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

37- Wednesday April 25, 2012.

Definition 37.1: For a field E, the symmetric group S_n acts on the polynomial ring $E[t_1, \dots, t_n]$ by $\sigma\, P = Q$ meaning $Q(t_1, \dots, t_n) = P(t_{\sigma(1)}, \dots, t_{\sigma(n)})$. $P \in E[t_1, \dots, t_n]$ is *symmetric* if and only if $\sigma\, P = P$ for all $\sigma \in S_n$. The *elementary* symmetric polynomials $s_1, \dots, s_n$ are defined by $(x + t_1) \cdots (x + t_n) = x^n + s_1 x^{n-1} + s_2 x^{n-2} + \dots + s_n$, i.e. $s_i = \sum_{a \subset \{1,\dots,n\}, |a|=i} \prod_{j \in a} t_j$ for $i = 1, \dots, n$.

Remark 37.2: Since $\left(\sum_i t_i\right)^2 = \sum_i t_i^2 + 2 \sum_{i<j} t_i t_j$, one deduces that $\sigma_2 = \sum_i t_i^2$ can be expressed in terms of the elementary symmetric polynomials, as $s_1^2 - 2s_1$; more generally, NEWTON derived formulas for computing $\sigma_k = \sum_i t_i^k$ for $k \geq 3$ (in terms of the elementary symmetric polynomials), but it was WARING who proved in 1770 that all rational symmetric functions of the roots of an equation can be expressed as rational functions of the coefficients.[1]

Definition 37.3: For $P \in E[x]$, the *discriminant* of P is $\Delta = \prod_{i<j} (t_i - t_j)^2$, where $t_1, \dots, t_n$ (for $degree(P) = n$) are the roots of P in a splitting field extension F for P over E, although it is an element of E (by Lemma 37.12).

Lemma 37.4: If a monic polynomial $P \in E[x]$ of degree n has roots $t_1, \dots, t_n$, then its discriminant is equal to $\Delta = (-1)^{\binom{n}{2}} \prod_i P'(t_i) \in E$ (by Lemma 37.12).
Proof: Writing $P = (x - t_i)\, Q_i$ (with $Q_i = \prod_{j \neq i} (x - t_j)$), one has $P' = Q_i + (x - t_i)\, Q_i'$, so that $P'(t_i) = Q(t_i) = \prod_{j \neq i} (t_i - t_j)$. For each pair $i \neq j$, the product $\prod_i P'(t_i)$ contains exactly one factor $t_i - t_j$ and one factor $t_j - t_i$, so that it $(-1)^m$ times the discriminant where m is the number of pairs.[2]

Example 37.5: If $P = x^2 + a\, x + b$, then $\Delta = a^2 - 4b$. Indeed, since $P' = 2x + a$, the discriminant is $-P'(t_1)\, P'(t_2) = -(2t_1 + a)\, (2t_2 + a) = -4t_1 t_2 - 2a\, (t_1 + t_2) - a^2$, and because $t_1 + t_2 = -a$ and $t_1 t_2 = b$, one has $\Delta = -4b + 2a^2 - a^2 = a^2 - 4b$.

Notice that the formula $\frac{-a \pm \sqrt{a^2 - 4b}}{2}$ for the roots is not valid for a field of characteristic 2.

Example 37.6: If $P = x^3 + p\, x + q$, then $\Delta = -(4p^3 + 27q^2)$. Indeed, since $P' = 3x^2 + p$, the discriminant is $-(3t_1^2 + p)\, (3t_2^2 + p)\, (3t_3^2 + p)$; one has $t_1^2 + t_2^2 + t_3^2 = (t_1 + t_2 + t_3)^2 - 2(t_1 t_2 + t_1 t_3 + t_2 t_3) = s_1^2 - 2s_2 = -2p$, $t_1^2 t_2^2 + t_1^2 t_3^2 + t_2^2 t_3^2 = (t_1 t_2 + t_1 t_3 + t_2 t_3)^2 - 2t_1 t_2 t_3 (t_1 + t_2 + t_3) = s_2^2 - 2s_1 s_3 = p^2$, and $t_1^2 t_2^2 t_3^2 = s_3^2 = q^2$, so that $\Delta = -27q^2 - 9p\, p^2 - 3p^2(-2p) - p^3 = -(4p^3 + 27q^2)$.

