Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

November 2, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Finite Fields

Finite Fields We will now describe all finite fields. First note that we have already seen that if K is a finite field then it is a field extension of some finite field $\mathcal{F}_p$. So in particular K can be considered as a finite dimensional vector space over $\mathcal{F}_p$. Lets say K has dimension r as an $\mathcal{F}_p$ vector space. Then K has p^r many elements.

Order

Definition 0.1.0.1. We say that $q = p^r = |K|$ is the order of a field K. When dealing with finite fields p will always be a prime and q will be the order of the field we are talking about.

Fields with $q = p^r$ elements are often denoted $\mathcal{F}_q$.

We will show that all finite fields with the same number of elements are isomorphic. However, the isomorphism will not be unique when $r > 1$. Here are the main facts about finite fields.

Main Properties

Theorem 0.1.0.2. *Let p be a prime and let $q = p^r$ be a power of p with $r \geq 1$. Let K be a field with order q.*

(a) There exists a field of order q

(b) Any two fields of order q are isomorphic.

(c) Let K be a field of order q. The multiplicative group $K^\times$ of nonzero elements of K is a cyclic group of order $q - 1$.

(d) The elements of K are roots of the polynomial

$x^q - x$. This polynomial has distinct roots and it factors into linear factors in K

(e) Every irreducible polynomial of degree r in $\mathcal{F}_p[x]$ is a factor of $x^q - x$. The irreducible factors of $x^q - x$ in $\mathcal{F}_p[x]$ are precisely the irreducible polynomials in $\mathcal{F}_p[x]$ whose degree divides r.

(f) A field K of order q contains a subfield of order $q' = p^k$ if and only if k divides r.

This proof isn't especially hard, but as it has a lot of parts it will take some time. As such we will first look at some consequences.

Corollary 0.1.0.3. *Let K be a finite field. Then there is an element $a \in K$ such that for all $b \in K, b \neq 0$ there is an $n \in \omega$ such that $a^n = b$.*

Proof. Immediate from part (c). □

As an example consider $\mathcal{F}_7$ and consider the powers of 3. We have that they are $\{1, 3, 2, 6, 4, 5\}$ which are all the non-zero elements.

Definition of Generator

Definition 0.1.0.4. A generator for the cyclic group $\mathcal{F}_p^{\times}$ is called an primitive element modulo p.

Which residues mod p are primitive is not well understood, but for small p can be determined by trial and error.

We how have two different ways to list all the non-zero elements of $\mathcal{F}_p$.

$$\mathcal{F}_p^{\times} = \{1, 2, \ldots, p-1\} = \{1, v, v^2, \ldots, v^{p-1}\}$$

where v is a primitive element modulo p.

Notice that the additive group governing a field $\mathcal{F}_p$ is also cyclic (of order p). However, it is the distribution law which fits them together in an interesting way.

We will now prove the theorem

Proof. **Proof Part D** Part (d):(Assuming Part (c))

Let K be a field of order q. The multiplicative group $K^\times$ has order $q-1$. Therefore the order of any element $\alpha \in K^\times$ divides $q-1$. So in particular $\alpha^{q-1} = 1$. This means that α is a root of the polynomial $x^{q-1} - 1 = 0$. The remaining element of K is 0 which is a root of the polynomial x. So every element is a root of $x^q - x$.

Since the polynomial $x^q - x$ has q distinct roots it must factor into

$$x^q - x = \prod_{\alpha \in K} (x - \alpha)$$

Proof Part C Part (c):

By an nth root of unity in a field F we man an element α whose nth power is 1. Thus α is an nth root of unity if and only if it is a root of the polynomial

$$x^n - 1$$

or if and only if it's order, as an element of $F^\times$ divides n. Notice that every element of $F^\times$ is a $q-1$th root of unity where q is the order of F

Finite Subgroups of the Multiplicative Group

Theorem 0.1.0.5. *Let F be a field and let H be a finite subgroup of the multiplicative group $F^\times$, of order*

n. Then H is a cyclic group and it consists of all the nth roots of unity of F

Proof. If H has order n then the order of an element α of H divides n so α is an nth root of unity and hence a root of $x^n - 1$. This polynomial has at most n roots so there aren't any other roots in F. It follows that H is the set of all nth roots of unity in F.

