

**Announcements:**

1. Lecture notes #13-16 are online.
2. Next Tuesday Oct 29th we do a review for the midterm on the 31st.
3. Syllabus for the midterm Chapters 1, 3, § 2.1,4.1,4.2.
4. HW #3 II.1.3, II.1.9, compute  $(x + 1)^{-1} \in \mathbf{F}_{5^3}$ . Please try but don't turn in. Solutions will be posted.

**Topics for today:**

1. Finite Field Construction contd.
2. Field Arithmetic
3. Construction of an extension field
4. Uniqueness of finite fields

**1. Finite Field Construction contd.**

We'll use the standard notation  $\mathbf{F}_p$  to denote the finite field of  $p$  elements consisting of the set  $\mathbf{Z}/p\mathbf{Z}$  with the field operations being modular addition and multiplication.

Last time we started to construct a field with 25 elements starting out with  $\mathbf{F}_5$  and the polynomial  $x^2 - 2$  which is irreducible over  $\mathbf{F}_5$ . Recall to construct  $\mathbf{F}_5 = \mathbf{Z}/5\mathbf{Z}$  we place all integers into 5 congruence classes and two integers are equivalent or in the same class iff their difference is divisible by 5. Similarly for  $\mathbf{F}_{5^2}$ , we place elements in  $\mathbf{F}_5[x]$  (which are polynomials with coefficients in  $\mathbf{F}_5$ ) into 25 equivalence classes and two polynomials are equivalent iff their difference is divisible by  $x^2 - 2$ .

Say  $f, g \in \mathbf{F}_5[x]$ , then  $f \equiv g \pmod{x^2 - 2} \Leftrightarrow (x^2 - 2) \mid (f - g)$ .

We claim that the 25 congruence classes form a field of 25 elements and we denote it by  $\mathbf{F}_5/(x^2 - 2)\mathbf{F}_5$  or more often just as  $\mathbf{F}_5/x^2 - 2$ . Next we undertake a more general finite field construction and prove that Euclid's algorithm can be used to find multiplicative inverses in the new field.

**Claim 1.** If  $h \in \mathbf{F}_p[x]$  and  $0 \neq \deg h < \deg f$  then  $hg \equiv 1 \pmod f$  for some  $g \in \mathbf{F}_p[x]$ .

**Proof.**  $hg \equiv 1 \pmod f \Rightarrow hg = 1 + ft \Rightarrow hg - ft = 1$  for some  $t \in \mathbf{F}_p[x]$ . It seems like Euclid's gcd algorithm might help us out. And it does as the *Division Thm* holds in  $\mathbf{F}_p[x]$ .

Let's talk about the extended gcd algorithm more generally in  $\mathbf{k}[x]$ , where  $\mathbf{k}$  is a field. Let  $A(x), B(x) \in \mathbf{k}[x]$ . By the Division Thm  $A(x) = q(x)B(x) + r(x)$  with  $\deg r(x) < \deg B(x)$ . As the set of common divisors of  $A(x)$  and  $B(x)$  is the same as the set of common divisors of  $B(x)$  and  $r(x)$ ,  $\gcd(A(x), B(x)) = \gcd(B(x), r(x)) = g(x)$ . Say  $g(x) = s(x)B(x) + t(x)r(x)$  where  $s(x), t(x) \in \mathbf{k}[x]$ . Replacing  $r(x)$  by  $A(x) - q(x)B(x)$ , we have  $c(x) = s(x)B(x) + t(x)(A(x) - q(x)B(x)) = t(x)A(x) + (s(x) - t(x)q(x))B(x)$ .

Switching back to our finite field discussion,  $0 \neq h, \deg h < \deg f$  and  $f$  is irreducible implies that  $\gcd(f, h)$  is a constant, that is an element of  $\mathbf{k}$ . Otherwise if  $\deg \gcd(f, h) > 0$  then we have a non-trivial divisor of irreducible polynomial  $f$ , which is a contradiction.

Hence if  $\gcd(f, h) = c \in \mathbf{F}_p$ , then the extended gcd gives us  $sf + th = c$  for some  $s, t \in \mathbf{F}_p[x]$  and multiplying by the  $c^{-1}$  this in turn implies  $th \equiv 1 \pmod f$  and the existence of an inverse of  $h \pmod f$ .  $\diamond$

**Claim 2.**  $\mathbf{F}_p[x]/f$  is a field of  $p^d$  elements where  $f \in \mathbf{F}_p[x]$  is an irreducible polynomial of degree  $d$ .

