Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

35- Wednesday April 18, 2012.

Lemma 35.1: If E is a field and $f \in E[x]$ has no common factor with f', i.e. the *gcd* (greatest common divisor) of f and f' is 1, then f is separable.
Proof: One has $f = P_1 \cdots P_k$, with $P_1, \ldots, P_k$ irreducible in $E[x]$, and by Definition 33.5 f is separable if and only if P_i is separable for $i = 1, \ldots, k$. If P_1 is not separable (for example), then by Definition 33.2 there exists a field extension F of E where P_1 has a repeated root, i.e. $P = (x-a)^2 Q$ for some $a \in F$ and $Q \in F[x]$; then $f = (x-a)^2 R$ with $R = Q\, P_2 \cdots P_k \in F[x]$, and $f' = (x-a)\,\big(2R + (x-a)\,R'\big)$, so that f and f' have a common factor $x-a$ in $F[x]$, and the *gcd* of f and f' in $F[x]$ has degree ≥ 1, but the Euclidean algorithm for the search of the *gcd* in $F[x]$ gives a non-zero constant, since it leads to the same computations than the Euclidean algorithm for the search of the *gcd* in $E[x]$.

Definition 35.2: An *extension by radicals* of a field E is a field extension F such that there exist $E_0 = E \subset E_1 \subset \ldots \subset E_k = F$, where for $i = 0, \ldots, k-1$ one has $E_{i+1} = E_i(\alpha_i)$ with $\alpha_i^{n_i} = a_i \in E_i$ (and $\alpha_i \in E_{i+1} \setminus E_i$, $n_i \geq 2$).

A polynomial $f \in E[x]$ is *solvable by radicals* if (and only if) there exists a splitting field extension F_1 for f over E, and a field extension F_2 of F_1 such that F_2 is an extension by radicals of E.

Definition 35.3: If E is a field, a *primitive* dth root of unity is an element $a \in E^*$ which generates a (cyclic) group of order d consisting of the d roots of $x^d - 1 = 0$.[1]

Lemma 35.4: Let E be a field whose characteristic is either 0 or a prime p not dividing n, and let F be a splitting field extension for $f = x^n - 1$ over E. Then, F is a Galois extension of E, there exists a primitive nth root ξ of 1 in F, and the Galois group $Aut_E(F)$ is Abelian.
Proof: $f' = n\,x^{n-1}$, and since n is invertible,[2] the *gcd* of f and f' is 1, and f is then separable by Lemma 35.1, so that F is a Galois extension of E. f splits in F with n distinct roots and one of them is a primitive root, since the nth roots of unity in F form a multiplicative subgroup of F^*, which is cyclic.

If ξ is a primitive root of unity in F, and $\sigma \in Aut_E(F)$, the value of $\sigma(\xi)$ characterizes σ, since $F = E(\xi)$, and there exists j with $\sigma(\xi) = \xi^j$; if $\tau \in Aut_E(F)$ with $\tau(\xi) = \xi^k$, then $\sigma \circ \tau(\xi) = \tau \circ \sigma(\xi) = \xi^{j\,k}$, so that $\sigma\,\tau = \tau\,\sigma$.

Lemma 35.5: Let E be a field whose characteristic is either 0 or a prime p not dividing n, and let F be a splitting field extension for $f = x^n - a$ over E, with $a \in E^*$. Then, f has n distinct roots in F, F is a Galois extension of E, and $F = E(\alpha, \xi)$, with $\alpha^n = a$, and ξ is a primitive nth root of 1 in F.

Moreover, the Galois group $G = Aut_E(F)$ is solvable.
Proof: As for Lemma 35.4, $f' = n\,x^{n-1}$, and the *gcd* of f and f' is 1, so that f is separable by Lemma 35.1, and F is a Galois extension of E. Since the roots are $\alpha, \alpha\,\xi, \ldots, \alpha\,\xi^{n-1}$, one has $F = E(\alpha, \alpha\,\xi, \ldots, \alpha\,\xi^{n-1}) = E(\alpha, \xi)$.

