Math 210B Lecture 21 Notes

Daniel Raban

March 1, 2019

1 Elementary Symmetric Functions and Discriminants

1.1 Elementary symmetric functions

Definition 1.1. If F is a field and $x_1, \dots, x_n$ are indeterminates, for $1 \leq k \leq n$, the k-th **elemetary symmetric polynomial** in $x_1, \dots, x_n$ is $s_{n,k} \in F[x_1, \dots, x_n]$ given by

$$s_{n_k} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k} = \sum_{\substack{P \subseteq [n] \\ |P|=k}} \prod_{i \in P} x_i.$$

Example 1.1. Here are some examples of elementary symmetric polynomials.

$$s_{n,1} = x_1 + \cdots + x_n$$

$$x_{n,n} = x_1 \cdots x_n$$

$$x_{n,2} = x_1 x + 2 + x_1 x_3 + \cdots + x_1 \cdots x_n + x_2 x_3 + \cdots + x_2 x_2 + \cdots + x_{n-1} x_n$$

The module generated by these polynomials is isomorphic to $T^k(F^{\oplus n})^{S_k} \cong \mathrm{Sym}^k(F^{\oplus n})$ if $k! \in F^\times$.

Proposition 1.1. *$F(x_1, \dots, x_n)/F(s_{n,1}, \dots, s_{n,n})$ is finite, Galois with Galois group S_n.*

Proof. Call this extension K/E. Then

$$f(y) = \prod_{i=1}^n (y - x_i) = \sum_{i=1}^n (-1)^{n-i} s_{n,i} y^i$$

has roots $x_1, \dots, x_n$. So K is the splitting field of f over E. If $\rho \in S_n$, there exists a unique $\phi(\rho) \in \mathrm{Aut}_R(K)$ such that $\phi(\rho)(h(x_1, \dots, x_n)) = h(x_{\rho(1)}, \dots, x_{\rho(n)})$. Then $\phi(\rho)(s_{n,k}) = s_{n,k})$ so $|phi(\rho) \in \mathrm{Gal}(K/E)$. So $\phi : S_n \to \mathrm{Gal}(K/E)$ is injective. This is also onto as $[K : E] \leq \deg(f)! = n!$. $\square$

Corollary 1.1. *Every finite group is the Galois group of some field extension.*

Proof. If $H \leq S_n$, take $\mathrm{Gal}(K/K^H)$. $\square$

Whether this happens for extensions of $\mathbb{Q}$ is still an open problem. This is false over $\mathbb{Q}_p$, the p-adic numbers, because all finite extensions of $\mathbb{Q}_p$ are solvable.

1.2 Discriminants

Definition 1.2. The **discriminant** of a monic, degree n polynomial $f \in F[x]$ with $f = \prod_{i=1}^n (x - \alpha_i) \in \overline{F}[x]$ is

$$D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Proposition 1.2. *Let $f \in F[x]$. The following are equivalent:*

1. *f is inseparable.*
2. *$D(f) = 0$.*
3. *$f = \sum_{i=0}^n a_i x^i$ and $f' = \sum_{i=1}^n i a_i x^i$ share a common factor in $F[x]$.*

Proposition 1.3. *$D(f) \in F$.*

Proof. We may assume f is separable. Let K be the splitting field and $\sigma \in \mathrm{Gal}(K/F)$. Then

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in F[x_1, \dots, x_n].$$

For $\sigma \in \Delta$, $\sigma(\Delta) = \mathrm{sgn}(\sigma)\Delta$. Then $\sigma(\Delta^2) = \Delta^2$. We have an injective map $\mathrm{Gal}(K/F) \to S_n$ sending $\tau \mapsto \rho(\tau)$. This tells us that $\tau(D(f)) = D(f)$. $\square$

We have actually shown the following.

Corollary 1.2. *Let f be monic, separable, and irreudcible. $D(f) \in (F^\times)^2$ if and only if $\mathrm{Gal}(K/F) \to A_n$ is an embedding via permutation of the roots.*

Example 1.2. Let $f = x^2 + ax + b$. Let α, β be the roots in $\overline{F}$. We also have $F(\alpha) = F(\beta)$. Then $-a = \alpha + \beta$, and $b = \alpha\beta$.

$$D = D(f) = (\alpha - \beta)^2 = a^2 - 4b.$$

If $\mathrm{char}(F) = 2$, then $a^2 - 4b = a^2$. So $F(\alpha)/F$ is trivial if $a \neq 0$ and inseparable if $a = 0$. If $\mathrm{char}(F) \neq 2$, then $F(a)/F$ is separable. Then $a^2 - rb \in F^2 \iff \alpha \in F$. The quadratic formua gives us that $F(\alpha) = F(\sqrt{D})$.

Example 1.3. Suppose $\mathrm{char}(F) \neq 3$, and let $f = x^3 + ax^2 + bx + c \in F[x]$. If we let $y = x + 1/3$, then

$$f(x) = f(y - a/3) = y^3 + \underbrace{(-a^2/3 + b)}_{p}\, y + \underbrace{(3a^2/27 - ab/3 + c)}_{q}.$$

So we have gotten rid of the degree 2 term. Let $g = x^3 + px + q \in F[x]$. Let K be the splitting field of f over F, and let $\alpha, \beta, \gamma \in K$ be the roots of g. Then

$$s_{3,1}(\alpha, \beta, \gamma) = \alpha + \beta + \gamma = 0$$

$$s_{3,2}(\alpha\beta, \gamma) = p$$

$$s_{3,3}(\alpha\beta, \gamma) = -\alpha\beta\gamma = q$$

Then

$$0 = (\alpha + \beta + \gamma)^2 = \alpha^2 + \beta^2 + \gamma^2 + 2p$$

$$p = (\alpha\beta + \alpha\gamma + \beta\gamma)^2 = \alpha^2\beta^2 + \alpha^2 2\gamma^2 + \beta^2\gamma^2.$$

We can the compute

$$g' = 3x^2 + p = s_{3,2}(x - \alpha, x - \beta, x - \gamma)$$

$$g'(x) = 3\alpha^2 + \beta = (\alpha - \beta)(\alpha - \gamma)$$

So in the end, we get

$$-D(g) = (3x^2 + p)(3\beta^2 + p)(3\gamma^2 + \beta) = 27q^2 + 4p^3.$$

Then observe that

$$D(f) = D(g) = -27q^2 - 4p^3.$$

If f is irreducible, then $\mathrm{Gal}(K/F) \to S_3$ is an embedding and the Galois group has order divisible by 3. So this is isomorphic to $A_3 \cong \mathbb{Q}/3$, or it is isomorphic to S_3 itself. We get $\mathrm{Gal}(K/F) \cong \mathbb{Z}/3\mathbb{Z}$ if $D(f) \in (F^\times)^2$, and $\mathrm{Gal}(K/F) \cong S_3$ otherwise.