**Proof.** Let  $f \in \mathbf{F}_p[x]$  be an irreducible polynomial over  $\mathbf{F}_p$  (that is there is no smaller degree non-constant polynomial in  $\mathbf{F}_p[x]$  which divides  $f$ ).

Let  $\mathbf{F}_p[x]/f$

= the set of equ. classes of  $\mathbf{F}_p[x]$  wrt the "modulo  $f$ " equ. relation

=  $\{h \in \mathbf{F}_p[x] \mid \deg h < \deg f = d\}$ .

Observe that this set is a vector space over  $\mathbf{F}_p[x]$  and there is a natural choice of basis, namely,  $\{1, x, \dots, x^{d-1}\}$ . If  $d$  is the degree of  $f$  then there are exactly  $p^d$  polynomials in the  $\mathbf{F}_p[x]/f$ .

Any polynomial of degree less than  $d$  can be written as a linear combination of the basis elements  $1, x, \dots, x^{d-1}$  with  $\mathbf{F}_p$  being the scalars. The

dimension of  $\mathbf{F}_p[x]/f$  over  $\mathbf{F}_p$  is  $d$  and is closed under  $+, * \bmod f$ ,  $0, 1$  are the identities wrt  $+, * \bmod f, \dots$ . The only thing which is not clear is that every non-zero element has a multiplicative inverse which follows by Claim 1. So this ends our proof of  $\mathbf{F}_p/f$  is a finite field of  $p^d$  elements.  $\diamond$

**Example.** And back to our favourite example with  $p = 5$  and  $f = x^2 - 2$ . What is the inverse of  $(x + 2)$  in  $\mathbf{F}_{5^2} = \mathbf{F}_5/x^2 - 2$ ?

$$x^2 - 2 = (x + 2)(x - 2) + 2 \Rightarrow 2^{-1}(x^2 - 2) = 2^{-1}(x + 2)(x - 2) + 1 \Rightarrow (x + 2)(x + 4) \equiv 1 \bmod x^2 - 2 \Rightarrow (2x - 4) = (x + 2)^{-1} \bmod x^2 - 2$$

**Recipe** for constructing a finite field of  $p^d$  elements

1. start with  $\mathbf{F}_p$
2. find an irreducible polynomial  $f \in \mathbf{F}_p[x]$  of degree  $d$
3.  $\mathbf{F}_p/f =$  all polynomials in  $\mathbf{F}_p[x]$  with degree  $\leq d - 1$  is our field of  $p^d$  elements with operations  $+, *$  modulo  $f$

Two different irreducible polynomials of same degree over  $\mathbf{F}_p$  will both give rise to fields which will have  $p^d$  elements. We'll later prove that the any two finite fields of with the same order are infact the same (isomorphic). But first we make a digression into roots of polynomials.

Flt says if  $p$  is a prime then  $a^p \equiv a \bmod p$  for all  $a \in \mathbf{Z}$ . A restatement of the above is that each  $\alpha \in \mathbf{F}_p$  is a root of the polynomial  $x^p - x$ . We discussed last time that a polynomial of degree  $d$  in  $\mathbf{F}_p[x]$  has atmost  $d$  roots in  $\mathbf{F}_p$ . Hence in the case of the  $x^p - x$  all the  $p$  roots of the polynomial are in  $\mathbf{F}_p$  itself.

More generally suppose  $\mathbf{k}$  is a finite field of characteristic  $p$  and  $|\mathbf{k}| = p^d = q$ . We know that  $\mathbf{k}^* = \mathbf{k} - \{0\}$  is a group and  $|\mathbf{k}^*| = q - 1$ . By Lagrange's Theorem for all  $\alpha \in \mathbf{k}^*$ ,  $order(\alpha) | q - 1$  hence  $\alpha^{q-1} = 1$  and so  $\alpha^q = \alpha$  holds for all  $\alpha \in \mathbf{k}$ . So all elements in  $\mathbf{k}$  are roots of the polynomial  $x^q - x$  and a polynomial of degree  $q$  can have atmost  $q$  roots in  $\mathbf{k}$ . Therefore the roots of  $x^q - x$  are all the elements of  $\mathbf{k}$ . Next we'll prove that  $\mathbf{k}^*$  is a cyclic group and hence an equivalent statement would be that the  $q - 1$  non-zero roots of  $x^q - x$  form a cyclic group.

