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

38- Friday April 27, 2012.

Lemma 38.1: If $\delta = \prod_{i<j}(t_i - t_j)$, then the *discriminant* $\Delta = \delta^2$ is a symmetric polynomial, i.e. $\Delta \in k$. If E has characteristic $\neq 2$, $\delta \notin k$, and $\ell = k(\delta)$ is a Galois extension of k with $[\ell : k] = 2$, and $Aut_k(\ell) = A_n$.
Proof: K is a Galois extension of k, with Galois group the symmetric group S_n by Lemma 37.8; the alternating group A_n is a normal subgroup of S_n (kernel of the signature homomorphism), so that $\ell = Fix(A_n)$ is an intermediate field which is a Galois extension of k with $[\ell : k] = 2$ by the fundamental theorem of Galois theory. By any transposition τ, δ is changed into $-\delta$, so that $\Delta = \delta^2$ is fixed by all transpositions, hence by all permutations, hence $\Delta \in Fix(S_n) = k$. If the characteristic of E is $\neq 2$, then $-1 \neq +1$, so that $\delta \notin k$; also, for any permutation σ, δ is changed into $sign(\sigma)\,\delta$, so that δ is fixed by all elements of A_n, and then belongs to ℓ by definition, but since $k(\delta) \subset \ell$ and $[k(\delta) : k] \geq 2$, one must have $k(\delta) = \ell$.

Remark 38.2: Here is the solution of the general cubic equation, assuming that E has characteristic $\neq 2$, and that it contains a primitive third root of unity ξ, which satisfies $1 + \xi + \xi^2 = 0$.

Since $Aut_k(\ell) = A_3 \simeq \mathbb{Z}_3$, it is cyclic, generated by the cyclic permutation (123); there are three characters, obtained in mapping (123) to $1, \xi, \xi^2$ respectively. Let $a_0 = t_1 + t_2 + t_3 = s_1 \in k, a_1 = t_1 + \xi\, t_2 + \xi^2 t_3 \in K, a_2 = t_1 + \xi^2 t_2 + \xi\, t_3 \in K$. If one finds a_1 and a_2, then t_1, t_2, t_3 are given by solving a linear system, with a Vandermonde matrix.

Since (123) maps t_1 to t_2 to t_3 to t_1, it maps a_1 to $t_2 + \xi\, t_3 + \xi^2 t_1$, which is $\xi^2 a_1$, so that a_1^3 is mapped to itself, hence it is fixed by A_3, and one deduces that $a_1^3 \in \ell$; similarly, $a_2^3 \in \ell$. Then, using $1 + \xi + \xi^2 = 0$, one has $a_1 a_2 = t_1^2 + t_2^2 + t_3^2 - (t_1 t_2 + t_1 t_3 + t_2 t_3) = s_1^2 - 3 s_2 \in k$; there are three choices for the cube root of a_1^3, and then a_2 is determined.

One has $\delta = (t_1 - t_2)\,(t_1 - t_3)\,(t_2 - t_3) = [t_1^2 t_2 + t_2^2 t_3 + t_3^2 t_1] - [t_1^2 t_3 + t_2^2 t_1 + t_3^2 t_2]$, and developing $a_1^3 = (t_1 + \xi\, t_2 + \xi^2 t_3)^3$ gives 27 terms, $(t_1^3 + t_2^3 + t_3^3) + 3\xi\,[t_1^2 t_2 + t_2^2 t_3 + t_3^2 t_1] + 3\xi^2 [t_1^2 t_3 + t_2^2 t_1 + t_3^2 t_2] + 6 t_1 t_2 t_3$, and one deduces that $a_1^3 + \frac{3}{2}\,(\xi^2 - \xi)\,\delta = P + \frac{3}{2}\,(\xi^2 + \xi)\,Q + 6R$, with the symmetric polynomials $P = t_1^3 + t_2^3 + t_3^3$, $Q = t_1^2 t_2 + t_2^2 t_3 + t_3^2 t_1 + t_1^2 t_3 + t_2^2 t_1 + t_3^2 t_2$, $R = t_1 t_2 t_3$; changing ξ into ξ^2 gives then the same value for $a_2^3 - \frac{3}{2}\,(\xi^2 - \xi)\,\delta$ (and $(\xi^2 - \xi)^2 = \xi + \xi^2 - 2 = -3$). It does not matter which root of Δ one takes, since one uses both $-\delta$ and δ.

For computing P, Q, R, one uses $s_1^3 = (t_1 + t_2 + t_3)^3 = P + 3Q + 6R$, $s_1 s_2 = (t_1 + t_2 + t_3)\,(t_1 t_2 + t_1 t_3 + t_2 t_3) = Q + 3R$, and $R = s_3$, so that $Q = s_1 s_2 - 3 s_3$, and $P = s_1^3 - 3 s_1 s_2 + 3 s_3$.