Example 37.7: If $P = x^3 + a\, x^2 + b\, x + c$, the discriminant is $-4a^3 c + a^2 b^2 + 18a\, b\, c - 4b^3 - 27c^2$. Indeed, since $P' = 3x^2 + 2a\, x + b$, the discriminant is $-(3t_1^2 + 2a\, t_1 + b)\, (3t_2^2 + 2a\, t_2 + b)\, (3t_3^2 + 2a\, t_3 + b)$. Ordering the coefficients by powers of a and then by powers of b, and using $+\dots$ to mean that one takes all similar terms par circular permutations, one obtains

the coefficient of a^3 is $-8t_1 t_2 t_3 = -8s_3 = 8c$

the coefficient of $a^2 b$ is $-4t_1 t_2 + \dots = -4s_2 = -4b$

the coefficient of a^2 is $-12t_1 t_2 t_3^2 + \dots = -12 s_3 s_1 = -12 a\, c$

the coefficient of $a\, b^2$ is $-2t_1 + \dots = -2s_1 = 2a$

the coefficient of $a\, b$ is $-6t_1 t_2^2 + \dots = -6(s_1 s_2 - 3s_3) = 6(a\, b - 3c)$

the coefficient of a is $-18 t_1 t_2^2 t_3^2 + \dots = -18 s_3 s_2 = 18 b\, c$

the coefficient of b^3 is -1

the coefficient of b^2 is $-3t_1^2 + \dots = -3(s_1^2 - 2s_2) = -3(a^2 - 2b)$

the coefficient of b is $-9t_1^2 t_2^2 + \dots = -9(s_2^2 - 2s_1 s_3) = -9(b^2 - 2a\, c)$

the coefficient of 1 is $-27 t_1^2 t_2^2 t_3^2 = -27 s_3^2 = -27 c^2$

[1] Edward WARING, English mathematician, 1736–1798. He worked in Cambridge, England, holding the Lucasian chair (1760–1798).

[2] The number of pairs $\binom{n}{2}$ is even if $n = 0, 1 \pmod 4$ and it is odd if $n = 2, 3 \pmod 4$.

so that the discriminant is $\Delta = a^3 8c - a^2 b\, 4b - a^2 12a\, c + a\, b^2 2a + a\, b 6(a\, b - 3c) + a 18 b\, c - b^3 - b^2 3(a^2 - 2b) - b9(b^2 - 2a\, c) - 27c^2 = -4a^3 c + a^2 b^2 + 18a\, b\, c - 4b^3 - 27c^2$.

Notice that for going from this general cubic polynomial to the reduced case of Example 37.6, one puts $y = x + \frac{a}{3}$, and one obtains easily $p = b - \frac{a^2}{3}$ and $q = c - \frac{a\, b}{3} + \frac{2a^3}{27}$, but this computation requires that the characteristic of E be $\neq 3$.

Lemma 37.8: For $K = E(t_1, \ldots, t_n)$, S_n can be seen as a subgroup of $Aut_E(K)$. For $k = Fix(S_n)$, K is a Galois extension of k, $S_n = Aut_k(K)$, and $[K:k] = n!$.
Proof: K is the field of fractions $\frac{A}{B}$ with $A, B \in E[t_1, \ldots, t_n]$, $B \neq 0$, identifying $\frac{A}{B}$ and $\frac{C}{D}$ if and only if $A\, D = B\, C$; then for $\sigma \in S_n$ one has $\sigma A\, \sigma D = \sigma(A\, D) = \sigma(B\, C) = \sigma B\, \sigma C$, i.e. $\frac{\sigma A}{\sigma B} = \frac{\sigma C}{\sigma D}$, so that mapping $\frac{A}{B}$ to $\frac{\sigma A}{\sigma B}$ is an automorphism of K; the constants in E are obviously symmetric, so that E is fixed by σ. Since $Aut_k(K) = S_n$, and K is a Galois extension of k, one has $[K:k] = |Aut_k(K)| = |S_n| = n!$.

