

**Algebra II**  
**Professor S Viswanath**  
**The Institute of Mathematical Sciences**  
**Lecture 32**  
**Solved Problems (Week 4)**

(Refer Slide Time: 00:16)



Problems

1.  $\mathbb{F}_p$  finite field  $p$  prime.

$$f(x) = x^p - x + a \quad a \in \mathbb{F}_p, a \neq 0.$$

PT:  $f(x)$  is an irreducible, separable polynomial  
in  $\mathbb{F}_p[x]$ .

Solution: Separable:  $Df(x) = px^{p-1} - 1 = -1$   
so  $\gcd(Df, f) = 1 \Rightarrow f$  is separable.



Let us do a problem. So here is the statement. So, let us take the field  $\mathbb{F}_p$ , this is the finite field with  $p$  being a prime. And consider the following polynomial, let us take  $f$  of  $x$  to be the polynomial  $x$  power  $p$  minus  $x$  plus a constant  $a$ , where  $a$  is an element of  $\mathbb{F}_p$ , but we assume is not 0. So, the question says prove that  $f$  is an irreducible separable polynomial, if it is an irreducible separable polynomial in  $\mathbb{F}_p$  of  $x$ .

So, let us prove this. So here is the solution. It involves lots of little things that we have learnt along the way. So, it is a nice application of many of the facts we have seen. So, let us go ahead and do this. So first, let us check separability. So why is  $f$  separable? Recall the criterion for separability, which says that if the GCD of  $f$  and  $f$  prime is 1, then  $f$  is automatically separable. So now in this case, we just have to compute the derivative. So, let me call this  $Df$  of  $x$  or  $f$  of, or  $f$  prime of  $x$ .

So, the derivative which is this case, just  $px$  to the  $p$  minus 1 minus 1, but remember, we are over  $\mathbb{F}_p$  and so  $p$  times any anything is just 0. So that is that first term vanishes. So, this is just the polynomial minus 1. So obviously, the GCD of this polynomial  $Df$  or  $f$  prime with the original polynomial  $f$  is clearly 1. So, this means then, so this is true. And so of course, this means that  $f$  is separable. So here, I have used the criterion for separability in terms of the

derivative. But there is another way of doing this, which is, so recall, we are asked to show two things one, that it is irreducible as well as separable.

(Refer Slide Time: 02:51)

Another way:  $\mathbb{F}_p$  is a perfect field  $\Rightarrow$  Every irreducible poly in  $\mathbb{F}_p[x]$  is separable.

$\therefore$  Enough to prove:  $f$  is irreducible!

If  $a=0$ ;  $X^p - X = \prod_{\alpha \in \mathbb{F}_p} (X - \alpha)$

$\alpha \in \mathbb{F}_p \Rightarrow \alpha^p = \alpha$  //

We have  $a \neq 0$ :  $f(x) = X^p - X + a = a(a^{-1}X^p - a^{-1}X + 1)$

$= a(Y^p - Y + 1)$  //

where  $Y = a^{-1}X \Rightarrow Y^p - (a^{-1})^p X^p = a^{-1}X^p$

And so, recall, so another way, maybe, another approach is the following, recall that  $\mathbb{F}_p$  is a perfect field, and recall that meant that, what we call the Frobenius automorphism, the map which sends every element to the  $p$ th power is an isomorphism of this field. So, this is a perfect field. Therefore, what does that mean? Any irreducible polynomial is automatically separable. So, this was what perfectness allowed us to conclude, this implies every irreducible polynomial in  $\mathbb{F}_p$  of  $x$  is automatically separable.

So, I have used that result that we proved about perfect fields. And so, what does it mean in this in the context of this problem? Therefore, it is enough to prove that  $f$  is irreducible. So, we were asked to prove both. So, it is enough to show just one thing that  $f$  is irreducible, that would automatically imply separability. So, let us show that  $f$  is irreducible. So, observe that, if  $a$  is 0, so remember, our assumption was that  $a$  is not 0. But let us just pause for a moment and wonder what happens if  $a$  is 0, then the polynomial is just  $x$  to the  $p$  minus  $x$ .

And this is of course, not irreducible, you can pull out a common factor of  $x$  definitely. But in fact, you can exactly say how this factorizes, observe that if I take any element  $\alpha$  in  $\mathbb{F}_p$ , the finite field, then  $\alpha$  power  $p$  is exactly  $\alpha$ . So, you have seen this in the construction of finite fields. So, what does this mean? This means that every element  $\alpha$  of  $\mathbb{F}_p$  is a root of this polynomial. And so, we can write this polynomial, it factorizes completely, it splits completely over  $\mathbb{F}_p$  as follows.