Since $E(\xi)$ is a Galois extension of E by Lemma 35.4, $N = Aut_{E(\xi)}(F)$ is a normal subgroup of G and $Aut_E\big(E(\xi)\big) \simeq G/N$ by the fundamental theorem of Galois theory. Since $Aut_E\big(E(\xi)\big)$ is Abelian by Lemma 35.4, G/N is Abelian, hence solvable.[3]

Since F is generated by α over $E(\xi)$, any element $\sigma \in N$ is determined by $\sigma(\alpha)$, which is a root of $x^n - a$, and then has the form $\alpha\,\xi^j$ for some j; for another element $\tau \in N$ one has $\tau(\alpha) = \alpha\,\xi^k$, and then, since $\sigma(\xi) = \tau(\xi) = \xi$ (by definition of N), one has $\tau\,\big(\sigma(\alpha)\big) = \tau(\alpha\,\xi^j) = \tau(\alpha)\,\tau(\xi)^j = \alpha\,\xi^k\,\xi^j = \alpha\,\xi^{j+k}$, which is then also $\sigma\,\big(\tau(\alpha)\big)$, implying that $\sigma \circ \tau$ and $\tau \circ \sigma$ coincide, so that N is Abelian, hence solvable. Since N and G/N are solvable, G is solvable.

[1] Once a primitive dth root of unity a exists, then a^k is another primitive dth root of unity if and only if $(k,d) = 1$, so that there are $\varphi(d)$ primitive dth roots of unity, by definition of the Euler φ function.

[2] n is considered as an element of the prime subfield, isomorphic to $\mathbb{Q}$ if the characteristic of E is 0, and isomorphic to $\mathbb{Z}_p$ if the characteristic of E is p.

[3] Any Abelian group H is solvable, by using the normal series $H_0 = \{e\}$, $H_1 = H$.

Definition 35.6: A *Kummer extension* of a field E is a splitting field extension for a polynomial $f \in E[x]$ having the form $\prod_{i=1}^{k}(x^{n_i} - a_i)$,[4] with (distinct) $a_i \in E^*$, $i = 1, \ldots, k$.

Lemma 35.7: If E has characteristic 0,[5] and if F is a Kummer extension of E, then F is a Galois extension of E, and the Galois group $Aut_E(F)$ is solvable.
Proof: By induction on k. The case $k = 1$ is Lemma 35.5. Assume that the result is proved for up to $k-1$ factors, so that for $g = \prod_{i=1}^{k-1}(x^{n_i} - a_i)$ a field extension F_{k-1} for g over E is a Galois extension with $H = Aut_E(F_{k-1})$ solvable. Since F_{k-1} is a Galois extension of E, it is the splitting field extension for a separable polynomial $\widetilde{g} \in E[x]$ over E. Let F_k be a splitting field extension for $h = x^{n_k} - a_k$ over F_{k-1}, which is a Galois extension with $N = Aut_{F_{k-1}}(F_k)$ solvable by Lemma 35.5. Let $d \in E[x]$ be the *gcd* of $\widetilde{g}$ and h, and $h = d\,\widetilde{h}$, then F_k is a splitting field extension for $\widetilde{g}\,\widetilde{h}$ over E;[6] moreover $\widetilde{g}\,\widetilde{h} \in E[x]$ is separable, since both $\widetilde{g}$ and $\widetilde{h}$ are separable,[7] and their *gcd* is 1, hence F_k is a Galois extension of E. Then, by the fundamental theorem of Galois theory, N is a normal subgroup of $G = Aut_E(F_k)$ and $H \simeq G/N$, so that G is solvable (since N and G/N are solvable).

Lemma 35.8: If E has characteristic 0, if F is an extension by radicals of E, there exists an extension $\overline{F}$ of F such that $\overline{F}$ is a Galois extension of E with a solvable Galois group $Aut_E(\overline{F})$.
Proof: By Definition 35.2, there exist $E_0 = E \subset E_1 \subset \ldots \subset E_k = F$, and $E_{i+1} = E_i(\alpha_i)$ with $\alpha_i \in E_{i+1}$ and $\alpha_i^{n_i} = a_i \in E_i$, $i = 0, \ldots, k-1$. If $k = 0$, there is nothing to prove.

