Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

November 9, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Symmetric Functions

Galois theory is concerned with determining the permutations of the roots of a polynomial which extend to a field automorphism. Now we will consider a simple situation in which every permutation extends. I.e. when the roots are independent variables.

Let R be any ring and consider $R[x_1, \ldots, x_n]$. A permutation σ of $\{1, \ldots, n\}$ can be made to operate on polynomials by simply permuting the variables. Notationally we will keep automorphisms on the left (so σ operates by inverse permutation). So

$$f = f(x_1, \ldots, x_n) \overset{\sigma}{\rightsquigarrow} f(x_{1\sigma^{-1}}, \ldots x_{n\sigma^{-1}}) = \sigma f$$

This clearly leads to an R-automorphism on the polynomial ring $R[\mathbf{x}]$. So we see that the symmetric group S_n operates by R-automorphism on $R[\mathbf{x}]$

Symmetric Polynomial

Definition 0.1.0.1. A polynomial is called symmetric if it is left fixed by all permutations.

Elementary Symmetric Functions

Definition 0.1.0.2. There are n symmetric polynomials with integer coefficients called the elementary symmetric functions s

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \textstyle\sum_{i<j} x_ix_j \\ s_3 &= \textstyle\sum_{i<j<k} x_ix_jx_k \\ &\cdots \\ s_n &= x_1x_2\cdots x_n \end{aligned}$$

They are the coefficients of the polynomial

$$p(x) = (x-x_1)(x-x_2)\cdots(x-x_n) = x^n - s_1x^{n-1} + \cdots \pm s_n$$

The main theorem of symmetric functions says that the elementary symmetric functions generates the ring of all symmetric functions.

Symmetric Polynomials in term of Elementary Polynomials

Theorem 0.1.0.3. *Every symmetric polynomial* $g(x_1, \ldots, x_n) \in R[\boldsymbol{x}]$ *can be written in a unique way as a polynomial in the elementary symmetric functions* $s_1, \ldots, s_n$ *In other words, let* $z_1, \ldots, z_n$ *be variables. For each symmetric polynomial* $g(\boldsymbol{x})$ *there is a unique polynomial* $\varphi(z_1, \ldots, z_n) \in R[z_1, \ldots, z_n]$ *such that*

$$g(x_1, \ldots, x_n) = \varphi(s_1, \ldots, s_n)$$

Proof. In the case $n = 1$ there is nothing to show as $u_1 = s_1$.

By induction lets assume the theorem is proved for $n-1$

variables to show it is true with n variables.

Given a symmetric polynomial f in $u_1, \ldots, u_n$ we consider the polynomial f^0 obtained by substituting 0 for the last variable

$$f^0(u_1, \ldots, u_{n-1}) = f(u_1, \ldots, u_{n-1}, 0)$$

We note that f^0 can be expressed as a polynomial in the elementary functions in $\{u_1, \ldots, u_{n-1}\}$ by induction. Denote the elementary symmetric polynomials in $\{u_1, \ldots, u_{n-1}\}$ by

$$s_1^0 = u_1 + \cdots + u_{n-1}, \cdots, s_{n-1} = u_1 \cdots u_{n-1}$$

Let $f^0 = g(s_1^0, \ldots, s_n^0)$. Moreover it follows form teh definition of the polynomials s_i that $s_i^0 = s_i(u_1, \ldots, u_{n-1}, 0)$ if $i \leq n-1$.

Consider

$$p(u_1, \ldots, u_n) = f((u_1, \ldots, u_n) - g(s_1, \ldots, s_{n-1})$$

As this is the difference of symmetric polynomials, it is itself symmetric. Also, it has the property that $p(u_1, \ldots, u_{n-1}, 0) = 0$. Hence every monomial polynomial in $p(u_1, \ldots, u_n)$ is divisible by u_n.

So by symmetry $p(u_1, \ldots, u_n)$ is divisible by u_i for all i. Hence

$$f(u_1, \ldots, u_n) = g(s_1, \ldots, s_{n-1}) + s_n h(u_1, \ldots, u_n)$$

for some symmetric polynomial h.

We can then do induction on the degree of h to see that h is a polynomial in the symmetric functions and hence so is f.