So, it is just a product of  $x$  minus  $\alpha$  as  $\alpha$  ranges over  $\mathbb{F}_p$ . So, we know that,  $\alpha$  is not 0 is definitely required. So, we have however, that  $\alpha$  is not 0. So, now let us write out our polynomial. So, this looks like  $x^p - x$ , and there is an additional factor of  $a$ . Now let us do the following since  $a$  is not 0, I will pull a common factor of  $a$  from everything, write this as  $a$  inverse  $x^p - a$  inverse  $x + 1$ . So, my goal is to get the constant term to be a 1 here.

Now, this is well, I can rewrite this as  $a$  times  $y^p - y + 1$ . So, I am changing variable here,  $y$  is just  $a$  inverse  $x$ , and why is that? Why is the first term  $y$  power  $p$ ? Observed that, we have just said that here, that every element of the base field  $\mathbb{F}_p$  its  $p$ th power gives you  $\alpha$ . So,  $y$  is  $a$  inverse  $x$  means that if I raise this to the  $p$ th power, it is going to give me  $a$  inverse to the  $p$ th power  $x$  to the  $p$ th power, but  $a$  inverse to the  $p$  is just the same as  $a$  inverse, because  $a$  inverse is an element of my field  $\mathbb{F}_p$ .

(Refer Slide Time: 06:36)

Let  $g(x) = x^p - x + 1 \in \mathbb{F}_p[x]$  Then  $f(x) = a g(a^{-1}x)$

or equiv:  $g(x) = a^{-1} f(ax)$   
 $\deg g = \deg f = p$

$f(x)$  is irreducible  $\Leftrightarrow g(x)$  is irreducible.

Pf: If  $g(x) = m(x)n(x)$   $m, n \in \mathbb{F}_p[x]$  with  
 $\deg m < p$   
 $\deg n < p$ .

Then  $f(x) = a m(a^{-1}x) n(a^{-1}x)$



Another way:  $\mathbb{F}_p$  is a perfect field  $\Rightarrow$  Every irreducible poly



in  $\mathbb{F}_p[x]$  is separable.

$\therefore$  Enough to prove:  $f$  is irreducible!

$$\textcircled{1} \text{ If } a=0; \quad X^p - X = \prod_{\alpha \in \mathbb{F}_p} (X - \alpha)$$

$$\alpha \in \mathbb{F}_p \Rightarrow \alpha^p = \alpha //$$

$$\textcircled{2} \text{ We have } a \neq 0: \quad f(x) = X^p - X + a = a \left( a^{-1} X^p - a^{-1} X + 1 \right)$$

$$= a \left( Y^p - Y + 1 \right) //$$

$$Y = a^{-1} X \quad \text{so } Y^p - Y + 1 = a^{-p} X^p - a^{-1} X + 1$$



So what does this mean? It basically means that I can rewrite this polynomial in such a way that my constant term is a 1. So let us, let us write that out here. So,  $g$  of  $x$  equals  $x$  to the  $p$  minus  $x$  plus 1. So, observe, so I am going to define  $g$  in this way, then, so let  $g$  be defined in this manner, then observe that  $f$  and  $g$  are more or less the same polynomial, they just differ by this following very simple transformation, I can change variable to a inverse  $x$ , and I pull out a common factor of  $a$ .

So,  $f$  of  $x$  is just a polynomial  $a$  times  $g$  of a inverse  $x$  or equivalently I can rewrite, I can change  $x$  to  $ax$  and write this is as  $g$  of  $x$  is nothing but a inverse  $f$  of  $ax$ . So, what is all this you need off? Well, in particular, this means the following. This says that if  $f$ , so maybe I will number the facts along the way. So, let us see this is if  $a$  equals 0, what happens? Step two, is this this simplification here. Step three, is realizing that, well, maybe this is still step two.

So, observe that if  $fx$  is irreducible, then so is  $gx$ . So, observe  $f$  of  $x$  is an irreducible polynomial. So, observe, this is also a polynomial with coefficients in  $\mathbb{F}_p$  of  $x$ . So,  $f$  of  $x$  is irreducible, if and only if  $g$  of  $x$  is irreducible. How do we prove this? Well, it is easy enough. So, let us suppose  $g$  is irreducible. So here is a little proof of this fact. If  $g$  can be written as a product of two polynomials, say, let me call them  $m$  of  $x$  and  $n$  of  $x$ , both polynomials with coefficients in  $\mathbb{F}_p$ , then just use this transformation property.