**Thm.** Let  $\mathbf{k}$  be a finite field of  $q = p^d$  elements where  $p$  is prime and  $d \in \mathbf{Z} > 0$ . Then  $\mathbf{k}^*$  is a cyclic group of order  $q - 1$  and has  $\phi(q - 1)$  generators.

**Proof.** Suppose  $\alpha \in \mathbf{k}^*$  and  $d = \text{order}(\alpha)$ , that is  $\alpha^d = 1$  then by Lagrange's theorem  $d|q-1$ .

Consider the polynomial  $x^d - 1 \in \mathbf{k}[x]$ . It has at most  $d$  roots in  $\mathbf{k}$ . But on the other hand all  $d$  elements in  $\langle \alpha \rangle$  are roots of  $x^d - 1$ . Therefore the set of roots of  $x^d - 1$  in  $\mathbf{k}$  is  $\langle \alpha \rangle$ .

Suppose  $\beta \in \mathbf{k}^*$  also has order  $d$ . Then by the above argument we reach the conclusion that the set of roots of  $x^d - 1$  in  $\mathbf{k}$  is  $\langle \beta \rangle$ . So  $\langle \alpha \rangle = \langle \beta \rangle$ .

Say the set of elements in  $\mathbf{k}$  of order  $d$  is  $S_d$ . Then  $S_d = \phi(d)$  or  $0$  since  $d|q-1$ . Hence  $q-1 = \sum_{d|q-1} S_d \leq \sum_{d|q-1} \phi(d) = q-1$ . The last equality is the result of the identity we discussed in the initial part of this course:  $n = \sum_{d|n} \phi(d)$ .

Can any of the  $S_d$  be  $0$ ? No! since if that is true then  $\sum_{d|q-1} S_d < \sum_{d|q-1} \phi(d)$ . So  $S_d = \phi(d)$  for all  $d|q-1$ . To prove that  $\mathbf{k}^*$  is cyclic it is enough to prove that there is an element of order  $q-1$ . So taking  $d = q-1$  we have  $S_{q-1} = \phi(q-1)$ . Hence there are  $\phi(q-1)$  many generators for the cyclic group  $\mathbf{k}^*$ .  $\diamond$

### Remarks

1. Think of irreducible polynomials in  $\mathbf{F}_p[x]$  as analogies of primes in  $\mathbf{Z}$ .
2. Imagine working with the  $x^d + x + 1$  (supposing it is irreducible) instead of  $\sum_{i=0}^d a_i x^i$  with some ugly  $a_i$  as coefficients. The right choice of the irreducible polynomial makes computation a lot easier. Also  $\{1, x, \dots, x^d\}$  though the most natural basis need not be the most efficient basis to work with.
3. An important question to ask is: "Are we sure we can always find an irreducible polynomial of degree  $d$  over  $\mathbf{F}_p$ ?" We'll do this next time
4.  $\mathbf{F}_q^*$  is cyclic of order  $q-1$  with  $\phi(q-1)$  generators. How do you efficiently find a generator? Of course if  $\phi(q-1) \sim q-1$  then a very good proportion of  $\mathbf{F}_q^*$  has order  $q-1$ . How about checking if you have a generator aka primitive element? Primitivity is not easy to check.

**Recap** and some general facts.

To construct a field of  $q = p^d$  elements  $\mathbf{F}_q$  pick an irreducible polynomial  $f \in \mathbf{F}_p[x]$  of degree  $d$ . Addition and multiplication are straight forward and so is computing the additive inverse. For the multiplicative inverse as usual we use Euclid's algorithm.

Say  $\alpha, \beta \in \mathbf{F}_q$

- $\alpha^d = \alpha$  for all  $\alpha \in \mathbf{F}_q$ .
- The characteristic is  $p$  and so  $p\alpha = 0$ .
- $(\alpha + \beta)^p = \alpha^p + \beta^p$  for all  $\alpha, \beta \in \mathbf{k}$  since in the binomial expansion all the intermediate terms are divisible by  $p$ .
- $(\alpha\beta)^p = \alpha^p\beta^p$  due to commutativity.
- $(\alpha^p)^{-1} = (\alpha^{-1})^p$  since  $(\alpha^{-1})^p\alpha^p = \alpha^{-1} \dots \alpha^{-1}\alpha \dots \alpha = \alpha^{-1}\alpha \dots \alpha^{-1}\alpha = 1$  again due to commutativity.

The above actually says that the field automorphism given by raising an element to the  $p$ th power respects the group law.

