see by the induction and the previous theorem that the Galois group of f over F_i is A_5 to for all i.

However, since $\alpha \in F_r$ we see that f is not irreducible over F_r. So in particular the Galois group of f over F_r

will not act transitively on the five roots of f in the splitting field. Hence the Galois group can't be the alternating group A_5. $\Rightarrow\Leftarrow$. □

Now we will come up with a specific quintic polynomial whose Galois group is S_5. The fact that G acts transitively on the roots $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ and that 5 is prime greatly limits the possible Galois extensions.

S_5 and transpose

Lemma 0.1.0.9. *If G contains a transpose then $G = S_5$.*

Proof. By a transpose we mean a permutation which interchanges two indices.

This isn't hard to show and we will leave it for you to try at home. □

Condition for Not Solvable By Radicals

Corollary 0.1.0.10. *Suppose our irreducible quintic has roots* $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ *and* K *is the splitting field. If* $F(\alpha_1, \alpha_2, \alpha_3) < K$ *then* $G(K/F) = S_5$.

Proof. For let $F' = F(\alpha_1, \alpha_2, \alpha_3)$. The only nontrivial permutation fixing $\alpha_1, \alpha_2, \alpha_3$ is the transposition (45). If $F' \neq K$ this permutation must be in $G(K/F')$. Thus $G(K/F)$ contains a transposition and is S_5 □

3 Real Roots Implies Quinitc Is Not Solvable

Corollary 0.1.0.11. *Let* $f(x)$ *be an irreducible quintic polynomial over* $\mathbb{Q}$ *with exactly 3 real roots. Then the Galois group is the symmetric group and hence the roots can't be expressed by radicals.*

Proof. Call the real roots $\alpha_1, \alpha_2, \alpha_3$. Then $F = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq \mathbb{R}$. But since α_4, α_5 aren't real we see that $F < K$ (where

K is the splitting field of f over $\mathbb{Q}$).

Hence $G(K/F) = S_5$ and f has no roots which can be expressed by radicals. □

Example Example:
$f(x) = x(x^2 - 4)(x^2 + 4) = x^5 - 16x$ has exactly 3 real roots. And we can add a small constant to it without changing the number of real roots. So $x^5 - 16x + 2$ has exactly 3 roots and is irreducible.

0.2 What To Do Next?

- Show that $V^{**} = V$.
- Latices and Boolean Algebras
- Valuation Rings and Completions.
- Modules
- More Advanced Galois Theory.
  - Infinite Galois Theory.

- Algebras

0.3 TODO

- Go through Lang's book on the same topics.