Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

November 14, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Proof of the Main Theorem

Let $f(x)$ be a monic polynomial of degree n with coefficients in a field F. We recall that a splitting field of $f(x) \in F[x]$ is a field of the form $K = F(\alpha_1, \ldots, \alpha_n)$ such that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $K[x]$. We now want to show that any two splitting fields of a given polynomial $f(x)$ are isomorphic. This follows from the fact that a field extension of the form $F(\alpha)$ is determined by the irreducible polynomial for α over F and from some "bookkeeping". The bookkeeping is notationally a little confusing but not hard.

Extending Isomorphism

Definition 0.1.0.1. Let $\varphi : F \to \overline{F}$ be an isomorphism. Then φ extends to an isomorphism $F[x] \to \overline{F}[x]$

by

$$\sum a_n x^n \rightsquigarrow \sum \overline{a_n} x^n$$

where $\overline{a_n} = \varphi(a_n)$. We denote by $\overline{f}(x)$ the image of $f(x)$ under this map.

Notice that as φ is an isomorphism, $f(x)$ is irreducible if and only if $\overline{f}(x)$ is irreducible.

Image of Root.

Lemma 0.1.0.2. *Let $f(x) \in F[x]$ be an irreducible polynomial. Let α is a root of $f(x)$ in an extension field K of F and let $\overline{\alpha}$ be a root of $\overline{f}(x)$ in an extension field $\overline{K}$ of $\overline{F}$. Then there is a unique isomorphism*

$$\varphi_1 : F(\alpha) \to \overline{F}(\overline{\alpha})$$

which restricts to φ on a the subfield F and which sends α to $\overline{\alpha}$.

Proof. We know that $F(\alpha)$ is isomorphic to the quotient $F[x]/(f)$ and similarly $\overline{F}(\overline{\alpha})$ is isomorphic to $\overline{F}[x]/(\overline{f})$.

The rings $F[x]$ and $\overline{F}[x]$ are isomorphic as we saw, and since f and $\overline{f}$ correspond under this isomorphism, so do the ideals (f) and $(\overline{f})$. Hence the rings $F[x]/(f)$ and $\overline{F}[x]/(\overline{f})$ are isomorphic, and combining these isomorphisms yields the isomorphism φ_1. □

Isomorphism of Splitting Fields

Theorem 0.1.0.3. *Let $\varphi : F \to \overline{F}$ be an isomorphism of fields. Let $f(x) \in F[x]$ be nonconstant and let $\overline{f}(x)$ be the corresponding polynomial in $\overline{F}[x]$. Let K and $\overline{K}$ be the splitting fields for $f(x)$ and $\overline{f}(x)$. Then there is an isomorphism $\psi : K \to \overline{K}$ which restricts to φ on F.*

Proof. If $f(x)$ factors into linear factors over F, then $\overline{f}(x)$ also factors into linear factors. In the case $K = F$ and $\overline{K} = \overline{F}$, so $\varphi = \psi$.

Now assume that f does not split completely. Choose an irreducible factor $g(x)$ of $f(x)$ of degree > 1. The corresponding polynomial $\overline{g}(x)$ will make an irreducible factor of $\overline{f}(x)$. Let α be a root of g in K and write $F_1 = F(\alpha)$. Make a similar choice for $\overline{\alpha}$ and let $\overline{F_1} = \overline{F}(\overline{\alpha})$ in $\overline{K}$. Then by the previous lemma we can extend φ to an isomorphism $\varphi_1 : F_1 \to \overline{F_1}$ which sends $\alpha \rightsquigarrow \overline{\alpha}$. Being a splitting field for f over F, K is also a splitting field of f over the larger field F_1 and similarly $\overline{K}$ is a splitting field for $\overline{f}$ over $\overline{F}_1$. Therefore we may replace $F, \overline{F}, \varphi$ by $F_1, \overline{F_1}, \varphi_i$ and proceed by induction. □