Lemma 37.9: For $j = 1, \ldots, n$, define $f_j = (x - t_1) \cdots (x - t_j)$ (so that $f_n = x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n \in E[s_1, \ldots, s_n]$). Then:
a) $k = E(s_1, \ldots, s_n)$.
b) K is a splitting field extension for f_n over k.
c) For $j = 1, \ldots, n$, t_j has degree j over $E(s_1, \ldots, s_n, t_n, \ldots, t_{j+1})$, and f_j is its minimal polynomial.[3]
d) For $j = 1, \ldots, n-1$, the coefficients of f_j are *polynomials* (not just rational fractions) in $E(s_1, \ldots, s_n, t_n, \ldots, t_{j+1})$ (and for $j = n$, one has $f_n = x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$).
Proof: One has $E(s_1, \ldots, s_n) \subset k$ since each s_j is symmetric, and $K = E(s_1, \ldots, s_n, t_1, \ldots, t_n)$ since the s_j are polynomials in $t_1, \ldots, t_n$.

Then, t_n is a root of f_n, and f_n is a polynomial of degree n whose coefficients are polynomials in $s_1, \ldots, s_n$, so that $[E(s_1, \ldots, s_n, t_n) : E(s_1, \ldots, s_n)] \leq n$. Dividing f_n by $x - t_n$ gives f_{n-1}, and Euclidean division shows that the coefficients of f_{n-1} are *polynomials* in $s_1, \ldots, s_n, t_n$, and since t_{n-1} is a root of f_{n-1} one has $[E(s_1, \ldots, s_n, t_n, t_{n-1}) : E(s_1, \ldots, s_n, t_n)] \leq n - 1$. Repeating the same operations leads to $[K : E(s_1, \ldots, s_n)] \leq n!$, but since $E(s_1, \ldots, s_n) \subset k$ and $[K : k] = n!$ by Lemma 37.8, one must have $k = E(s_1, \ldots, s_n)$, which proves a), and for $j = 1, \ldots, n-1$ one must have $[E(s_1, \ldots, s_n, t_n, \ldots, t_{j+1}) : E(s_1, \ldots, s_n, t_n, \ldots, t_j)] = j$, so that f_j is the monic minimal polynomial of t_j, and this proves c). b) follows from the fact that f_n splits in K, and that its roots being $t_1, \ldots, t_n$, they generate K. d) follows from the remark concerning Euclidean divisions.

Lemma 37.10: A basis M of $K = E(t_1, \ldots, t_n)$ over $k = E(s_1, \ldots, s_n)$ is made of the $n!$ monomials $t_1^{\alpha_1} \cdots t_n^{\alpha_n}$ with $0 \leq \alpha_j < j$, for $j = 1, \ldots, n$.
Proof: Notice that α_1 is necessarily 0, since $t_1 = s_1 - t_2 - \ldots - t_n$, and one easily eliminates powers of t_1. By Lemma 37.9, a basis of $K(s_1, \ldots, s_n, t_n)$ over $K(s_1, \ldots, s_n)$ is $1, t_n, \ldots, t_n^{n-1}$, a basis of $K(s_1, \ldots, s_n, t_n, t_{n-1})$ over $K(s_1, \ldots, s_n, t_n)$ is $1, t_{n-1}, \ldots, t_{n-1}^{n-2}$, and so on. Then, one applies repeatedly the argument that if $E \subset F \subset G$ and $a_i \in F, i \in I$, is a basis of F as an E-vector space, and $b_j \in G, j \in J$, is a basis of G as an F-vector space, then $a_i b_j \in G, i \in I, j \in J$, is a basis of G as an E-vector space.

