21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

36- Monday April 23, 2012.

Lemma 36.1: Assume that E has characteristic 0, that F is a splitting field extension for $f \in E[x]$ over E, and that $Aut_E(F)$ is solvable. Then for all $n \geq 2$, there is a field extension $F(\xi)$ of F such that ξ is a primitive nth root of unity, and $Aut_{E(\xi)}\big(F(\xi)\big)$ is solvable.
Proof: One may assume that f is separable.[1] Let $F(\xi)$ be a splitting field extension for $x^n - 1$ over F, so that $F(\xi)$ is a splitting field extension for $(x^n - 1)\, f$ over E, and (since $(x^n - 1)\, f$ may be replaced by a separable polynomial) $F(\xi)$ is a Galois extension of E. One considers the mapping which sends $\sigma \in Aut_{E(\xi)}\big(F(\xi)\big)$ to $\sigma\,|_F$, which is an homomorphism from F into $F(\xi)$, and in order to show that it maps F into F, one notices that F is a normal extension of E, so that for $a \in F$ its monic irreducible polynomial $P_a \in E[x]$ splits over F, and since σ permutes the roots of P_a it maps F into F; since this also shows that σ^{-1} maps F into F, $\sigma|_F$ is an automorphism of F, which fixes $E(\xi) \cap F$, in particular it fixes E, so that $\sigma|_F \in Aut_E(F)$. Then $\sigma \mapsto \sigma\,|_F$ is an homomorphism, and the kernel of this homomorphism is the (normal) subgroup of $Aut_{E(\xi)}\big(F(\xi)\big)$ whose restriction to F is id_F, but since σ fixes $E(\xi)$ one has $\sigma(\xi) = \xi$, so that the kernel is reduced to the identity on $F(\xi)$, and the first isomorphism theorem shows then that $Aut_{E(\xi)}\big(F(\xi)\big)$ is isomorphic to a subgroup of $Aut_E(F)$, which is then solvable.

Definition 36.2: If F is a field and G is a finite subgroup of $Aut(F)$, then the *Noether equations* consist in finding $\{x_\sigma \in F^* \mid \sigma \in G\}$ satisfying $x_\sigma \sigma(x_\tau) = x_{\sigma\,\tau}$ for all $\sigma, \tau \in G$.

Lemma 36.3: Any solution of the Noether equations has the following form: there exists $a \in F^*$ such that $x_\sigma = a\,\big(\sigma(a)\big)^{-1}$ for all $\sigma \in G$.
Proof: Since the $\tau \in G$ are F-linearly independent, $\sum_{\tau \in G} x_\tau \tau \neq 0$, so that there exists $\alpha \in F^*$ with $\sum_{\tau \in G} x_\tau \tau(\alpha) = a \neq 0$. One deduces that $x_\sigma \sigma(a) = \sum_{\tau \in G} x_\sigma \sigma(x_\tau)\, \sigma\,\tau(\alpha)$, which is $\sum_{\tau \in G} x_{\sigma\,\tau}\, \sigma\,\tau(\alpha)$ by Noether's equations, which is $\sum_{g \in G} x_g\, g(\alpha) = a$ since G is a (finite) group.

Lemma 36.4: Let F be an extension field of E, and let G be a finite subgroup of $Aut_E(F)$. Then for any character ψ of G with values in E^*, there exists $a \in F^*$ such that $\psi(\sigma) = a\,\big(\sigma(a)\big)^{-1}$ for all $\sigma \in G$.
Proof: Since ψ satisfies $\psi(\sigma\,\tau) = \psi(\sigma)\,\psi(\tau)$ for all $\sigma, \tau \in G$, the Noether equations are satisfied if one defines $x_\sigma = \psi(\sigma) \in E^*$ for all $\sigma \in G$, since $\sigma(x_\tau) = x_\tau = \psi(\tau)$, because $x_\tau \in E^*$ and all elements of G fix E, so that $x_\sigma \sigma(x_\tau) = \psi(\sigma)\,\psi(\tau) = \psi(\sigma\,\tau) = x_{\sigma\,\tau}$ for all $\sigma, \tau \in G$. One then applies Lemma 36.3.