Corollary 0.1.0.4. *Any two splitting fields of $f(x) \in F[x]$ are isomorphic.*

Proof. Set $F = \overline{F}$ and $\varphi = id$ in the previous theorem. □

Splitting Fields are Galois

Theorem 0.1.0.5. *Let K be the splitting field of a polynomial $f(x) \in F[x]$. Then K is a Galois extension of F. That is $|G(K/F)| = [K : F]$*

Number of Isomorphisms

Lemma 0.1.0.6. *With the notation of the previous lemma, the number of isomorphisms $\psi : K \to \overline{K}$ extending φ is equal to $[K : F]$*

Proof. We proceed as in the proof of the previous theorem. Choose an irreducible factor $g(x)$ of $f(x)$ and one of the roots α of $g(x)$ in K. Let $F_1 = F(\alpha)$. Any isomorphism $\psi : K \to \overline{K}$ extending φ will send F_1 to some subfield $\overline{F_1}$ of $\overline{K}$. This field $\overline{K}$ will have the form $\overline{F}(\overline{\alpha})$ where $\overline{\alpha} = \psi(\alpha)$ is a root of $\overline{g}(x)$ in $\overline{K}$.

Conversely to extend φ to ψ we may start by choosing any root $\overline{\alpha}$ of $\overline{g}(x)$ in $\overline{K}$. We then extend φ to a map

$\varphi_1 : F_1 \to \overline{F}_1 = \overline{F}(\overline{\alpha})$ by setting $\varphi_1(\alpha) = \overline{\alpha}$.

We use induction on $[K : F]$. Since $[K : F_1] < [K : F]$ the induction hypothesis tells us that for this particular choice of φ_1 there are $[K : F_1]$ extensions of φ_1 to an isomorphism $\psi : K \to \overline{K}$. On the other hand, $\overline{g}$ has distinct roots in $\overline{K}$ because $g, \overline{g}$ are irreducible. So the number of choices for $\overline{\alpha}$ is the degree of g which is $[F_1 : F]$. So there are $[F_1 : F]$ choices for the isomorphism φ_1. This gives us a total of $[K : F_1][F_1 : F] = [K : F]$ extensions of φ to $\psi : K \to \overline{K}$. □

Galois Group of Polynomial

Definition 0.1.0.7. Since any two splitting fields K of $f(x) \in F[x]$ are isomorphic, the Galois group $G(K/F)$ depends, up to isomorphism, only on f. It is often referred to as the Galois group of the polynomial over F.

Collection of Equivalences

Corollary 0.1.0.8. *Let K/F be a finite field extension. the following are equivalent.*

(i) K is a Galois extension of F.

(ii) K is the splitting field of an irreducible polynomial $f(x) \in F[x]$.

(ii') K is the splitting field of a polynomial $f(x) \in F[x]$.

(iii) F is the fixed field for the action of the Galois group $G(K/F)$ on K.

(iii') F is the fixed field for an action of a finite group of automorphisms of K.

Main Theorem of Galois Theory

Theorem 0.1.0.9 (Main Theorem)**.** *Let K be a Galois extension of a field F and let $G = G(K/F)$ be its*

Galois group. the function

$$H \rightsquigarrow K^H$$

is a bijective map form the set of subgroups of G *to the set of intermediate fields* $F \subset L \subset K$*. Its inverse function is*

$$L \rightsquigarrow G(K/L)$$

This correspondence has the property that if $H = G(K/L)$ *then*

$$[K : L] = |H| \text{ and } [L : F] = [G : H]$$

Proof. Let K/F be a Galois extension. We have to show that the maps

$$L \rightsquigarrow G(K/L) \text{ and } H \rightsquigarrow K^H$$

are inverse functions between sets of intermediate fields and the set of subgroups of $G = G(K/F)$. To do so we verify the compositions of the two maps in either direction are the identity.

