Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

November 7, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 The Main Theorem of Galais Theory

Last chapter we studied algebraic field extensions using extensions generated by a single element. This amounts to studying the properties of a single root of an irreducible polynomial

$$f(x) = \Sigma_i a_i x^i$$

Now we will study all roots of such a polynomial and the symmetries between them. We will assume for now that all fields are of characteristic 0 as it will make things simpler.

Field Extension Notation

Definition 0.1.0.1. If K is a field extension of F we say K/F.

We know that if we want to compute with a single root of

f over a field F we can consider $F[x]/(f)$. However suppose f factors into linear polynomials $(x-\alpha_1)\cdots(x-\alpha_n)$ in some larger field K. It is less clear how to calculate with all of these roots.

The most important result which came about through the work of Lagrange and Galois is that the relationships between the roots can be understood in terms of symmetry. The original model for this symmetry was complex conjugation. So to start lets consider extensions of degree 2.

Degree two extensions

Theorem 0.1.0.2. *Let K/F be of degree 2. Then K is generated by a single element α over F. Further α is the root of an irreducible polynomial $f(x) = x^2 + bx + c$*

Proof. From Previous Lecture Notes. □

We then know that $\alpha' = -b - \alpha$ is also a root of $f(x)$. So in K

$$f(x) = (x - \alpha)(x - \alpha')$$

In particular we then know that there is an isomorphism

$$\sigma : F(\alpha) \to F(\alpha')$$

such that $\sigma|F = id$ and $\sigma(\alpha) = \alpha'$.

But we then have

$$\alpha + \alpha' = b$$

and since σ fixes b we also have

$$\sigma(\alpha) + \sigma(\alpha') = \alpha' + \sigma(\alpha') = b$$

So we have $\sigma(\alpha') = \alpha$ and $\sigma^2 = id$.

Definition F automorphisms

Definition 0.1.0.3. An F-automorphism of K is an automorphism of K which is the identity on F.

Definition Galois Group

Definition 0.1.0.4. The group of all F-automorphisms of K is called the Galois Group of the field extension $(G(K/F))$

*****MAYBE FILL IN THE BIQUADRATIC EXAMPLE (P. 539) *****

Order of Galois Group Divides D

Theorem 0.1.0.5. *For any finite extension K/F the order of $|G(K/F)|$ divides the degree $[K : F]$ of the field extension.*

Proof. Later □

Definition Galois Extension

Definition 0.1.0.6. A finite field extension K/F is called a Galois Extension if

$$|G(K/F)| = [K : F]$$

Definition Fixed Field

Definition 0.1.0.7. Let G be a group of automorphisms of K. The set of elements fixed by every element of G is called the fixed field of G

$$K^G = \{\alpha \in K : \varphi(\alpha) = \alpha \text{ for all } \varphi \in G\}$$

Fixed Field

Corollary 0.1.0.8. *Let K/F be a Galois extension with Galois group $G = G(K/F)$. The fixed field of G is F.*

Proof. Let L denote the fixed field of G. Then $F \subset L$ and this inclusion shows that every L-automorphism of K is also an F-automorphism. That is $G(K/L) \subseteq G$. On the other hand by the definition of fixed field, every element of G is an L-automorphism. So $G(K/L) = G$. Now $|G| = [K : F]$ because K/F is a Galois extension. But we then also have $|G|$ divides $[K : L]$. However,

since $F \subset L \subset K$ this shows $[K : F] = [K : L]$ and we are done. $\square$

Definition Splitting Field

Definition 0.1.0.9. Let $f(x) \in F[x]$ be a nonconstant monic polynomial. A splitting field for $f(x)$ over F is an extension K of F such that

(i) $f(x)$ factors into linear factors in K : $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ with $\alpha_i \in K$

(ii) K is generated by the roots of $f(x)$: $K = F(\alpha_1, \ldots, \alpha_n)$

Notice that every polynomial has a splitting field. To see this just choose an extension where F splits into linear factors and then take the field generated by the roots.

Fixed Fields are Galois Extensions

Theorem 0.1.0.10. *If K is a splitting field of a polynomial $f(x)$ over F then K is a Galois extension of*

F. Conversely, every Galois extension is a splitting field of some polynomial $f(x) \in F[x]$.

Proof. Later □

Every Finite Extension and Galois Extensions

Corollary 0.1.0.11. *Every finite extension is contained in a Galois extension.*

Proof. Let K/F be a finite extension and let $\alpha_1, \ldots, \alpha_n$ be generators for K over F. Let $f_i(x)$ be the monic irreducible polynomial for α_i over F. We extend K to a splitting field L of the product $f = f_1 \cdots f_n$ over K. Then L will also be a splitting field of f over F. So L is the required Galois extensions. □

Galois Extensions and Intermediate Fields

Corollary 0.1.0.12. *Let K/F be a Galois extension and let L be an intermediate field: $F \subset L \subset K$. Then K/L is a Galois extension too.*

Proof. If K is the spliting field of a polynomial $f(x)$ over F, then it is also the splitting field of the same polynomial over the larger field L, so K is a Galois extension of L. □

Theorem 0.1.0.13. *(a) Let K be an extension of a field F, let $f(x)$ be a polynomial with coefficients in F and let σ be an F-automorphism of K. If α is a root of $f(x)$ in K then $\sigma(\alpha)$ is also a root.*

(b) Let K be a field extension generated over F by elements $\alpha_1, \ldots, \alpha_r$ and let σ be an F-automorphism of K. If σ fixes each of the generators α_i then σ is the identity automorphism.

(c) Let K be a splitting field of a polynomial $f(x)$ over F. The Galois group $G(K/F)$ operates faithfully

on the set $\{\alpha_1, \ldots, \alpha_r\}$.

Proof. We proved part (a) previously.

To prove part (b) assume that K is generated by $\alpha_1, \ldots, \alpha_n$. Then every element of K can be expressed as a polynomial in $\alpha_1, \ldots, \alpha_n$ with coefficients in F. If σ is an automorphism which is the identity on F and which also fixes each of the elements α_i, then it fixes every polynomial in $\{\alpha_i\}$ with coefficients in F. Hence it is the identity.

Part (c) follows from the first two. The first tells us that every $\sigma \in G(K/F)$ permutes the set $\{\alpha_1, \ldots, \alpha_n\}$ and the second tells us that the operation on this set is faithful. □

We still have one very interesting question which we haven't answered yet "Which permutations of the roots of poly-

nomials extend to automorphisms of the splitting field?" This question is the central theme of Galois theory.

One of the most important parts of Galois theory is the determination of the Intermediate fields L. Those sandwiched between F and K. I.e. $F \subset L \subset K$. The main theorem of Galois theory says that when K/F is a Galois extension there is a bijective correspondence between these fields and subgroups of $G(K/F)$.

The intermediate field corresponding to a subgroup H of $G(K/F)$ is the fixed field K^H. Further if L is a subfield of K then the group corresponding to it is $G(K/L)$.

Main Theorem of Galois Theory

Theorem 0.1.0.14 (The 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 from the set of subgroups of G to the set of intermediate fields $F \subset L \subset K$. It's inverse is

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

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

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

Proof. Later □

K and F are included among the intermediate fields. The group corresponding to K is $\{1\}$ and the group corresponding to F is G (the whole group).

0.2 TODO

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