Lemma 36.5: Let F be a (finite) Galois extension of E, with Galois group $Aut_E(F)$ cyclic of order r, and assume that E contains a primitive rth root of 1. Then, there exists $a \in F$ such that $F = E(a)$ and $a^r \in E$, i.e. F is an extension obtained by adding a radical.
Proof: Let $\xi \in E^*$ be a primitive rth root of 1, and let σ be a generator of $Aut_E(F)$. For $G = Aut_E(F)$, one obtains a character ψ by taking $\psi(\sigma^i) = \xi^i$ for $i = 1, \ldots, r$, so that by Lemma 36.4 there exists $a \in F$ such that $\xi^i = a\,\big(\sigma^i(a)\big)^{-1}$, i.e. $\sigma^i(a) = a\,\xi^{-i}$ for $i = 1, \ldots, r$. This shows that the monic irreducible polynomial $P_a \in E[x]$ associated to a has the r roots $a\,\xi^{-i}$ for $i = 1, \ldots, r$ (which are distinct because ξ is a primitive rth root of 1), so that $[E(a) : E] = deg(P_a) \geq r$; on the other hand, since F is a Galois extension of E one has $[F : E] = |Aut_E(F)| = r$, which implies $[E(a) : E] \leq r$, so that $F = E(a)$ and $deg(P_a) = r$. Since it implies that $P_a = \prod_{i=1,\ldots,r}(x - a\,\xi^{-i})$, the constant coefficient is a^r times an element in E^*, and because it belongs to E, one deduces that $a^r \in E$.[2]

[1] One may assume that f is monic, and written as a product of monic irreducible polynomials; if one irreducible polynomial is repeated, one only keeps one copy, and this replaces f by $g \in E[x]$ without changing the splitting field extension; the derivative of an irreducible polynomial is not zero, since E has characteristic 0, hence each irreducible polynomial is separable, which makes g separable.

[2] It is a general fact that if $G = Aut_E(F)$ is finite, and $a \in F$, the element $b = \prod_{\tau \in G} \tau(a)$ is fixed by all elements of G because of the group property, i.e. $b \in Fix(G)$, so that if F is a Galois extension of E one deduces that $b \in E$.

Lemma 36.6: Let F be a finite Galois extension of E, and assume that the Galois group $Aut_E(F)$ is isomorphic to $C_1 \times \cdots \times C_k$, where C_i is cyclic of order r_i. Suppose that E has a primitive rth root of 1, where r is the *lcm* (least common multiple) of the r_i, $i = 1, \ldots, k$. Then, $F = E(a_1, \ldots, a_k)$, where $a_i \in F$ with $a_i^{r_i} \in E$, $i = 1, \ldots, k$, i.e. F is an extension obtained by adding k radicals.
Proof: One chooses $\sigma_i \in Aut_E(F)$, $i = 1, \ldots, k$, so that every element of $Aut_E(F)$ has the form $\sigma_1^{m_1} \cdots \sigma_k^{m_k}$ with $0 \le m_i < r_i$ for $i = 1, \ldots, k$. Let N_i, $i = 1, \ldots, k$, be the subgroup generated by the σ_j for $j \ne i$, so that $Aut_E(F)/N_i$ is cyclic of order r_i and is generated by the coset $\sigma_i N_i$. Then, let $E_i = Fix(N_i)$, so that by the fundamental theorem of Galois theory $Aut_{E_i}(F) = N_i$, E_i is a Galois extension of E, and $Aut_E(E_i) \simeq Aut_E(F)/Aut_{E_i}(F) = Aut_E(F)/N_i$, which is cyclic of order r_i, and is then generated by the restriction of σ_i to E_i. Since r_i divides r, and E has a primitive rth root of unity ρ, a power of ρ is a primitive r_ith root of unity, and by Lemma 36.5 $E_i = E(a_i)$ for some $a_i \in F$ with $a_i^{r_i} \in E$.