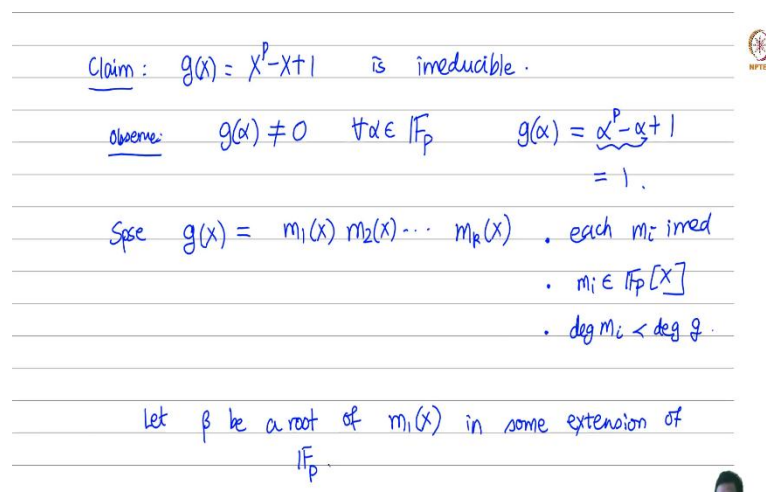
How do you get  $f$  from  $g$ ? Well,  $f$  of  $x$  is just  $a$  times  $g$  of a inverse  $x$ . So, it is  $m$  of a inverse  $x$ ,  $n$  of a inverse  $x$ . Now observe that this gives me a way of writing  $f$  as a product of two polynomials, because well, these are also polynomials with coefficients in  $\mathbb{F}_p$ . So, let me assume that  $m$  and  $n$  with, let us say degree of  $m$  and degree of  $n$ , now they are both

polynomials of degree strictly smaller than the degree of  $g$ , so degree of  $m$  smaller than degree of  $g$ .

So, you can write it as a product in this manner, then the same is true of  $f$  because for example, look at this guy here. This is a polynomial whose degree is strictly smaller than the degree of  $g$ . This is a polynomial whose degree is smaller than the degree of  $g$ , but the degree of  $f$  and the degree of  $g$  are the same. So, degree  $g$  is the same as degree of  $f$ .

In fact, both degrees are equal to  $p$  in this case. So, this gives me a way of rewriting  $g$ , so, this gives us a way of rewriting  $f$  as a product of two polynomials again whose degrees are strictly smaller than  $f$ . In other words, if  $g$  is reducible, then  $f$  is reducible. And sort of you can work the same argument with the roles of  $f$  and  $g$  reversed. So, that just shows that if  $f$  is irreducible, then  $g$  is reducible and vice versa. So, let us just prove that  $g$  is irreducible.

(Refer Slide Time: 10:40)



Claim:  $g(x) = x^p - x + 1$  is irreducible.

Observe:  $g(\alpha) \neq 0 \quad \forall \alpha \in \mathbb{F}_p \quad g(\alpha) = \alpha^p - \alpha + 1 = 1.$

Spse  $g(x) = m_1(x) m_2(x) \dots m_r(x)$ . each  $m_i$  irred

- $m_i \in \mathbb{F}_p[x]$
- $\deg m_i < \deg g$ .

let  $\beta$  be a root of  $m_1(x)$  in some extension of  $\mathbb{F}_p$ .

So, claim  $g$  is irreducible, so proving it essentially, we are saying that if you, recall  $g$  is just nothing but  $f$  with the value  $a$  equals 1. So, what we are saying is we prove it for equals 1, you prove it for all values of nonzero, all nonzero values of  $a$ . Claims that  $g$  of  $x$  is irreducible, so it is  $x$  to the  $p$  minus  $x$  plus 1 is irreducible.

So, observe the following that definitely, this has no roots in the base field  $\mathbb{F}_p$ , so observe  $g$  of  $\alpha$  is definitely not 0, for all  $\alpha$  in the base field because, in fact, if I compute  $g$  of  $\alpha$  for any element of the base field, it is  $\alpha$  to the  $p$  minus  $\alpha$  plus 1, but we know that this is 0, so this is actually 1.