To see that H is cyclic we use the structure theorem of abelian groups which tells us that H is isomorphic to a direct product of groups

$$H \cong \mathbb{Z}/(d_1) \oplus \cdots \oplus \mathbb{Z}/(d_k)$$

where $d_1|d_2, d_2|d_3, \ldots$ and $n = d_1 \cdots d_k$ The order of any element of this product divides d_k because d_k is a common multiple of all the d_i's. So every element of H is a root of $x^{d_k} - 1$. This polynomial has at most d_k roots in F. But H contains n-elements and as $n = d_1 \cdots d_k$ the only possibility is $n = d_k$ and $1 = d_i$ and hence H is cyclic. □

Proof Part A Part (a):

We need to prove the existence of a field with q elements. Since we have already proved part (d) of the theorem we know that the elements of a field of order q are roots of the polynomial $x^q - x$. Also there exists a field L containing $\mathcal{F}_q$ in which this polynomial (or any given polynomial) factors into linear factors. The natural thing to try is to take such a field L and hope for the best– that the roots of $x^q - x$ form a subfield K of L. We get this by the next proposition

Polynomial $x^q - x$

Theorem 0.1.0.6. *Let p be a prime and let $q = p^r$.*

(a) The polynomial $x^q - x$ has no multiple root in any

field L of characteristic p.

(b) Let L be a field of characteristic p and let K be the set of roots of $x^q - x$ in L. Then K is a subfield of L.

Proof. **Proof Part A** Part a:

The derivative of $x^q - x$ is $qx^{q-1} - 1$ which in characteristic p is just -1. Since the constant polynomial -1 has no root, $x^q - x$ has no multiple root.

Proof Part B Part b:

Let $\alpha, \beta \in L$ be roots of $x^q - x$. We have to show that $\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ are all roots of $x^q - x$.

To see this observe that if γ is a root of the polynomial if and only if $\gamma^q = \gamma$. So we obviously have $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$ and similarly $(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$. For the case of the sum we need another theorem.

$$\boxed{(x+y)^q = x^q + y^q}$$

Theorem 0.1.0.7. *Let L be a field of characteristic p, and let $q = p^r$. Then in the polynomial ring $L[x, y]$, we have $(x+y)^q = x^q + y^q$*

Proof. Case 1: $p = q$

We expand $(x+y)^p$ in $\mathbb{Z}[x, y]$ and we see by the binomial theorem

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p$$

But $\binom{p}{r}$ is an integer, and if $0 < r < p$ then it is divisible by p. It follows that the map $\mathbb{Z}[x, y] \to L[x, y]$ sends every monomial except x^p, y^p to zero and hence $(x+y)^p = x^p + y^p$ in L.

Case 1: $p^{r+1} = q$ where we know the theorem holds for

$q' = p^r$

We therefore have $(x+y)^q = ((x+y)^{q'})^p = (x^{q'}+y^{q'})^p = (x^{q'p} + y^{q'p}) = x^q + y^q$. □

Now to finish the proof of the previous theorem we we can conclude that $(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta$ and we are done. (The case of $\alpha - \beta$ is done by substituting $-\beta$ for β). □

Proof Part B Continued

Part (b) continued:

Let K and K' be fields of order q and let α be a generator of the cyclic group $K^\times$. Then K is certainly generated as a field extension of $F - \mathcal{F}_p$ by the element $\alpha : K = F(\alpha)$. Let $f(x)$ be the irreducible polynomial of α over F. So $K \cong F[x]/(f)$. So α is a root of two polynomials, $f(x)$ and $x^q - x$.

Now lets go over to the second field K' where $x^q - x$ factors into linear factors. In this field f must have a root $\alpha' \in K'$. But then $K \cong F[x]/(f) \cong F(\alpha')$. And since K and K' have the same order, $F(\alpha') = K'$ and hence K and K' are isomorphic.

