Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

October 19, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Examples of Fields

We are now ready to begin the study of fields which will eventually lead us to Galois theory. Back when I took this class this was by far the coolest part of it. In the study of fields we will often consider pairs of field $F \subseteq K$. However unlike the case of groups where we often start with a group G and look at subgroups, in the case of fields we will be more interested in starting with a field F and looking as different extensions of F to fields K.

Extension Field

Definition 0.1.0.1. Let F be a field. If $F \subset K$ then we say K is a extension field of F.

The three most important classes of fields we will encounter are the following.

(1) **Number Fields:** A number field K is any subfield of $\mathbb{C}$.

As any subfield of $\mathbb{C}$ contains 1 it must also contain $\mathbb{Q}$. The number fields most commonly studied are those were every element is algebraic.

(2) **Finite Fields:** A field having only finitely many elements.

If K is finite then the kernel of the unique homomorphism $\mathbb{Z} \to K$ is a prime ideal since $\mathbb{Z}$ is infinite. So in particular K contains a subfield isomorphic to $\mathbb{Z}/(p) = \mathcal{F}_p$ for some prime p. And hence we can consider K as an extension of $\mathcal{F}_p$.

(3) **Function Fields:** Certain extensions of the field $\mathbb{C}(x)$.

Specifically, suppose we have an irreducible polynomial in $f \in \mathbb{C}[x,y]$ which is not a polynomial in x alone. Since it is irreducible in $\mathbb{C}[x,y]$ we know that it is irreducible in $\mathbb{C}[x][y]$ and hence, by the generalized Guass's Lemma we have that we have that f is also irreducible in $F = \mathbb{C}(x)$ the fraction field of $\mathbb{C}[x]$.

In particular this means that the idea $(f) \in F[y]$ is maximal. and hence $F[y]/(f)$ is a field.

0.2 Algebraic and Transcendental Elements

Similarly to the case of the complex numbers we define

Algebraic/Transcendental Extensions

Definition 0.2.0.2. Let F be a field. And let $\alpha \in K$

such that $K \supseteq F$. We say that α is algebraic over F if there is a polynomial over F which is satisfied by α. I.e. if

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + \alpha = 0$$

for some $a_0, \ldots, a_{n-1} \in F$

We say that α is transcendental over F if it is not algebraic over F.

We can think of the two possibilities in terms of the evaluation homomorphism. Specifically

Lemma 0.2.0.3. *Let $F \subset K$ be fields with $\alpha \in K$. Then if*

$$\varphi_\alpha : F[x] \to K \ f(x) \rightsquigarrow f(\alpha)$$

we have α is transcendental if and only if φ is injective. Or more specifically if the kernel of φ is 0.

Proof. Immediate □

Similarly we have

Irreducible Polynomial

Definition 0.2.0.4. Let $F \subset K$ be fields with $\alpha \in K$. Further let

$$\varphi_\alpha : F[x] \to K \ f(x) \rightsquigarrow f(\alpha)$$

We then know that $ker(\varphi_\alpha)$ is principle as $F[x]$ is a principle ideal domain. So in particular it is generated by a single element $f_\alpha(x) \in F[x]$.

But because K is a field we must have $f_\alpha(x)$ is irreducible (because otherwise K would have a zero divisor) Hence $f_\alpha(x)$ is the only irreducible polynomial in $(f_\alpha(x))$ (because every element of the ideal is a multiple of $f_\alpha(x)$) and we call f_α the Irreducible Polynomial for α over F.

It is important to note that the base field we are working over is crucial when determining the irreducible polyno-

mial of an element. Or for that matter even if a polynomial is irreducible. For example

Let $\alpha = \sqrt{i}$. Then the irreducible polynomial for α over $\mathbb{Q}$ is $x^4 + 1$. However, over $\mathbb{Q}[i]$ the irreducible polynomial is $x^2 - 1$. And what is more, over $\mathbb{Q}[i]$ $x^4 + 1$ is not irreducible as

$$x^4 + 1 = (x^2 + i)(x^2 - i)$$

$F(\alpha)$

Definition 0.2.0.5. Let $F(\alpha)$ be the smallest field containing both α and F. Similarly let $F(\alpha_1, \ldots, \alpha_n)$ be the smallest field containing $\alpha_1, \ldots, \alpha_n$ and F.

