Mathematics 202 – Seminar in Algebra 2
An "Abstract" of Galois Theory, and
Solvability by Radicals
April 18, 2008

The following is a compendium of the "high points" in

- the logical development of Galois Theory for fields of characteristic zero, and
- the theorem that there exist quintic polynomials $f(x) \in \mathbb{Q}[x]$ whose roots cannot be expressed in terms of radicals.

These are summarized in outline form, the later ones with "telegraphic" proofs showing how they follow from the earlier ones. Since the results of this subject are highly interrelated, this summary may be more helpful in piecing together what implies what than the textbook presentation or the class notes, which include lots of examples, comments, etc. so are more discursive.

(0) Terminology and Notation: For a finite extension K over F:

  (a) An *F-automorphism* of K is a 1-1, onto, ring homomorphism $\sigma : K \to K$ such that $\sigma(a) = a$ for all $a \in F$.

  (b) $\mathrm{Gal}_F K$ is set of all F-automorphisms of K, which is a group under function composition, called the *Galois group of K over F.*

  (c) For any subgroup H of $\mathrm{Gal}_F K$, $E_H = \{a \in K : \sigma(a) = a, \text{ all } \sigma \in H\}$, called the *fixed field* of H. (It is a field, because it is closed under differences, products, and inverses in K.)

(1) (Consequence of the "Key Corollary" of Theorem 10.7): *Let $F(u)$ contain another root v of the minimal polynomial of u over F. Then there exists an F-automorphism σ of $F(u)$ with $\sigma(u) = v$.*

(2) (The induction step of the proof of the Primitive Element Theorem) *Let $[K : F] < \infty$ and let K be separable over F. α, β be elements of K (hence both algebraic over F). Then there exists a $\gamma \in K$ such that $F(\alpha, \beta) = F(\gamma)$.* (Idea of the proof: For well-chosen $c \in F$, we can find a γ of the form $\gamma = \alpha + c\beta$.)

(3) *If K is any finite-dimensional extension of F of characteristic zero, then $K = F(\gamma)$ for some $\gamma \in K$.*

(4) (Lemma for the proof of Theorems 11.7 and 11.8) *Let H be a subgroup of* $\mathrm{Gal}_F K$*, and let $E = E_H$. Then*

  (a) *If $\beta = \beta_1 \in K$, and $\{\beta_1, \ldots, \beta_t\}$ is the are the distinct images of β under the elements of H, then $f(x) = (x - \beta_1) \cdots (x - \beta_t)$ is in $E[x]$. (In fact $f(x)$ is irreducible in $E[x]$, though we did not say this in class).*

(**Proof:** The coefficients of g are the elementary symmetric polynomials in the β_i, hence are fixed by all permutations of the β_i, including those induced by H. Hence they are in the fixed field $E_H = E$. Let $p(x)$ be the minimal polynomial of β_1 over E. Then $p(\beta_1) = 0$, so $p(\sigma(\beta_1)) = 0$ for all $\sigma \in H$. Hence $f(x)$ divides $p(x)$ in $E[x]$. But this implies $f = p$; since p is irreducible, so is f.)

(b) $[K : E] = |H|$.

(**Proof:** Apply the proof of (a) to $\beta = u$ satisfying $K = E(u)$, using the Primitive Element Theorem. We get $\deg p(x) = [K : E] = |H|$.)

(5) (A Corollary of 4.) *If K is any finite extension of F, $|\mathrm{Gal}_F K|$ divides the degree $[K : F]$.* (This follows from 4 part b, by letting E be the fixed field of $\mathrm{Gal}_F K$: E is a subfield of K containing F, *possibly larger* than F. By 4, part b, $[K : E] = |\mathrm{Gal}_F K|$. But $[K : E][E : F] = [K : F]$, so $|\mathrm{Gal}_F K|$ divides $[K : F]$.)

(6) A *Galois* extension is a normal, separable, finite dimensional extension field K of F. If F and K have characteristic zero, this is equivalent to saying that K is the splitting field of some polynomial in $f(x) \in F[x]$ (Theorem 10.15).

(7) If K is a Galois extension of F and E is any intermediate field – $F \subseteq E \subseteq K$, then K is also a Galois extension of E (the polynomial $f \in F[x]$ is also in $E[x]$.)