Let L be an intermediate field. The corresponding subgroup of G is $H = G(K/L)$. By definition, H acts trivially on L, so $L \subseteq K^H$. On the other hand, K is a Galois extension of L by previous results. Hence $[K : L] = |H|$. However also by previous results we have $|H| = [K : K^H]$ and so $L = K^H$.

In the other direction, suppose that we start with a subgroup $H \subset G$ and let $L = K^H$. Then $H \subset G(K/L)$. But $|H| = [K : K^H] = [K : L] = |G(K/L)|$. Therefore $H = G(K/L)$.

We therefore have that these two maps are inverses. Further since K is a Galois extension of $L = K^H$, $[K : L] = |H|$ and $[L : F] = [G : H]$ □

There are a few properties of the Main Theorem which

are worth discussing. First notice that the correspondence between fields and groups is order reversing. That is if L, L' are two fields and $H = G(K/L)$ and $H' = G(K/L')$ then $L \subset L$ if and only if $H \subset H'$ **Images of Intern**

Theorem 0.1.0.10. *Let K/F be a Galois extension and let L be an intermediate field. Let $H = G(K/L)$ be the corresponding subgroup of $G = G(K/F)$. Then*

(a) Let σ be an element of G. The subgroup of G which corresponds to the conjugate subfield σL is the conjugate subgroup $\sigma H \sigma^{-1}$. In other words $G(K/\sigma L) = \sigma H \sigma^{-1}$.

(b) L is a Galois extension of F if and only if H is a normal subgroup of G. When this is so, then $G(L/F)$ is isomorphic to the quotient group G/H

*****SEE DIAGRAM ON PAGE 559 *****

Proof. Part (a):

Let $\sigma L = L'$. If τ is an element of $H = G(K/L)$ then $\sigma\tau\sigma^{-1}$ is in $H' = G(K/L')$. To check this we mush show that $\sigma\tau\sigma^{-1}$ fixes every element $\alpha' \in L'$. By the definition of σL $\alpha' = \sigma(\alpha)$ for some $\alpha \in L$. Then $\sigma\tau\sigma^{-1}(\alpha') = \sigma\tau(\alpha) = \sigma(\alpha) = \alpha'$ as required. Hence $H' \supset \sigma H\sigma^{-1}$ and by counting elements we have $H' = \sigma H\sigma^{-1}$

Part (b):

Now suppose that H is normal. Then $H = \sigma H\sigma^{-1}$ for all $\sigma \in G$. Hence $G(K/L) = G(K/\sigma L)$. this implies that $L = \sigma L$ for all σ. Thus every F-automorphism of K carries L to itself and hence defines an F-automorphism of L by restriction. The restriction defines a homomorphism

$$\pi : G \to G(L/F)$$

Its kernel is the set of $\sigma \in G$ which induce the identity on L, which is H. Therefore G/H is isomorphic to $G(L/F)$. Counting degrees and orders we have

$$[L : F] = |G/H| \leq |G(L/F)|$$

Hence L is a Galois extension and that $G/H \approx G(L/F)$

Conversely suppose that L/F is Galois. Then L is a splitting field of some polynomial $g(x) \in F[x]$. So $L = F(\beta_1, \ldots, \beta_k)$ where the β_i are the roots of $g(x)$ in K. An F-automorphism σ of K permutes these roots and therefore carries L to itself. $L = \sigma l$ By Part (a), $H = \sigma H \sigma^{-1}$ and thus H is normal. □

0.2 Kummer Extensions

Now we will consider extensions which contain pth roots of unity where p is a prime. For now we will assume that all fields are subfields of $\mathbb{C}$.

Definition 0.2.0.11. Let $F \subseteq \mathbb{C}$ be a subfield of $\mathbb{C}$ which contains a primitive pth root of unity $\zeta_p = e^{2\pi i/p}$.