So now, let us prove it is irreducible, suppose, suppose not, suppose  $g$  can be written as a product, let us say  $m_1x$  and  $m_2x$ , I decompose it into a bunch of irreducible factors  $m_k$  of  $x$ , each  $m_i$  is irreducible, each  $m_i$  belongs to  $\mathbb{F}_p$  of  $x$ . And what more do I know about each  $m_i$ ? I also know that the degree of  $m_i$  is strictly smaller than degree of  $g$ .

Now, let us do the following. Let us take the first polynomial  $m_1$  of  $x$  and that is some irreducible polynomial. So, it has a root in some extension of  $\mathbb{F}_p$ . So, let  $\beta$  be a root of the first polynomial  $m_1$  of  $x$  in some extension of  $\mathbb{F}_p$ . So, recall this is one of the things that you learned about symbolic adjunction which is that given any polynomial, the non-constant polynomial, you can always construct some extension, some finite extension in fact of the base field in which that polynomial has a root.

(Refer Slide Time: 13:12)

$$[\mathbb{F}_p(\beta) : \mathbb{F}_p] = d = \text{degree of } m_1 < \text{deg } g = p$$

$$d \neq 1 \text{ since } \beta \notin \mathbb{F}_p$$

Thus  $|\mathbb{F}_p(\beta)| = p^d$ ; thus  $\mathbb{F}_p(\beta)$  is just the finite field of cardinality  $p^d$   
 $\Rightarrow \forall \gamma \in \mathbb{F}_p(\beta), \gamma^{p^d} = \gamma$   
 put  $\gamma = \beta$

So, let us take that extension. So, let us consider  $\mathbb{F}_p$  beta. So, I take that extension in which there is a root beta and I consider the field  $\mathbb{F}_p$  beta over  $\mathbb{F}_p$ . So, what is the degree of this extension? Well, the degree of this extension, so let us call the degree as  $d$ . So, let  $d$  denote the degree of this extension. What do we know about  $d$ ?  $d$  is just the degree of  $m_1$ ,  $m_1$  is the irreducible polynomial. So, the degree of  $m_1$  is definitely less than the degree of  $g$ . That was the starting assumption, which is  $p$ .

So, degree of  $m_1$  is smaller than  $p$ , that is what you know,  $d$  is smaller than  $p$ . Well, that is one thing we know about  $d$ . Another thing we know about  $d$  is that remember, beta is not in  $\mathbb{F}_p$ . So, this is fact 1, is that  $d$  is less than  $p$ . Fact 2, is that  $d$  is at least 1. So, I claim in fact, I can say more  $d$  cannot equal 1. Why is that? That is because  $d$  cannot equal 1, since if  $d$  is 1 that will mean that beta belongs to the base field.

But we have already seen that  $g$  has no roots in the base field. We have already shown that  $\beta$  is a root of  $g$ . So, what this means is that, this is an extension of degree equal to  $d$ , which is a number strictly between 1 and  $p$ . What does that mean? Well recall from your construction of finite fields, you have learned that if I have a finite field,  $F_p$  and I have a degree  $d$  extension of finite extension.

What does that mean? It just means that the field on top, thus  $F_p$  of  $\beta$ , it is a field whose cardinality, I mean as a vector space over the base field, it is of dimension  $d$ . So, the cardinality of the field on top is just  $p$  power  $d$ . And you know that finite fields of a given cardinality are unique. So, this is just the finite field of cardinality  $p$  power  $d$ .

Thus, what does that mean  $F_p$  of  $\beta$  is just the finite field of cardinality  $p$  power  $d$ , which means, in particular that if you take any element from this field, which means that if I take  $\gamma$ , for all  $\gamma$  in this field, if I raise  $\gamma$  to the power  $p$  power  $d$ , the cardinality of the field I am supposed to get back  $\gamma$ . This is the property that these finite fields have. In particular, this is true if  $\gamma$  equals  $\beta$ . So, let me now put  $\gamma$  equals  $\beta$  because  $\beta$  in particular is an element here.

(Refer Slide Time: 16:13)

Two  $\beta^{p^d} = \beta$  ; ALREADY KNOW :  $g(\beta) = 0 \Rightarrow \beta^p - \beta + 1 = 0$

can't both hold if  $1 < d < p$ .