So all that is left is to prove the uniqueness of $\varphi(s_1, \ldots, s_n) = f(u_1, \ldots, u_n)$. In other words the kernel of

$$\sigma : R[z] \to R[u],\ z_i \rightsquigarrow s_i$$

is zero. To show this suppose that $\varphi(s_1, \ldots, s_n) = 0$ for some $\varphi \in R[z]$. Setting $u_n = 0$ we still get 0. I.e. $\varphi(s_1^0, \ldots, s_{n-1}^0, 0) = 0$. By induction on n this implies $\varphi(z_1, \ldots, z_{n-1}, 0) = 0$. Therefore z_n divides $\varphi(\mathbf{z}_1, \ldots, z_n)$ and $\varphi(z) = z_n\psi(z)$ and so $0 = \varphi(s) = s_n\psi(s) = u_1 \cdots u_n\psi(s)$. And, since $u_1 \cdots u_n$ is not a zero divisor in $R[u]$, we must have $\psi(s) = 0$. But the polynomial $\psi(z)$ has lower total degree in z than $\varphi(z)$ so we can apply induction to the degree to conclude $\psi = 0$ and hence $\varphi = 0$. □

For example

$$\Sigma_i u_i^2 = s_1^2 - 2s_2$$

Definition of Discriminant

Definition 0.1.0.4. the discriminant of the polynomial $p(x)$ is defined to be

$$D = \prod_{i<j}(u_i - u_j)^2 = (-1)^{n(n-1)/2}\prod_{i\neq j}(u_i - u_j)$$

This is probably the most important elementary polynomial. Symmetric Polynomials are Independent

Corollary 0.1.0.5. *There are no polynomial relations among the elementary symmetric functions* $s_1, \ldots, s_n$. *Equivalently, the subring* $R[s_1, \ldots, s_n]$ *of* $R[\boldsymbol{x}]$ *generated by* $\{s_i\}$ *is isomorphic to the polynomial ring* $R[z_1, \ldots, z_n]$

Proof. Immediate from previous theorem. □

Now suppose that $R = F$ is a field. WE can for the field of fractions of $F[x_1, \ldots, x_n]$ and S_n acts on this field as well (by permuting the variables). We then have the following theorem.

Rational Symmetric Polynomial

Theorem 0.1.0.6. *Every symmetric rational function is a rational function in* $s_1, \ldots, s_n$.

Proof. Let $r(u) == f(u)/g(u)$ be a symmetric rational function, where $f, g \in F[u]$. We can build a symmetric function from g by multiplying all the σg together

$$G = \prod_{\sigma \in S_n} \sigma g$$

is a symmetric polynomial. Then $G(u)r(u)$ is a symmetric rational function and it is also a polynomial in $\{u_1, \ldots, u_r\}$ and hence is a symmetric polynomial.

By the previous theorem $G(u)$ and $G(u)r(u)$ are polynomials in the elementary functions $\{s_i\}$. Thus $r(u)$ is a rational function in $\{s_i\}$ □

Now consider the pair of fields

$$F(\int) = F(s_1, \ldots, s_n) \subset F(x_1, \ldots, x_n) = F(\mathbf{x})$$

We see that $F[\mathbf{x}]$ is a Galois extension of $F(\int)$. This follows because $F(\mathbf{x})$ is a splitting field of the polynomial $p(x)$ and because the roots are distinct.

We know from a previous result that the Galois group $G(F(\mathbf{x})/F(\int))$ operates faithfully on the roots of $p(x)$. However G also contains the full symmetric group S_n by the construction. So $G = S_n$ and $|G| = [F(\mathbf{x}) : F(\int)] = n!$.

0.2 Primitive Elements

Recall from the case of finite fields that we had a primitive element $a \in \mathcal{F}_q$ is one such that $(\forall b \in \mathcal{F}_q - \{0\})(\exists n \in \omega)$ such that $a^n = b$. And in particular such that $\mathcal{F}_q = \mathcal{F}_p(a)$. We now want to generalize that to the case of characteristic 0

Existence of Primitive Elements

Theorem 0.2.0.7 (Existence of a primitive element)**.** *Let K be a finite extension of a field F of characteris-*

tic 0. there is an element $\gamma \in K$ such that $K = F(\gamma)$.

Definition of Primitive Element

Definition 0.2.0.8. We call an element $\gamma \in K$ such that $F(\gamma) = K$ a primitive element for K over F.

Notice that the assumption the field has characteristic p is important as in characteristic 0 this theorem isn't true (although for finite fields it is).

Proof. We will do this by induction on the number of generators of K. Say $KK = F(\alpha_1, \ldots, \alpha_n)$.

If $n = 1$ then we are done

So we may assume that $F(\alpha_1, \ldots \alpha_{n-1})$ is generated by a single element β and hence $K = F(\beta, \alpha_n)$. So we have thereby reduced to the case when $n = 2$.

Lets assume $K = F(\alpha, \beta)$ and let $f(x), g(x)$ be the irreducible polynomials of α, β over F. Let K' be an extension of K such that $f(x)$ and $g(x)$ split completely and let $\alpha = \alpha_1, \ldots, \alpha_n$ and $\beta = \beta_1, \ldots, \beta_m$ be their roots. We then know that the roots are distinct.