## 2. Field Arithmetic

Last lecture we saw how to construct finite fields with the size of the field being the power of a prime. For example  $\mathbf{F}_{5^2} = \mathbf{F}_5[x]/x^2 - 2$ . We also pointed out that if you took a different irreducible polynomial but with the same degree you end up with the same field. For instance  $\mathbf{F}_{5^2} = \mathbf{F}[x]/x^2 + 2$ . Observe that we've been using the  $=$  sign to indicate that  $\mathbf{F}_{5^2}$  is the *only* field of 25 elements irrespective of how it is constructed and how the field elements look like. Today we will make progress in proving the uniqueness aspect.

**Thm.** For every  $d$  there exists a unique finite field  $\mathbf{F}_{p^d}$  upto isomorphism.

$\mathbf{F}_5[x]/x^2 - 2$  is a field where  $x^2 - 2$  splits, that is it is the smallest field containing the roots of  $x^2 - 2$  and  $\mathbf{F}_5[x]/x^2 - 2 = \{[ax + b] \mid a, b \in \mathbf{F}_5\}$

We use  $[ ]$  to indicate that the elements of the field are really congruence classes and the  $ax+b$  denotes that canonical representatives of the congruence classes are given by linear polynomials and constants (elements in  $\mathbf{F}_p$ ).

Let's look at some field arithmetic examples.

- $[x] + [1] = [x + 1]$  since  $x + 1 \equiv x + 1 \pmod{x^2 - 2}$ .
- $[x].[x] = [x^2] = [2]$  since  $x.x \equiv x^2 \equiv 2 \pmod{x^2 - 2}$ .
- $[x^2 + x - 2] = [x]$ .

The elements fall into the same class iff their difference is divisible by  $x^2 - 2$ . Very soon we will drop the  $[ ]$  as it is awkward notation but keep in mind the fact that we are working with congruence classes.

So can we find a root to the polynomial  $x^2 - 2$ ? The constants are obviously not roots as  $x^2 - 2$  is irreducible over  $\mathbf{F}_p$ . What about  $[x]$  the class of  $x$ ? Yes since  $[x]^2 - 2 = [x^2] - 2 = [x^2 - 2] = [0]$ .

Let  $\alpha = [x]$  where  $\alpha^2 = 2$  and we have a field with 25 elements.

$$\mathbf{F}_5[x]/x^2 - 2 = \mathbf{F}_5(\alpha) = \{a\alpha + b \mid a, b \in \mathbf{F}_5\}$$

As we constructed the above field by *adjoining* a root of  $x^2 - 2$  to  $\mathbf{F}_5$  we will read  $\mathbf{F}_5(\alpha)$  as  $\mathbf{F}_5$  *adjoined*  $\alpha$  and it is the smallest field containing  $\mathbf{F}_5$  and  $\alpha$ .

If this construction seems artificial recall that we've come across similar constructions earlier. If we accept  $\mathbf{R}$  to be natural then  $\mathbf{C} = \mathbf{R}(i) = \{ai + b \mid i^2 + 1 = 0\}$  is not a natural construction.  $\mathbf{C} = \mathbf{R}(i)$  doesn't make sense. So we consider a set  $\mathbf{R}[x]$  which is bigger than  $\mathbf{R}$  and check if  $\mathbf{R}[x]/x^2 + 1$  is a field over which  $x^2 + 1$  splits. Now  $\mathbf{R}[x]/x^2 + 1 = \mathbf{R}(i) = \mathbf{C}$ . So we construct the complex field by adjoining a root of  $x^2 + 1$ .

So now we've seen illustrations of how to construct extensions of finite and infinite fields. We'll move on to a more general method.

### 3. Construction of an extension field

Let  $\mathbf{k}$  be a field and  $f \in \mathbf{k}[x]$  be an irreducible polynomial of degree  $d$ . Consider the equivalence classes of  $\mathbf{k}[x]$  modulo  $f$ .

$\mathbf{k}[x]/f :=$  set of equivalence classes of  $\mathbf{k}[x]$  modulo  $f$ . This is clearly an additive group and the non-zero elements form a multiplicative group due to euclid's algorithm to compute inverses. Observe that we need  $f$  to be irreducible for the existence of inverses (analogous to the  $\mathbf{Z}/p\mathbf{Z}$  case)

Let  $\alpha = [x]$ . Then  $\mathbf{k}[x]/f = \mathbf{k}(\alpha) = \{a_0 + a_1\alpha + \dots + a_{d-1}\alpha^{d-1} \mid a_i \in \mathbf{k}\}$ . The above field is called the field obtained by adjoining  $\alpha$  to  $\mathbf{k}$

Lets prove some theorems about  $\mathbf{k}[x]$ , polynomial rings over the field  $\mathbf{k}$  before we go and use these results to the finite field case.