(8) (The Fundamental Theorem of Galois Theory – Theorem 11.11) *Let K be a Galois extension of F.*

(a) *There is a one-to-one, inclusion reversing correspondence between the set of intermediate fields $F \subseteq E \subseteq K$ and the set of subgroups $\mathrm{Gal}_F K \supseteq H \supseteq \{id\}$. The correspondence is given by $E \mapsto \mathrm{Gal}_E K$ and $H \mapsto E_H$. Moreover, if $E = E_H$, then $[E : F] = [G : H]$, where $G = \mathrm{Gal}_F K$.*

(b) *The subfield E is normal over F if and only if its corresponding subgroup $H = \mathrm{Gal}_E K$ is a normal subgroup of $\mathrm{Gal}_F K$. Moreover, if E is Galois over F, then $\mathrm{Gal}_F E$ is isomorphic to the quotient group $\mathrm{Gal}_F K / \mathrm{Gal}_E K$.*

The proof of the direct implication is based on the observation that if E is normal over F, any element $\sigma \in \mathrm{Gal}_F K$ must satisfy $\sigma(E) \subseteq E$. Therefore we have a restriction mapping

$$\begin{aligned} \rho : \mathrm{Gal}_F K &\to \mathrm{Gal}_F E \\ \sigma &\mapsto \sigma|_E , \end{aligned}$$

which is a group homomorphism. It is onto because of the "Key Corollary" of Theorem 10.7 (see 10.14). The kernel is $\mathrm{Gal}_E K$, which is therefore a normal subgroup of $\mathrm{Gal}_F K$. The isomorphism

$$\mathrm{Gal}_F E \simeq \mathrm{Gal}_F K / \mathrm{Gal}_E K$$

is then a consequence of the First Isomorphism Theorem for groups.

(10) (Root Towers, I) An polynomial $f(x) \in F[x]$ with $F \subset \mathbf{C}$ is said to be *solvable by radicals* if there is a "root tower"

$$F = F_0 \subset F_1 \subset \cdots \subset F_n,$$

where $\alpha \in F_n$, and for each i, $F_i = F_{i-1}(\beta_i)$ where $\beta_i^{n_i} \in F_{i-1}$ for some integer n_i, and F_n contains the splitting field of $f(x)$.

(11) *Let F be a subfield of $\mathbf{C}$ containing the primitive pth root of 1, denoted ζ_p. Let a be an element of F which is not a pth power in F. Then the splitting field K of $x^p - a$ over F has degree p over F and $\mathrm{Gal}_F K$ is cyclic of order p.*

(**Proof**: Let α be any one root of $x^p - a$, and let $K = F(\alpha)$. The other roots of $x^p - a$ are $\zeta_p\alpha, \ldots, \zeta_p^{p-1}\alpha$. Since $\zeta_p \in F$, all these roots are in K, so K is the splitting field. By 6, K is Galois over F. If $\sigma \in \mathrm{Gal}_F K$ is not the identity, then $\sigma(\alpha) = \zeta_p^i\alpha$ for some i. It is easy to see that σ generates a subgroup of $\mathrm{Gal}_F K$ isomorphic to the cyclic group $\mathbb{Z}_p$. Since $K = F(\alpha)$, and α is a root of a polynomial of degree p over F, $[K : F] \leq p$. Hence $[K : F] = p = |\mathrm{Gal}_F K|$ and $\mathrm{Gal}_F K$ is cyclic as claimed.)

(12) *Let p be a prime and let ζ_p be as in 11. Then*

(a) *$\mathbb{Q}(\zeta_p)$ is Galois over $\mathbb{Q}$ and $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_p)$ is cyclic of order $p-1$.*

(**Proof:** The minimal polynomial of ζ_p over $\mathbb{Q}$ is $\phi_p(x) = x^{p-1} + \cdots + x + 1$. The roots of ϕ_p are just the powers ζ_p^i for $i = 1, \ldots, p-1$. Hence $\mathbb{Q}(\zeta_p)$ is the splitting field of ϕ_p over $\mathbb{Q}$, and we're done by 6. The Galois group $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_p)$ is isomorphic to the multiplicative group of the field $\mathbb{Z}/\langle p \rangle$, hence is cyclic of order $p-1$.)

(b) *If F is any subfield of $\mathbf{C}$, then $F(\zeta_p)$ is Galois over F and $\mathrm{Gal}_F F(\zeta_p)$ is cyclic.* (Follows since this Galois group is isomorphic to a subgroup of $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_p)$.)