Proof Part E

Part (e):

Let $f(x)$ be an irreducible polynomial of degree f in $F[x]$ where $F = \mathcal{F}_p$ as before. It has a root α in some field extension L of F and the subfield $K = F(\alpha)$ of L has degree r over F. Therefore K has order $q = p^r$ and by part (d) of this theorem α is also a root of $x^q - x$. Since f is irreducible it divides $x^q - x$ as required.

In order to prove the same thing for irreducible polynomials whose degree k divides r it suffices to prove the following lemma

Lemma 0.1.0.8. *Let k be an integer dividing r, say $r = ks$, and let $q = p^r$, $q' = p^k$. Then $x^{q'} - x$ divides*

$x^q - x$.

Proof. We will use the identity

$$y^d - 1 = (y-1)(y^{d-1} + \cdots + y + 1)$$

Substituting $q' = y$ and $d = s$ shows that $q' - 1$ divides $q - 1 = q'^s - 1$. Hence if we then let $x^{q'-1} = y$ and $d = (q-1)/(q'-1)$ we find $x^{q'-1} - 1$ divides $x^{q-1} - 1$ and hence $x^{q'} - x$ divides $x^q - x$. □

So we have every irreducible polynomial whose degree divides r is a factor of $x^q - x$. On the other hand if f is irreducible and if its degree k doesn't divide r then since $[K : F] = r, f$ doesn't have a root in K and hence f doesn't divide $x^q - x$. Part (f):

If k does not divide r then $q = p^r$ is not a power of $q' = p^k$ so a field of order q can not be an extension of a field of order q'. On the other hand if K does divide r then by the previous lemma and part (d) of the theorem we see that the polynomial $x^{q'} - x$ has all its roots in a field K of order q. Hence by a previous result K contains a field with q' elements. $\square$

0.2 Algebraically Closed Fields

Algebraically Closed Fields **Definition of A**

Definition 0.2.0.9. A field F is algebraically closed if every polynomial $f(x) \in F[x]$ has a root in F.

Fundamental Theorem of Algebra

Theorem 0.2.0.10 (Fundamental Theorem of Algebra)**.** *Every nonconstant polynomial with complex coefficients has a complex root.*

Note that if F is algebraically closed then every nonconstant polynomial has a linear factor and hence the only irreducible polynomials are those of the form $x - \alpha$

for α in the field.

Hence every polynomial is a product of linear factors and there is no algebraic extension of F other than itself (if F is algebraically closed).

Algebraic Closure

Definition 0.2.0.11. Let F be a field. $\overline{F}$ is an algebraic closure of F if

- $\overline{F}$ is algebraically closed
- $\overline{F}$ is algebraic over F.

Corollary 0.2.0.12. *Let F be a subfield of $\mathbb{C}$. Then the subset $\overline{F}$ of $\mathbb{C}$ consisting of all numbers algebraic over F is an algebraic closure of F.*

Proof. We have already seen that $\overline{F}$ is a field. To see that $\overline{F}$ is algebraically closed let $f(x) \in F[x]$ be a non-constant polynomial. Then $f(x)$ has a root $\alpha \in \mathbb{C}$ and

$\overline{F}(\alpha)$ is algebraic over F. Hence, as $\overline{F}$ is algebraic over F we see that α is algebraic over F and hence in $\overline{F}$ □

Isomorphism of Algebraically Closed Fields.

Theorem 0.2.0.13. *Every field F has an algebraic closure and if K_1, K_2 are algebraic closures of F there is an isomorphism $\varphi : K_1 \to K_2$ which is the identity map on F.*

Proof. Lets first consider the case where F is a finite field. We will construct this as a sequence of fields. Let $r_1, r_2, \ldots$ be a sequence of numbers such that

- r_i divides r_{i+1}
- Every integer n divides some r_i.

(for example take $r_i = i!$.)