**Definition.** Let  $f \in \mathbf{k}[x]$  where  $\mathbf{k}$  is a field and  $f = \sum_{i=0}^n a_i x^i$  with  $a_i \in \mathbf{k}$  then  $f' := a_1 + 2a_2x + 3a_3x^2 + \dots + na_nx^{n-1}$

By the Division Thm,  $f$  decomposes into unique irreducible factors.

**Lemma 1.** Let  $\mathbf{k}$  be any field. If  $f \in \mathbf{k}[x]$  then  $\deg \gcd(f, f') > 0 \Leftrightarrow$  there exists a irreducible polynomial  $h$  of degree  $> 0$  such that  $h^2|f$ .

**Proof.** Suppose  $h \in \mathbf{k}[x]$  with  $\deg h \geq 1$  and  $f = h^2g$  for some  $g \in \mathbf{k}[x]$ . Recall that the chain rule is given by  $(f_1f_2)' = f_1'f_2 + f_1f_2'$ . Applying the chain rule both sides of  $f = h^2g$  gives us  $f' = (h^2g)' = 2hh'g + h^2g'$ . As  $h$  divides both the terms on the right hand side,  $h|f'$  which inturn implies  $h|\gcd(ff')$ .

Conversely if  $\deg \gcd(f, f') \geq 1$  then there exists an irreducible polynomial  $h$  of degree  $\geq 1$ . Say  $h|f$  and  $h|f'$ . So let  $f = hg$  for some  $g$ . Applying the chain rule gives us  $f' = h'g + hg' \Rightarrow f' - hg' = h'g$ . As  $h$  divides the left hand side, we have  $h|h'g$ . But as  $h$  is irreducible and  $\deg h' < \deg h$  we get  $h|g \quad \diamond$

A restatement of the above lemma says:  $f$  has multiple factors iff  $f, f'$  have a non-trivial gcd.

**Lemma 2.** Let  $\mathbf{k}$  be any field and  $\mathbf{L}$  be a field extension of  $\mathbf{k}$ . For  $\alpha \in \mathbf{L}$ , suppose  $f(\alpha) = 0$  for some  $f \in \mathbf{k}[x]$  then there exists a unique irreducible polynomial  $f$  of minimal possible degree.

**Proof.** Suppose  $f$  is of minimum possible degree but on the contrary  $f$  is not irreducible. Say  $f = gh \Rightarrow f(\alpha) = g(\alpha)h(\alpha)$ . As this arithmetic is happening in a field so two non-zero elements cannot multiply to give zero either and so  $g(\alpha) = 0$  or  $h(\alpha) = 0$ . But  $\deg g, \deg h < \deg f$  which contradicts the minimality of the degree of  $h$ . Minimality of degree of  $f$  and uniqueness also have a straightforward arguments.  $\diamond$

**General method to construct extension fields.** Let  $\mathbf{k}$  be any field and  $f \in \mathbf{k}[x]$  to construct a field  $\mathbf{L} \supseteq \mathbf{k}$  over which  $f$  splits completely. If  $f$  splits into linear factors over  $\mathbf{k}$  we are done. Otherwise there exists a polynomial  $h \in \mathbf{k}[x]$  irreducible of degree  $> 1$  such that  $h|f$ . Construct field  $\mathbf{k}_1$  by adjoining a root of  $h$ .  $\mathbf{k}_1 = \mathbf{k}[x]/h = \mathbf{k}(\alpha)$  where  $h(\alpha) = 0$  in other words  $\alpha = [x]$ . Now we've found a larger field where more roots of  $f$  are found. Let's factor  $f$  over  $\mathbf{k}_1$ . Say  $f = (x - \alpha)f_1$  for some  $f_1$ . Now  $\deg f_1 = \deg f - 1$ . Inductively we construct a list of fields  $\mathbf{k} \subseteq \mathbf{k}_1 \subseteq \dots \subseteq \mathbf{k}_m$ . We stop when the polynomial is completely split and take field  $\mathbf{L} = \mathbf{k}_m$  and we have  $f(x) = \prod_{i=1}^{\deg f} (x - \alpha_i)$  with  $\alpha_i \in \mathbf{L}$ .

