Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

October 31, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Symbolic Adjunction of Roots

When dealing with subfields of $\mathbb{C}$ it is easy to construct field extensions of a field F by simply taking an element α of $\mathbb{C}$ and looking at the smallest field containing F and α.

However, when we are looking at finite fields and function fields we find that they are not subfields of some nice overarching structure. As such we need to consider other ways of adjoining elements.

The way we are going to do this is to use the method of adjoining a root of a polynomial $f(x) \in F[x]$ which was originally developed for rings.

Recall that if R is a ring and $f(x) \in R[x]$ then to adjoin a root of $f(x)$ means taking the field $R[x]/(f(x))$. We then naturally have a homomorphism

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

which takes x to an element such that $f(\varphi(x)) = 0$.

However, we are going to be interested in not only having $R[x]/(f(x))$ be a ring, but also being a field.

But we then have the following theorem

Field Iff Irreducible Kernel

Theorem 0.1.0.1. *Let F be a field. Let $F' = F[x]/I$. Then $I = (f)$ for some $f \in F[x]$ and F' is a field if and only if the (f) is irreducible.*

Proof. We know that $F[x]$ is a PID and hence I is of the above form. But we also know that $g \in F[x]$ divides

$f \in F[x]$ is the same as saying that $(g) \supset (f)$. Hence (f) is maximal if and only if f is irreducible. So in particular F' is a field if and only if f is irreducible. □

Root in Polynomial Ring

Corollary 0.1.0.2. *Let F be a field and let $f \in F[x]$ be irreducible. Then $K = F[x]/(f)$ is a field extension of F and the residue of x is a root of f in K.*

Proof. We know that the map $F \to K$ which is the identity on F is injective because F is a field. K is a field extension of F. That the residue of x is a root of f is immediate. □

Linear Factorization of Polynomial

Theorem 0.1.0.3. *Let F be a field and let $f(x)$ be a monic polynomial in $F[x]$ of positive degree. Then there is a field extension K of F such that $f(x)$ factors into linear factors over K.*

Proof. We use induction on the degree of f. The first case is that f has a root α in F so $f(x) = (x - \alpha)g(x)$ for some polynomial $g(x)$. I so we replace $f(x)$ by $g(x)$ and we are done.

Otherwise we choose an irreducible factor $g(x)$ of $f(x)$. By the previous lemma there is a field extension of F, call it F_1 in which $g(x)$ has a root α. We replace F by F_1 and thereby reduce to the first case. □

When we have a field extension K of a field F there is a relationship between their polynomial rings. Here are some of the most important facts about this relationship.

Division in Field Extensions

Theorem 0.1.0.4. *Let $f, g \in F[x]$ and let K be a field extension of F.*

(a) Division with remainder of g by f gives the same

answer whether carried out in $F[x]$ or in $K[x]$.

(b) f divides g in $K[x]$ if and only if f divides g in $F[x]$.

(c) The monic greatest common divisor d of f, g is the same wether computed in $K[x]$ or in $F[x]$.

(d) If f and g have a common root in K, then they are not relatively prime in $F[x]$. Conversely if f and g are not relatively prime in $F[x]$ then there exists an extension field L in which they have a common root.

(e) If f is irreducible in $F[x]$ and f and g have a common root in K then f divides g in $F[x]$.

Proof. Part (a):

Carry out division in $F[x]$: $g = fq + r$. This equation also holds in $K[x]$ which is a bigger ring. And, further division by f is not possible as r has degree $< f$.

Part (b):

This is the case that the remainder is zero.

Part (c):

Let d, d' denote the monic greatest common divisor of f and g in $F[x]$ and in $K[x]$. Then d is also a common divisor in $K[x]$. So d divides d' in $K[x]$ (by the definition of d'). In addition we know that d has the form $d = pf + qg$ for some elements $p, q \in F[x]$. Since d' divides f and g, it divides $pf + qg = d$ too. Thus d, d' are associates in $K[x]$. And, being monic, are equal.

Part (d):

Let α be a common root of f and g in K. Then $x - \alpha$ is a common divisor of f and g in $K[x]$. So their greatest common divisor in $K[x]$ is not 1. By (c) it is not 1 in

$F[x]$ either. Conversely if f and g have a common divisor d of degree > 0 then we know that d has a root in some extension field L. This root will be common to both f and g.

Part (e):

If f is irreducible, then its only divisors in $F[x]$ are 1, f, and their associates. Part (d) tells us that the greatest common divisor of f and g in $F[x]$ is not 1 and is therefore f. □

Next we want to consider derivatives.

Definition of Derivative

Definition 0.1.0.5. Let F be a field and let $f \in F[x]$. If

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

then we define

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} \cdots a_1$$

Where we interpret n as the image of $n \in \mathbb{Z}$ under the unique ring homomorphism $\mathbb{Z} \to F$.

It can be shown that things like the product rule hold for these formal derivatives.

While taking the derivative is an algebraic procedure there is no reason to believe that it has much significance. However we see that it in fact is very useful for recognizing multiple roots.