We then set $q_i = p^{r_i}$ and $F_i = \mathcal{F}_{q_i}$. It follows that F_{i+1}

contains a subfield isomorphic to F_i so we can build a tower of fields $F_1 \subset F_2 \subset \cdots$. Let $\overline{F}$ be the union of this chain of fields. Then the conditions on r_i tell us that every finite field $\mathcal{F}_q$ where $q = p^r$ is isomorphic to a subfield of some F_i and hence a subfield of $\overline{F}$. This field is hence an algebraic closure of $\overline{F}$.

We can then do the general case similarly by adjoining successive roots to our fields until every function can be factored and then using Zorns lemma.

*******THE ISOMORPHISM PART IS HOMEWORK
******* □

Corollary 0.2.0.14. *Let $\overline{F}$ be an algebraic closure of F, and let K be any algebraic extension of F. Then there is a subextension $K' \subset \overline{F}$ which is isomorphic to K.*

Proof. Immediate □

Proof Fundamental Theorem of Algebra

Fundamental Theorem of Algebra. To show $f(x_0) = 0$ it is enough to show that $|f(x_0)| = 0$. The existence of such a value for $x_0 \in \mathbb{C}$ is proved as follows.

Lemma 0.2.0.15. *Let $f(x)$ be a nonconstant polynomial and let $x_0 \in \mathbb{C}$ be a point at which $f(x_0) \neq 0$. Then $|f(x_0)|$ is not the minimum value of $|f(x)|$.*

Proof. First note that the polynomial $x^k - c$ has a root for all $c \in \mathbb{C}$. A nonnegative real f has a real kth root because the continuous function x^k, which is zero at 0 and large when x is a large real number takes on all real values ≥ 0 by the intermediate value theorem. We write the complex number c in the form $re^{i\theta}$ where $r = |c|$ and $\theta = arg(c)$. Let s be a real kth root of r. Then the required kth root of c is $se^{i\theta/k}$

Now let $f(x)$ be a nonconstant polynomial and let $x_0 \in \mathbb{C}$ be a point at which $f(x_0) \neq 0$. It is convenient to normalize f. We make a change of variable, replacing x with $x + x_0$ to shift the point in question to the origin. So now $x_0 = 0$. We also multiply $f(x)$ by $f(0)^{-1}$ to get $f(0) = 1$.

So it suffices to show that 1 is not the minimum value of $|f(x)|$.

Let k denote the lowest nonzero power of x occurring in f so that

$$f(x) = 1 + ax^k + (\text{ terms of degree } > k)$$

Let α be a kth root of $-a^{-1}$. We make a final change of variable replacing x by αx. Then f takes the form

$$f(x) = 1-x^k + \text{ (higher degree terms) } = 1-x^k+x^{k+1}g(x)$$

for some polynomial $g(x)$. For small positive real x the triangle inequality shows that

$$|f(x)| \leq |1-x^k|+|x^{k+1}g(x)| = 1-x^k+x^{k+1}g(x) = 1-x^k(1-x|g(x))$$

Since $x|g(x)|$ is small for small x the term $x^k(1-x|g(x)|)$ is positive when x is a sufficiently small real number. For such x $|f(x)| < |f(0)|$. □

Lemma 0.2.0.16. *Let $f(x)$ be a complex polynomial. Then $|f(x)|$ takes on a minimum value at some point $x_0 \in \mathbb{C}$.*

Proof. We may assume that f is non a constant polynomial. For large x $f(x)$ is also large

$$|f(x)| \to \infty \text{ as } |x| \to \infty$$

To prove this the constant term of f is irrelevant so we may suppose it is 0. Then $f(x)$ is divisible by $x : f(x) = xg(x)$. By induction on the degree the assertion is true for $g(x)$ or else $g(x)$ is constant. Hence it follows for $f(x)$ as well.

Now since $f(x)$ is large for large x the greatest lower bound m of $|f(x)|$ is a continuous function and hence the greatest lower bound on the whole complex plane is also the greatest lower bound in a sufficiently large disc $|x| \leq r$. And since the disk is compact and $|f(x)|$ is continuous we see that it takes on a minimum value. $\square$

$\square$

0.3 TODO

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