Connection between $F[\alpha]$ and $F(\alpha)$

Lemma 0.2.0.6. *Recall that $F[\alpha]$ is the ring*

$$\{\Sigma a_n \alpha^n : a_n \in F\}$$

and is the smallest ring containing both F and α. We then have $F(\alpha)$ is isomorphic to the field of fractions of $F[\alpha]$

In particular we have that if α is transcendental then $F[x] \to F[\alpha]$ is an isomorphism and hence $F(\alpha)$ is isomorphic to the field $F(x)$ of rational functions.

Proof. Immediate □

Notice that this means that if α and β are both transcendental over F then $F(\alpha) \cong F(\beta)$. For example this means that $\mathbb{Q}(\pi) \cong \mathbb{Q}(e)$ which is not at all obvious at first glance. However, if α and β are algebraic the case is very different.

Isomorphism of Equivalent Extensions

Theorem 0.2.0.7. *(a) Suppose that α is algebraic over*

F and let $f(x)$ be its irreducible polynomial over F. The map $F[x]/(f) \to F[\alpha]$ is an isomorphism and $F[\alpha]$ is a field. Thus $F[\alpha] = F(\alpha)$

(b) More generally let $\alpha_1, \ldots, \alpha_n$ be algebraic elements of a field extension K of F. Then $F[\alpha_1, \ldots, \alpha_n] = F(\alpha_1, \ldots, \alpha_n)$.

Proof. Let φ be the map which takes $f(x)$ to $f(\alpha)$. Since $f(x)$ generates $ker(\varphi)$, we know that $F[x]/(f)$ is isomorphic to the image of φ which is $F[x]$. Since f is irreducible we know that (f) is a maximal ideal and hence $F[x]/(f)$ is a field. Since $F(\alpha)$ is the smallest field containing $F[\alpha]$ we must have $F[x]/(f) = F(\alpha)$.

The second part follows from the first and is let as an exercise. □

Field Extensions as Vector Spaces

Theorem 0.2.0.8. *Let α be an algebraic over F and let $f(x)$ be its irreducible polynomial. Suppose $f(x)$ has degree n. Then $(1, \alpha, \ldots, \alpha^{n-1})$ is a basis for $F[\alpha]$ as a vector space over F*

Proof. This is a special case of the same theorem for rings which we have already seen. □

The following is one of the most important results concerning field extensions

Isomorphism of Equivalent Extensions

Theorem 0.2.0.9. *Let $\alpha \in K$ and $\beta \in L$ be algebraic elements of two extensions of F. There is an isomorphism of fields*

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

which is the identity on F and which sends $\alpha \rightsquigarrow \beta$ if and only i the irreducible polynomials for α and β

over F are equal.

Proof. Assume $f(x)$ is the irreducible polynomial for α and β over F. We therefore get two isomorphisms

$$\varphi : F[x]/(f) \to F[\alpha]$$

and

$$\psi : F[x]/(f) \to F[\beta]$$

The map $\sigma = \psi\varphi^{-1}$ is the required isomorphism sending α to β and preserving F.

Conversely, if such an isomorphism σ which sends α to β and is the identity on F exists, then $f(\alpha) = 0$ if and only if $f(\beta) = 0$ and so α, β have the same irreducible polynomial. □

Isomorphism of Field Extensions

Definition 0.2.0.10. Let K, K' be field extensions of

F. An isomorphism

$$\varphi : K \to K'$$

which restricts to the identity on F is called an Isomorphism of field exte

of an F-isomorphism

Field Extension Automorphisms and Roots of

Theorem 0.2.0.11. *Let $\varphi : K \to K'$ be an isomorphism of field extensions of F and let $f(x)$ be a polynomial with coefficients in F. Let α be a root of f in K and let $\alpha' = \varphi(\alpha)$ be its image in K'. Then α' is also a root of f.*

Proof. Say $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Then $\varphi(a_i) = a_i$ and $\varphi(\alpha) = \alpha'$. Since φ is a homomorphism, we can expand as follows

$$0 = \varphi(0) = \varphi(f(\alpha)) = \varphi(a_n \alpha^n + \cdots + a_1 \alpha + a_0)$$

$$= \varphi(a_n)\varphi(\alpha)^n + \cdots + \varphi(a_1)\varphi(\alpha) + \varphi(a_0) = a_n\alpha'^n + \cdots + a_1\alpha' + a_0$$

Hence α' is a root of $f(x)$. $\square$

0.3 TODO

- Flush out the outline of math.
- Come up with A BUNCH of examples (more than I can use) so that I don't run out of time.
- Go through Lang's book on the same topics.