## 4. Uniqueness of finite fields

We are finally back to our finite field discussion. To construct a finite field of  $q = p^d$  elements. Recall that if there exists a field  $\mathbf{k}$  with  $|\mathbf{k}| = q$  then  $\alpha^q = \alpha$  for all  $\alpha \in \mathbf{k}$ . So to construct a field  $\mathbf{L}$  over which  $x^q - x$  splits completely we need  $x^q - x = \prod_{i=1}^q (x - \alpha_i)$  with  $\alpha_i \in \mathbf{L}$ .

Applying *general method* to construct extension fields outlined above with  $\mathbf{k} = \mathbf{F}_p$  and  $x^q - x$  where  $q = p^d$  we obtain  $\mathbf{F}_q$  in no more than  $d$  steps. Suppose  $\mathbf{L}$  is a finite field containing  $\mathbf{F}_q$  over which  $x^q - x \in \mathbf{L}[x]$  splits that is  $x^q - x = \prod_{i=1}^q (x - \alpha_i)$  with  $\alpha_i \in \mathbf{L}$ .

*Lemma 1* tells us that  $x^q - x$  has multiple roots in  $\mathbf{L}$  iff degree of  $\gcd(x^q - x, (x^q - x)') > 0$ . But  $(x^q - x)' = qx^{q-1} - 1 = -1$  as  $\mathbf{L}$  is a field of characteristic  $p$ . So  $x^q - x$  cannot have multiple roots and hence all the  $\alpha_i$ 's are distinct.

**Claim.** The roots of  $x^q - x$  in  $\mathbf{L}$  form a subfield of  $\mathbf{L}$ .

**Proof.** Since we know that there are  $q$  roots. It is enough to check that for all  $\alpha, \beta \in \mathbf{L}$ ,  $\alpha^q = \alpha$ ,  $\beta^q = \beta$ .

- $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$  by commutativity.
- if  $\alpha \neq 0$  then  $(\alpha^{-1})^q = \alpha^{-1}$ .
- $(\alpha + \beta)^q = \alpha^q + \sum_{i=1}^{q-1} C_i^q \alpha^i \beta^{q-i} + \beta^q = \alpha^q + \beta^q = \alpha + \beta$  where  $C_i^q = \frac{q!}{i!(q-i)!}$  and as for each  $i$ ,  $C_i^q$  is divisible by  $q$  the summation term disappears as we are working in characteristic  $p$ .

So we have formed a subfield of  $\mathbf{L}$  with  $q$  elements.  $\diamond$

Next we make the following strong claim.

**Thm.** Let  $\mathbf{k}$  be a finite field with  $q = p^d$  elements then  $x^q - x = \prod h(x)$  where the product is over all polynomials  $h \in \mathbf{F}_p[x]$  with  $h$  irreducible and  $\deg h | d$ .

**Proof.**

**Claim.** If  $h \in \mathbf{F}_p[x]$  is irreducible polynomial and  $h | x^q - x$  then  $\deg h | d$

**Proof.** Let  $\alpha^q = \alpha$  with  $\alpha \in \mathbf{k}$ . Let  $h \in \mathbf{F}_p[x]$  be the minimal polynomial of  $\alpha$  over  $\mathbf{F}_p$  then we know that  $h$  is irreducible by *Lemma 2* and say  $l$  is the degree of  $h$ . Consider  $\mathbf{F}_p(\alpha) = \mathbf{F}_p[x]/h = \{a_0 + a_1\alpha + \dots + a_{l-1}\alpha^{l-1} \mid a_i \in \mathbf{F}_p\}$ .

Now  $|\mathbf{F}_p(\alpha)| = p^l$  now viewing  $\mathbf{k}$  as a vector space over  $\mathbf{F}_p(\alpha)$  and let  $\dim_{\mathbf{F}_p(\alpha)} \mathbf{k} = m$ . So we have  $|\mathbf{k}| = |\mathbf{F}_p(\alpha)|^m \Rightarrow p^d = p^{lm} \Rightarrow l | d$   $\diamond$

Conversely...

**Claim.** Suppose  $h \in \mathbf{F}_p[x]$  is irreducible and  $\deg h \mid d$  then  $h \mid x^d - x$

**Proof.** Observe that  $\mathbf{F}_p[x]/h$  is a field with  $p^l$  elements where  $l = \deg h$  and the field contains all roots of  $x^{p^l} - x$  therefore  $h \mid x^{p^l} - x$ . Now  $l \mid d$  and since  $p^l - 1 \mid p^d - 1$  we have  $x^{p^l} - x \mid x^{p^d} - x$ , that is  $h \mid x^d - x$   $\diamond$

This completes the proof of the thm.  $\diamond$