(13) (Root Towers, II) *If $f(x) \in F[x]$ is solvable by radicals over F, then there is a root tower*

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

as in 10 above (for each i, $F_i = F_{i-1}(\beta_i)$ where $\beta_i^{n_i} \in F_{i-1}$ for some integer n_i) such that the splitting field of $f(x)$ is contained in F_n, F_n is Galois over F, and in addition, for each i, F_i is Galois over F_{i-1} with $\mathrm{Gal}_{F_{i-1}} F_i$ a cyclic group.

(**Proof:** Since α is expressible in terms of radicals, there is a root tower as in 10. Since $\sqrt[mn]{\beta} = \sqrt[m]{\sqrt[n]{\beta}}$, by inserting additional fields in the tower, we may assume that all the n_i are *prime*. Make a new root tower by first adjoining the primitive roots of unity ζ_{n_i} one at a time. Then adjoin the β_i. Each step of this new tower falls into the categories studied in 11 or 12. Hence we are done.)

(14) (Corollary of 13.) *Suppose we have a root tower as in 13. Then $G = \mathrm{Gal}_{\mathbb{Q}} F_n$ has a chain of subgroups of the form:*

$$\{id\} \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

where for all i, G_i is normal in G_{i+1}, and G_{i+1}/G_i is cyclic.

(**Proof:** Let $G_i = \mathrm{Gal}_{F_i} F_n$. By 7, F_n is Galois over each of the intermediate fields F_i. Hence by the last part of 9,

$$G_{i+1}/G_i \simeq \mathrm{Gal}_{F_{i+1}} F_n / \mathrm{Gal}_{F_i} F_n \simeq \mathrm{Gal}_{F_i} F_{i+1},$$

which is a cyclic group by hypothesis.)

(15) (Continuation) Since F_n is Galois over $\mathbb{Q}$ and $\alpha \in F_n$, the splitting field K of α is contained in F_n, it is Galois over $\mathbb{Q}$ by 6, and $\mathrm{Gal}_{\mathbb{Q}} K = \mathrm{Gal}_{\mathbb{Q}} F_n / \mathrm{Gal}_K F_n$. As a result, $H = \mathrm{Gal}_{\mathbb{Q}} K$ also has chain of subgroups of the form in 14:

$$\{e\} \subset H_1 \subset H_2 \subset \cdots \subset H_n = G$$

where for all i, H_i is normal in H_{i+1}, and H_{i+1}/H_i is cyclic. Groups with this property are said to be *solvable groups*.

(16) *The symmetric group S_5 is not solvable.*

(**Proof**: We try to construct a chain of subgroups as in 14 or 15. Each normal subgroup must be a union of conjugacy classes in S_n. By examining the sizes of the conjugacy classes, we see that the only possible nontrivial normal subgroup in S_5 is the alternating group A_5. But A_5 is simple (it has no normal subgroups except the identity subgroup and A_5). Hence the only chains of subgroups $\{e\} \subset H_1 \subset H_2 \subset \cdots \subset H_n = S_5$ with H_i normal in H_{i+1} for all i are are $\{()\} \subset A_5 \subset S_5$ and $\{()\} \subset S_5$. Since A_5 and S_5 are not cyclic, S_5 is not solvable.)

(17) (The "punch line") Let $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$. By the Eisenstein Criterion with $p = 5$, f is irreducible. Let K be the splitting field of f. The Galois group $\mathrm{Gal}_F K$ permutes the five roots of f, so it is isomorphic to a subgroup of S_5. By calculus, you can see that f has exactly three real roots and one pair of complex conjugate roots. If we number the two complex roots as α_1, α_2 and the three real roots as $\alpha_3, \alpha_4, \alpha_5$, complex conjugation induces an automorphism of the splitting field K of f over $\mathbb{Q}$ giving the permutation (12) on the roots. Moreover, since $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = 5$, 5 divides $[K : F] = |\mathrm{Gal}_F K|$. By the Sylow theorems, $\mathrm{Gal}_F K$ must contain an element of order 5. But the only permutations of the 5 roots that have order 5 are the 5-cycles. It is easy to see that if a subgroup of S_5 contains a 5-cycle and a 2-cycle, then it is all of S_5. But then by 16, $\mathrm{Gal}_F K$ is not a solvable group. So by the reasoning leading up to 15, the roots of f are not expressible by radicals(!)