Multiple Roots and Derivative

Lemma 0.1.0.6. *Let F be a field and let $f(x) \in F[x]$. Let $\alpha \in F$ be a root of $f(x)$. Then α is a multiple root, i.e. that $(x-\alpha)^2$ divides $f(x)$ if and only if α is a root of $f(x)$ and of $f'(x)$.*

Proof. If α is a root of $f(x) \in F[x]$ then $x - \alpha$ divides f : $f(x) = (x - \alpha)g(x)$. Then α is a root of g if and only if it is a multiple root of f. By the product rule or differentiation

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

Substituting $x = \alpha$ shows that $f'(\alpha) = 0$ if and only if $g(\alpha) = 0$. □

Derivatives, Multiple Roots, Field Extensions

Theorem 0.1.0.7. *Let $f(x) \in F[x]$ where F is a field. Then there exists a field extension K of F in which f has a multiple root if and only if f and f' are not relatively prime.*

Proof. If f has a multiple root in K then f and f' have a common root in K by the previous lemma and so they

are not relatively prime in K. Hence they are not relatively prime in F either. Conversely, if f and f' are not relatively prime then they have a common root in some field extension K, hence f has a multiple root there. $\square$

Multiple Roots and Irreducible Polynomials

Theorem 0.1.0.8. *Let f be an irreducible polynomial in $F[x]$. Then f has no multiple roots in any field extension of F unless the derivative f' is the zero polynomial. In particular if F has characteristic 0, then f has no multiple root.*

Proof. By the previous proposition, we must show that f and f' are relatively prime unless f' is the zero polynomial. Since f is irreducible the only way it can have a non-constant factor in common with another polynomial g is for f to divide g. Hence if f divides g then

$\deg(g) \geq \deg(f)$ or else $g = 0$. Now the degree of the derivative f' is less than the degree of f. So f and f' have no non-constant common factor unless $f' = 0$. And, in a field of characteristic 0 the derivative of a constant polynomial is not zero. □

Notice however that there are polynomials which are not 0 but whose derivative is identically zero. Consider the following polynomial in the field $\boldsymbol{F}_5$

$$x^{15} + ax^{10} + bx^5 + c$$

it's derivative is

$$15x^{14} + 10ax^9 + 5bx^4 = 0$$

for any a, b, c. However whether or not this polynomial is irreducible depends on a, b and c.

0.2 Transcendental Extensions

We saw that if we have two elements x, y of a field extension K of F such that both elements are transcendental

over F then the field extensions $F(x) \cong F(y)$. Now we will ask the question what does $F(x, y)$ look like.

Definition Algebraically Dependent

Definition 0.2.0.9. Let K be a field extension of F. Let $\alpha_1, \ldots, \alpha_n$ be a sequence of elements of K. We say that $\alpha_1, \ldots, \alpha_n$ are Algebraically Dependent if there is a polynomial $f \in F[x_1, \ldots, x_n]$ such that $f(\alpha_1, \ldots, \alpha_n) = 0$. We say $\alpha_1, \ldots, \alpha_n$ are algebraically independent otherwise.

Lemma 0.2.0.10. *Let $F \subseteq K$. $\alpha_1, \ldots, \alpha_n$ are algebraically independent if and only if the substitution map $\varphi : F[x_1, \ldots, x_n] \to K$ which takes $f(x_1, \ldots, x_n)$ to $f(\alpha_1, \ldots, \alpha_n)$ has $ker(\varphi) = 0$.*

Proof. Immediate □

Corollary 0.2.0.11. *If $\alpha_1, \ldots, \alpha_n$ are algebraically independent over F then $F(\alpha_1, \ldots, \alpha_n)$ is isomorphic*

to $F(x_1, \ldots, x_n)$ the field of rational functions in $x_1, \ldots, x_n$.

Proof. Immediate □

Definition of Pure Transcendental Extension

Definition 0.2.0.12. An extension o the form $F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are algebraically independent is called a Pure Transcendental extension.

Definition of Transcendence Basis

Definition 0.2.0.13. A transcendence basis for a field K of F is a set of elements $\alpha_1, \ldots, \alpha_n$ such that K is algebraic over $F(\alpha_1, \ldots, \alpha_n)$

Uniqueness of Transcendence Degree

Theorem 0.2.0.14. *Let $(\alpha_1, \ldots, \alpha_m)$ and $(\beta_1, \ldots, \beta_n)$ be elements in a field extension K of F which are algebraically independent. If K is algebraic over $F(\beta_1, \ldots, \beta_n)$*

then $m \leq n$ and $(\alpha_1, \ldots, \alpha_m)$ can be completed to a transcendence basis for K by adding $n - m$ many of the β_i.

Theorem 0.2.0.15. *********Theorem 13.8.3. MAYBE GIVE AS HOMEWORK *********

Corollary 0.2.0.16. *Any two transcendence basis for a field extension $F \subseteq K$ have the same number of elements.*

Proof. Immediate. □

As an example notice that $F(x_1, \ldots, x_m)$ is not isomorphic to $F(x_1, \ldots, x_n)$ if $n \neq m$ because they have different number of elements in their transcendence basis.

Consider $f, g \in F(x)$. We know the transcendence degree of $F(x)$ over F is 1. Hence there must be a non-zero $\varphi \in F[y, z]$ such that $\varphi(f, g) = 0$. So in particular any two rational functions are algebraically dependent over F.

0.3 TODO

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