Lemma 37.11: Any polynomial $P \in E[t_1, \ldots, t_n]$ can be written in a unique way as a linear combination of the $n!$ monomials $t_1^{\alpha_1} \cdots t_n^{\alpha_n}$ with $0 \leq \alpha_j < j$, for $j = 1, \ldots, n$, with coefficients in $E[s_1, \ldots, s_n]$ (i.e. *polynomials* in $s_1, \ldots, s_n$, and not arbitrary elements in k, which are rational fractions in $s_1, \ldots, s_n$).
Proof: Since f_j is monic, t_j^j is a linear combination of the t_j^a for $0 \leq a < j$ with coefficients which are polynomials in $s_1, \ldots, s_n, t_n, \ldots, t_{j+1}$, and then by induction the same is true for all powers t_j^m for $m \geq j$. By first replacing all powers t_1^m with $m \geq 1$, then by replacing all powers t_2^m with $m \geq 2$, and so on, one deduces that every polynomial in $E[t_1, \ldots, t_n]$ can be expressed as a linear combination of elements of M with coefficients belonging to $E[s_1, \ldots, s_n]$, i.e. which are polynomials in $s_1, \ldots, s_n$ with coefficients in E; since M is a basis for K as a k-vector space, this decomposition is unique.

Lemma 37.12: Any polynomial $P \in E[t_1, \ldots, t_n]$ which is symmetric can be expressed as a *polynomial* in $s_1, \ldots, s_n$ (i.e. its decomposition on the basis M only uses the vector 1, corresponding to $\alpha_1 = \ldots = \alpha_n = 0$).
Proof: One decomposes P on the basis, and by regrouping terms, one has $P = A + t_2 B_1 + C$, with $A \in E[s_1, \ldots, s_n]$, and B_1, C being polynomials in $t_3, \ldots, t_n$ with coefficients in $E[s_1, \ldots, s_n]$. By using the

[3] For $j = n$, it means t_n has degree n over $E(s_1, \ldots, s_n) = k$, with minimal polynomial f_n.

invariance of P by transposition of t_1 and t_2, one has $P = A + t_1 B_1 + C$, so that $(t_2 - t_1) B_1 = 0$, and since rings of polynomials over Integral Domains are Integral Domains, and $t_2 - t_1 \neq 0$, one has $B_1 = 0$. Then, one has $P = A + t_3 C_1 + t_3^2 C_2 + D$, with C_1, C_2, D being polynomials in $t_4, \ldots, t_n$ with coefficients in $E[s_1, \ldots, s_n]$. By using the invariance of P by transposition of t_1 and t_3, and by transposition of t_2 and t_3, one finds that $t_1 C_1 + t_1^2 C_2 = t_2 C_1 + t_2^2 C_2 = t_3 C_1 + t_3^2 C_2$, and calling the common value $-C_0$, one finds that C_0, C_1, and C_2 satisfy an homogeneous linear system,[4] whose matrix is a Vandermonde matrix, whose determinant is $(t_3 - t_2)(t_3 - t_1)(t_2 - t_1) \neq 0$,[5] so that $C_0 = C_1 = C_2 = 0$. By repeating this argument, one arrives at the conclusion that $P = A \in E[s_1, \ldots, s_n]$.

[4] One may consider that t_1, t_2, t_3, as well as C_0, C_1, C_2, belong to a common field of fractions.

[5] The determinant of a Vandermonde matrix of any size is a polynomial, which is 0 if $t_i = t_j$ with $i \neq j$ (since two rows are equal), so that it has $t_i - t_j$ as a factor, and once it is a polynomial Q times the product of all $t_i - t_j$ for $i > j$, the degree of Q must be 0, and checking the product of the diagonal elements gives Q.