If $k \geq 1$, one uses an induction on k, so one finds an extension $\overline{E_{k-1}}$ of E_{k-1} which is a Galois extension of E with a solvable Galois group $G_{k-1} = Aut_E(\overline{E_{k-1}})$. One chooses $g \in E[x]$, separable over E, such that $\overline{E_{k-1}}$ is a splitting field extension for g over E. Then, one defines $h \in \overline{E_{k-1}}[x]$ by $h = \prod_{\sigma \in G_{k-1}}\big(x^{n_{k-1}} - \sigma(a_{k-1})\big)$, and one wants to show that $h \in E[x]$: for an arbitrary $\tau \in G_{k-1}$, using the fact that G_{k-1} is a group, τ permutes the factors of h, so that $\tau(h) = h$, i.e. each coefficient of h is fixed by τ, hence belongs to $Fix(G_{k-1})$, which is E by definition of G_{k-1} being a Galois extension of E.

One lets $\overline{E_k}$ be a splitting field extension for h over $\overline{E_{k-1}}$, so that $\overline{E_k}$ is a splitting field extension for $g\,h$ over E (hence the importance of knowing that $h \in E[x]$), and as in Lemma 35.7 one may replace $g\,h$ by a separable polynomial, showing that $\overline{E_k}$ is a Galois extension of E. Let $P \in E_{k-1}[x]$ be the monic irreducible polynomial associated to $\alpha_{k-1} \in E_k$; then, P divides $x^{n_{k-1}} - a_{k-1}$, so that it divides h. Choosing any $\beta \in \overline{E_k}$ such that $P(\beta) = 0$, there is an isomorphism from $E_k = E_{k-1}(\alpha_{k-1})$ onto $E_{k-1}(\beta)$ fixing E_{k-1}, so that, without loss of generality, one may assume that $E_k \subset \overline{E_k}$. By Definition 35.6 $\overline{E_k}$ is a Kummer extension of $\overline{E_{k-1}}$, so that by Lemma 35.7 $H = Aut_{\overline{E_{k-1}}}(\overline{E_k})$ is solvable; $Aut_E(\overline{E_{k-1}})$ is solvable by the induction hypothesis. Since $\overline{E_{k-1}}$ and $\overline{E_k}$ are Galois extensions of E, the fundamental theorem of Galois theory implies that H is a normal subgroup of $G = Aut_E(\overline{E_k})$ and $Aut_E(\overline{E_{k-1}})$ is isomorphic to G/H, so that H and G/H being solvable, G is solvable.

Lemma 35.9: If E has characteristic 0, if $f \in E[x]$ is solvable by radicals (Definition 35.2), and if F is a splitting field extension for f over E, then $Aut_E(F)$ is a solvable group.
Proof: Let F_1 be an extension of F such that F_1 is an extension by radicals of E, and let $\overline{F_1}$ be associated as in Lemma 35.8. Since one may assume that f is separable,[8] F is a Galois extension of E, and by the fundamental theorem of Galois theory, $Aut_E(F)$ is isomorphic to the quotient $Aut_E(\overline{F_1})/Aut_F(\overline{F_1})$, and a quotient of a solvable group (by a normal subgroup) is solvable.

---

[4] Ernst Eduard Kummer, German mathematician, 1810–1893. He worked in Berlin, Germany.

[5] The proof shows that the result is also true if E has characteristic p, and if none of the n_i is a multiple of p.

[6] The smallest field containing E and the roots of $\widetilde{g}$ is F_{k-1}, and the smallest field containing F_{k-1} and the roots of $\widetilde{h}$ contains the roots of $d\,\widetilde{h} = h$ (since d divides $\widetilde{g}$), and is F_k.

[7] Since the *gcd* of h and h' is 1, h is separable, and from Definition 33.5 a factor of a separable polynomial is separable.

[8] One may assume that f is monic, and write it as a product of monic irreducible polynomials; if one irreducible polynomial is repeated, one only keeps one copy, 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, so that one may assume that f is separable.

Definition 35.10: For $f \in E[x]$, the *Galois group of* f over E is the Galois group of a splitting field extension for f over E.