Extensions Generated by Single Root of $x^p - a$

Lemma 0.2.0.12. *If α is a root of $f(x) = x^p - a$ then $\alpha, \zeta_p\alpha, \zeta_p^2\alpha, \ldots, \zeta_p^{p-1}\alpha$ are the roots of $f(x)$. So the splitting field of $x^p - a$ is generated by a single root $K = F[\alpha]$*

Proof. This is easy to see as $(\alpha\zeta_p^m)^p = a$ for all m. And further as $\zeta_p^m \neq \zeta_p^{m'}$ for all $m' \neq m$ these are all the roots. So it suffices to show that $\zeta_p \in F(\alpha, \alpha\zeta_p, \ldots, \alpha\zeta_p^{p-1})$. But this is true because $\zeta_p = (\alpha\zeta_p)/\alpha$. □

Splitting Field of $x^p - a$

Theorem 0.2.0.13. *Let $F \subseteq \mathbb{C}$ and let F contain a pth root of unity. Further let $a \in F$ be an element which is not a pth power in F. Then the splitting field*

of $f(x) = x^p - a$ has degree p over F and its Galois group is a cyclic group of order p.

Proof. Let K be a splitting field of f and let α be one of its roots in K. Assume that α is not in F. Then there is an automorphism σ of K/F which does not fix α. Since the roots of f are $\zeta^i\alpha, i = 0, \ldots, p-1, \sigma(\alpha) = \zeta^m\alpha$ for some $m \neq 0$.

We now compute powers of σ. Remembering that σ is an automorphism and that $\sigma(\zeta) = \zeta$ because $\zeta \in F$ we find that $\sigma^2(\alpha) = \sigma(\zeta^m\alpha) = \zeta^m\sigma(\alpha) = \zeta^{2m}\alpha$. Similarly, $\sigma^i(\alpha) = \zeta^{im}$ for all i. Since ζ is a pth root of unity the smallest positive power of σ which fixes α is σ^p. Hence the order of σ in the Galois group is at least p. On the other hand, α generates K over F and α is a root of the polynomial $x^p - a$ of degree p, so $[K : F] \leq p$. This shos at the same time that $[K : F] = p$, that $x^p - a$ is

irreducible over F, and that $G(K/F)$ is cyclic of order p. □

Galois Extensions of Degree p

Theorem 0.2.0.14. *Let F be a subfield of $\mathbb{C}$ which contains a pth root of unity ζ_p and let K/F be a Galois extension of degree p. Then K is obtained by adjoining a pth root to F.*

Proof. The Galois group G has prime order $p = [K : F]$ so it is a cyclic group. Any element σ, not the identity, will generate it. Let us view K as an F-vector space. Then σ is a linear operator on K. For, since σ is an F-automorphism,

$$\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta) \text{ and } \sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\sigma(\alpha)$$

for all $c \in F$ and $\alpha, \beta \in K$. Since G is a cyclic group of order $p, \sigma^p = 1$. An eigenvalue λ for this operator must satisfy the relation $\lambda^p = 1$ which means that λ is a power

of ζ. By hypothesis, these eigenvalues are in the field F. Moreover, there is at least one eigenvalue different from 1. This is a fact about any linear operator T such that some power of T is the identity, because such a linear operator can be diagonalized. Its eigenvalues are the entries of the diagonal matrix A which represents it. If T is not the identity, as is the case here, then $A \neq I$, so some diagonal entry is different from 1.

We choose an eigenvector α with an eigenvalue $\zeta^i \neq 1$. Then $\sigma(\alpha) = \zeta^i\alpha$ and hence $\sigma(\alpha^p) = \sigma(\alpha)^p = (\zeta^i\alpha)^p = \zeta^{ip}\alpha^p = \alpha^p$. So σ fixes α^p. Since σ generates G the element α^p is in the fixed field K^G which is F.

We have therefore found an element $\alpha \in K$ whose pth power is in F. Since $\sigma(\alpha) \neq \alpha$ the element α is not in F. But, since $[K : F]$ is prime, α generates K. $\square$

Kummer Extensions

Definition 0.2.0.15. Extensions of the above type are called Kummer Extensions

0.3 TODO

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