Now let $\gamma = \beta + c\alpha$ for $c \in F$. Further let $L = F(\gamma)$. So it suffices to show that $\alpha \in L$ as then $\beta = \gamma - c\alpha \in L$ and so $L = K$.

We will do this by determining the irreducible polynomial of α over L. This is the monic polynomial of least degree in $L[x]$ which has α as a root.

Now we know that α is a root of $f(x)$. Now the key is to realize that $h(x) = g(\gamma - cx)$ also has α as a root and has coefficients in L. So we need to show that the

greatest common divisor of f and h in L is $(x - \alpha)$. It will then follow that $-\alpha$, being one of the coefficients of $(\mathbf{x} - \alpha)$ is in L.

Now we know that the monic greatest common divisor of f and h is the same no matter if it is computed in L or in K'. So we may make our computation in $K'[x]$. In that ring f is a product of linear factors $(x - \alpha_i)$ and so it suffices to show that none of them divide h except for $\alpha = \alpha_1$.

So all that is left is to compute the roots of h. Since the roots of g are the β_i the roots of $h(x) = g(\gamma - cx)$ are obtained by solving the equations

$$\gamma - cx = \beta_i$$

for x. Since $\gamma = \beta + c\alpha$ the roots are $\gamma - \beta_j/c =$

$(\beta - \beta_j)/c + \alpha$. We want these roots to be different from α_i for all $i \neq 1$. This will be the case as long as c is not one of the finite values

$$-(\beta_j - \beta)/(\alpha_i - \alpha)$$

with $i, j \neq 1, 1$. □

This is an important result because it then allows us to use the tools we have developed for studying extensions by a single element to study arbitrary finite extensions of a field.

Permutations of a root

Theorem 0.2.0.9. *Let G be a finite group of automorphisms of a field K and let F be its fixed field. Let $\{\beta_1, \ldots, \beta_r\}$ be the orbit of an element $\beta = \beta_1 \in K$ under the action of G. Then β is algebraic over F, it's degree over F is r and its irreducible polynomial over F is $g(x) = (x - \beta_1) \cdots (x - \beta_r)$. Further note*

that r divides $|G|$.

Proof. Let $f(x)$ be the irreducible polynomial of β over F. Since $f(x)$ is fixed by each G each element β_i is a root of f and so g divides f. Also g is fixed by all permutations of $\{\beta_1, \ldots, \beta_r\}$ and hence by the operation of G which permutes the orbit. Therefore $g(x) \in F[x]$ and so $g = f$ as f is irreducible. □

This result gives us a method of determining the irreducible polynomial for an element β of a Galois extension K over F.

Galois Extensions As Splitting Fields

Corollary 0.2.0.10. *Let K/F be a Galois extension. Let $g(x)$ be an irreducible polynomial in $F[x]$. If g has one root in K then it factors into linear factors in $K[x]$*

Proof. According to the previous corollary F is the fixed

field of the Galois group $G(K/F)$. Let β be a root of $g(x)$ in K. By the previous proposition the irreducible polynomial for β over F is $(x-\beta_1)\cdots(x-\beta_r)$ where $\{\beta_1,\ldots,\beta_r\}$ is the G-orbit of β since $g(x)$ is the irreducible polynomial for β, it is equal to this product so it factors into linear factors in K as asserted. □

Fixed Field of a Group of Automorphisms

Theorem 0.2.0.11. *Let G be a group of order n of automorphisms of a field K and let F be its fixed field. Then $[K:F]=n$.*

Proof. We know that every element $\beta\in K$ is algebraic over F and that its degree divides $|G|$. The theorem of the primitive element implies that the degree of the whole field extension K/F is bounded by n too because we know that $K=F(\alpha_1,\ldots,\alpha_m)$ and hence $K=F(\gamma)$ for some $\gamma\in K$.

Now any element of G which fixes γ is the identity on K. As such the stabilizer of γ is $\{1\}$ and so the orbit of γ has size $|G|/1 = |G|$. Hence we have that the order of γ is n and $[K : F] = n$ □

This then allows to see that if K/F is any finite extension then the order of the Galois group must divide the degree. To prove this let $G = G(K/F)$. then G operates on K so $|G| = [K : K^G]$ and since $F \subset K^G \subset K$ $[K : K^G]$ divides $[K : F]$.

Fixed Field as Galois Group

Corollary 0.2.0.12. *Let G be a finite group of automorphisms of a field K and let F be its fixed field. Then K is a Galois extension of F and its Galois group is G.*

Proof. By the definition of fixed field, the elements of G

are F-automorphisms of K. Hence $G \subset G(K/F)$. Since $|G(K/F)| \leq [K : F]$ and $[K : F] = |G|$ it follows that $|G(K/F)| = [K : F]$ and that $G = G(K/F)$. $\square$

0.3 TODO

- Go through Lang's book on the same topics.