Lemma 35.11: If $\sigma \in S_5$ is a cyclic permutation, and $\tau \in S_5$ is a transposition, then σ and τ generate S_5.
Proof: One may label the 5 elements so that $\sigma = (12345)$ and for the case where τ transposes two adjacent elements one may consider that $\tau = (12)$, and for the case where τ transposes two non-adjacent elements one may consider that $\tau = (13)$.

In the first case, $\sigma\,(12)\,\sigma^{-1} = (23)$, and repeating the conjugation by σ gives the transpositions (34), (45), and (51); then $(12)\,\sigma\,(12) = (21345)$, and $(21345)\,(23) = (13)\,(245)$ whose power 3 is (13), which by conjugation by σ gives (24), (35), (41), and (52), so that one has generated all transpositions, hence the subgroup generated by σ and (12) is S_5.

In the second case, $\sigma^2 = (13524)$ so that (13) transposes two adjacent elements of the cycle of σ^2 and the first case applies.

Lemma 35.12: If $f \in \mathbb{Q}[x]$ is irreducible of degree 5, and has 3 real roots and 2 non-real roots, then the Galois group of f over $\mathbb{Q}$ is isomorphic to S_5, and f cannot be solved by radicals.
Proof: Let F be the subfield of $\mathbb{C}$ generated by the roots of f, which is a splitting field extension for f over $\mathbb{Q}$, hence a Galois extension of $\mathbb{Q}$, since f is separable, so that $|Aut_{\mathbb{Q}}(F)| = [F:\mathbb{Q}]$, which is $[F:\mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha):\mathbb{Q}]$ for any root α of f, i.e a multiple of $5 = [\mathbb{Q}(\alpha):\mathbb{Q}]$. By Cauchy's theorem, $Aut_{\mathbb{Q}}(F)$ contains an element σ of order 5, and it contains the complex conjugation τ; the action of σ on the roots of f corresponds to a cyclic permutation, while τ corresponds to a transposition (since it exchanges the two non-real roots), and by Lemma 35.11 they generate S_5, so that all permutations are obtained and $Aut_{\mathbb{Q}}(F) \simeq S_5$. Since S_5 is not solvable, Lemma 35.9 shows that f cannot be solved by radicals.

Example 35.13: $x^5 - 80x + a$ with $a \in \mathbb{Z}$, $|a| < 128$ and a either even but not a multiple of 4, or a multiple of 5 but not a multiple of 25, is not solvable by radicals.
Proof: By applying Eisenstein criterion to $f = x^5 - 80x + a$, it is irreducible if either a is a multiple of 2 but not of 4 by taking $p = 2$, or if a is a multiple of 5 but not of 25 by taking $p = 5$.[9] Since $f' = 5(x^4 - 16)$ has roots ± 2, f has 3 real roots if and only if $f(-2) > 0 > f(2)$, i.e. $|a| < 128$, and Lemma 35.12 applies.

Example 35.14: More generally $P = A\,x^5 + B\,x + C$ with $A, B, C \in \mathbb{Z}$ and $A > 0, B < 0, C \neq 0$ has 3 real roots and 2 non-real roots if and only if $P(-y) > 0 > P(y)$ with $y \in \mathbb{R}_+$ defined by $5A\,y^4 + B = 0$, which means $3125A\,C^4 < -256B^5$, so that if P is irreducible over $\mathbb{Q}$ it is not solvable by radicals. Eisenstein criterion applies (and proves that P is irreducible over $\mathbb{Q}$) if there exists a prime p such that p does not divide A, p divides B and C, and p^2 does not divide C (or if p does not divide C, p divides A and B, and p^2 does not divide A).

Remark 35.15: It will be shown later that if E has characteristic 0 and F is a splitting field extension for $f \in E[x]$ over E with the Galois group $Aut_E(F)$ being solvable, then f is solvable by radicals.

[9] Notice that $|a| \in \{20, 40, 60, 80, 120\}$ gives an irreducible polynomial by Eisenstein criterion with $p = 5$, while Eisenstein criterion with $p = 2$ does not apply.