If $\tau \in Aut_{E(a_1,\ldots,a_k)}(F)$ then $\tau(a_i) = a_i$ since $a_i \in E(a_1, \ldots, a_k)$, i.e. $\tau \in N_i$, but the intersection of all the N_i is $\{e\}$, i.e. $\tau = id_F$, and by the Galois correspondence $Aut_{E(a_1,\ldots,a_k)}(F) = \{id_F\}$ implies $E(a_1, \ldots, a_k) = Fix(\{id_F\}) = F$.

Remark 36.7: The definition of a group G being solvable is that there is a subnormal series, i.e. $G_0 = G \triangleleft G_1 \triangleleft \cdots \triangleleft G_k = G$, such that the quotient G_{i+1}/G_i is Abelian for $i = 0, \ldots, k-1$.

A normal series must satisfy the supplementary property $G_i \triangleleft G$ for $i = 1, \ldots, k-1$ (since it is automatic for $i = 0$ and $i = k$). If G is solvable, there is indeed a normal series by taking $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for $i \ge 0$, and then $G^{(k)} = \{e\}$, where $[H, H]$ denotes the subgroup generated by $h_1 h_2 h_1^{-1} h_2^{-1}$ for $h_1, h_2 \in H$ (subgroup of G), and $[H, H]$ is a characteristic subgroup of H.

Lemma 36.8: Assume that E has characteristic 0, that F is a splitting field extension for $f \in E[x]$ over E, and that $Aut_E(F)$ is solvable. Then f is solvable by radicals.
Proof: Since F is a Galois extension of E (because separability of f is not necessary in characteristic 0), one has $n = |Aut_E(F)| = [F\!:\!E]$. One then adds a primitive nth root of unity ξ by using Lemma 36.1, and one finds that $Aut_{E(\xi)}\big(F(\xi)\big)$ is a (necessarily solvable) subgroup of $Aut_E(F)$ (by sending σ to $\sigma\big|_F$), so that $\big|Aut_{E(\xi)}\big(F(\xi)\big)\big| = m$ divides n; since $F(\xi)$ is a Galois extension of E, hence of $E(\xi)$ by the fundamental theorem of Galois theory, one has $[F(\xi)\!:\!E(\xi)] = \big|Aut_{E(\xi)}\big(F(\xi)\big)\big| = m$, and $\zeta = \xi^{n/m}$ is a primitive mth root of unity in $E(\xi)$.

Renaming $E(\xi)$, $F(\xi)$, m, and ξ, one may then assume that $[F\!:\!E] = n$ and that E contains a primitive nth root of unity ξ.

Let $G = Aut_E(F)$, and let k be such that $G^{(k)} = \{e\}$. Let $E_i = Fix(G^{(i)})$, so that $Aut_{E_i}(F) = G^{(i)}$ and F is a Galois extension of E_i, and $E_0 = E \subset E_1 \subset \ldots \subset E_k = F$. Since $G^{(i)}$ is a normal subgroup of G, E_i is a Galois extension of E by the fundamental theorem of Galois theory, and similarly, since $G^{(i+1)}$ is a normal subgroup of $G^{(i)}$, E_{i+1} is a Galois extension of E_i, and $Aut_{E_i}(E_{i+1}) \simeq Aut_{E_i}(F)/Aut_{E_{i+1}}(F) = G^{(i)}/G^{(i+1)}$, which is Abelian; since $r = [E_{i+1}\!:\!E_i]$ divides n, $\xi^{n/r}$ is a primitive rth root of unity and E_{i+1} is a radical extension of E_i (Lemma 36.1), hence F is an extension by radicals of E and f is solvable by radicals.