$\beta^p = \beta - 1$

$\beta^{p^2} = (\beta^p)^p = (\beta - 1)^p = (\beta + (-1))^p = \beta^p + (-1)^p = \beta - 1 - 1 = \beta - 2$

So, I conclude that  $\beta$  thus,  $\beta$  satisfies the following equation,  $\beta$  power  $p$  power  $d$  is  $\beta$ . So, I get one equation that  $\beta$  satisfies. But we already knew something about  $\beta$ , what do we know? We already know the following that  $\beta$  was the root of  $g$ .  $\beta$  was in fact a root of  $m_1$ , which was one of the irreducible factors of  $g$ . So, this means, in particular that  $\beta$  power  $p$  minus  $\beta$  plus 1 is 0. So here is the second equation that  $\beta$  satisfies.

Now, our claim is that these two equations cannot be simultaneously satisfied for  $d$  a number strictly between 1 and  $p$ . So, these cannot both hold, if  $d$  is a number between 1 and  $p$ . Why is that? Let us prove this. So, probably many different ways of going about the proof. But let me start with the second equation here. So, I know that beta power  $p$ , I will rewrite it as beta power  $p$  is beta minus 1.

Now from this I can compute what is beta power  $p$  square. So, I will just take beta power, sorry beta power  $p$  square is nothing but beta power  $p$  the whole power  $p$ . So that is beta minus 1 the whole power  $p$ . Now, well what is that? That is beta plus minus 1, the whole power  $p$ . And you have seen this computation many times, this is just beta power  $p$  plus minus 1 power  $p$ , because all these are taking place over a field of characteristic  $p$ . All the intermediate terms that you get in the binomial theorem are all divisible by  $p$ . So, they all go away.

So, beta to the  $p$  square is just beta to the  $p$  plus minus 1 to the  $p$ . Well, what is that? So, this is just beta to the  $p$ . So, beta to the  $p$ , I already know is beta minus 1. So, this is just beta minus 1 and minus 1 to the  $p$ , well, for now, if  $p$  is an odd prime, so maybe we should just assume, let us just make that assumption. Suppose  $p$  is an odd prime, I mean, you can just do it similarly for  $p$  equals 2. So, let me just say case 1,  $p$  is an odd prime. Then this is again, a minus 1. So, this is beta minus 2.

(Refer Slide Time: 18:41)

$$\beta^{p^3} = (\beta^{p^2})^p = (\beta - 2)^p = \beta^p - 2^p = \beta^p - 2 = \beta - 2 \quad \begin{matrix} 2^p = 2 \\ 2 \in \mathbb{F}_p \end{matrix}$$

$$\vdots$$

$$\beta^{p^d} = \beta - d \quad \text{ALSO KNOW : } \beta^{p^d} = \beta$$

$$\Rightarrow d = 0 \quad \text{BUT } 1 < d < p$$

Contradiction!







Two  $\beta^{pd} = \beta$  ; ALREADY KNOW :  $g(\beta) = 0 \Rightarrow \beta^p - \beta + 1 = 0$

can't both hold if  $1 < d < p$ .

cancel  $p$  odd prime

$$\beta^p = \beta - 1$$

$$\beta^{p^2} = (\beta^p)^p = (\beta - 1)^p = (\beta + (-1))^p = \beta^p + (-1)^p = \beta - 1 - 1 = \beta - 2$$



Now, you can already see how this is going to go, if I compute the next power of beta to the p cubed is just beta to the p square the whole to the p, that is now beta minus 2 the whole to the p. And by the same token it is going to be beta to the p minus 2 to the p. But 2 to the p is just 2. Recall this is because 2 belongs to the base field, 2 is in  $F_p$ . And therefore, when you raise it to the power p, you just get back itself, and so on. So, what does that mean? Oh, sorry, beta to the p on the other hand is beta minus 1.

So, this is beta minus 3. So, in general, well, or let us do it d times, this will just give me beta minus d. So, I have just repeatedly I have iterated my second equation, and concluded that beta to the p to the d is beta minus d. On the other hand, the first equation tells me sorry, I am here. But we also know, also know the first equation which says that beta power p power d is beta. Now, how can these two equations be true?

Well, this means automatically that d is 0. But observe, that cannot happen. Why not? Well, because d is a number between 1 and p. So, since d is strictly smaller than p, it cannot happen that d is 0 in this field. So, d is 0 is a contradiction. So, if d is p then it is okay. If d equals p then of course, it means that p is just 0 in a finite field of cardinality p, or any characteristic p field. So that completes the proof.