Lemma 38.3: A field E is *algebraically closed* if and only if one of the following equivalent conditions holds
a) every $P \in E[x]$ splits over E,
b) if F is an algebraic extension of E, then $F = E$,
c) if F is a finite extension of E, then $F = E$.
Proof: a) implies b), since each $a \in F$ has a monic irreducible polynomial $P_a \in E[x]$, which then splits over E, so that irreducibility implies $deg(P_a) = 1$ and $a \in E$. b) implies c) since a finite extension is automatically an algebraic extension. c) implies a) since a splitting field extension for P over E is a finite extension of E, and because it is then E, it implies that P splits over E.

Definition 38.4: A field F is an *algebraic closure* of a field E if and only if F is an algebraic extension of E and F is algebraically closed (so that if K is an intermediate field, F is an algebraic closure of K).

Lemma 38.5: If F is an algebraic extension of E such that every $P \in E[x]$ splits over F, then F is algebraically closed, so that F is an algebraic closure of E.
Proof: Assume that $Q \in F[x]$ does not split over F, so that Q has a root $\alpha \notin F$, belonging to $F(\alpha)$; then α being algebraic over F and F being an algebraic extension of E, α is algebraic over E, and has a monic irreducible polynomial $P \in E[x]$, which by hypothesis splits over F, so that $\alpha \in F$, a contradiction.

Lemma 38.6: For every field E, there exists an algebraically closed field K containing E.[1]

[1] Up to now one has considered algebraic elements over E inside an extension F, but here one must construct a large extension F.

Proof: (E. Artin) Let Z be the set of all non-constant monic polynomials in $E[x]$, and for $z \in Z$ let $P_z \in E[x]$ be the corresponding polynomial in $E[x]$. One considers the ring $R = E[Z]$ of all the polynomials in (a finite number of) variables of Z with coefficients in E, and one lets I be the ideal generated by all the polynomials $P_z(z)$. One first shows that one cannot find distinct $z_1, \ldots, z_m \in Z$ and polynomials $r_1, \ldots, r_m \in E[Z]$ such that $\sum_{i=1}^{m} r_i P_{z_i}(z_i) = 1$, so that I is a proper ideal, since it does not contain 1; let $z_{m+1}, \ldots, z_n$ be the other remaining variables in Z occurring in the polynomials $r_1, \ldots, r_m$; let F be a field extension of E where P_{z_i} has a root α_i for $i = 1, \ldots, m$, then the identity between polynomials is still valid in F, and by giving the values $\alpha_1, \ldots, \alpha_m$ to $z_1, \ldots, z_m$, and whatever values one likes to $z_{m+1}, \ldots, z_n$ one deduces that $0 = 1$, a contradiction. By Zorn's lemma, I is included in a maximal (proper) ideal M and $K_1 = R/M$ is a field containing an isomorphic copy of E, and such that each monic polynomial in $E[x]$ is one P_z, which has a root, the class of z, since $P_z(z) \in I \subset M$.

Performing the same construction with K_1 instead of E, one constructs a field K_2 containing K_1 in which every non-constant polynomial from $K_1[x]$ has a root. Repeating the construction gives $E = K_0 \subset K_1 \subset \ldots \subset K_k \subset \ldots$, where every non-constant polynomial from $K_k[x]$ has a root in K_{k+1}, and $K_\infty = \bigcup_{k \geq 0} K_k$ is algebraically closed. Indeed, $P \in K_\infty[x]$ has all its coefficients in some K_k, and so it has a root $a \in K_{k+1} \subset K_\infty$, and $P = (x - a)\, Q$ with $Q \in K_{k+1}[x]$ and a root in K_{k+2}, and so on.

Lemma 38.7: If E is a field, then it has an algebraic closure F. If F_1 and F_2 are two algebraic closures of E, there exists an isomorphism σ of F_1 onto F_2 such that $\sigma|_E = id_E$.
Proof: By Lemma 38.6, E is included in an algebraically closed field K, and one defines then F as the field generated in K by all the roots of polynomials $P \in E[x]$, and that includes E, so that F is an algebraic extension of E. By Lemma 38.5, F is algebraically closed, hence it is an algebraic closure of E.

For the existence of the isomorphism σ, one uses an argument of maximality, for intermediate fields, i.e. $E \subset K_1 \subset F_1$, $E \subset K_2 \subset F_2$, with an isomorphism τ between K_1 and K_2 extending id_E, ordered by inclusion and extension, and the hypotheses of Zorn's lemma apply; if a maximal element is not $(K_1, K_2) = (F_1, F_2)$, then there is a polynomial $P \in E[x]$ which does not split over K_1 (and the corresponding polynomial does not split over K_2), and one extends the isomorphism to the splitting field extensions.