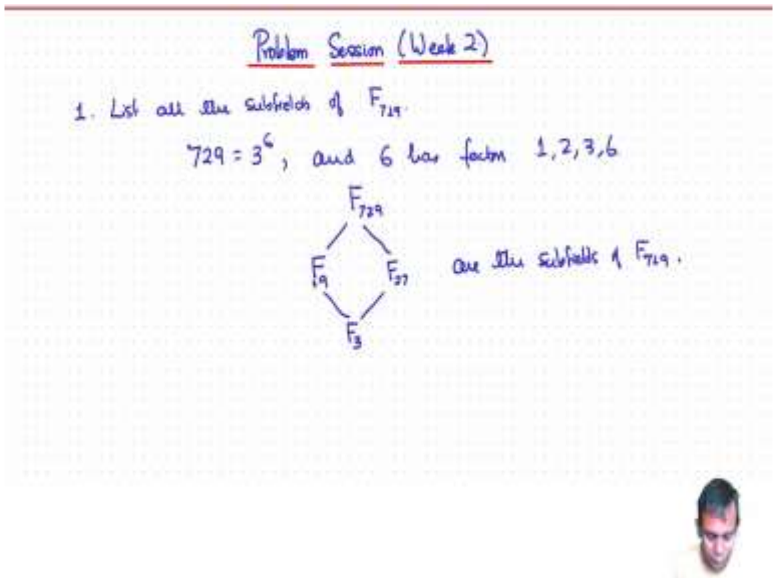
Algebra - II
Professor Amritanshu Prasad
Mathematics
The Institute of Mathematical Sciences
Solved Problems (week 2)

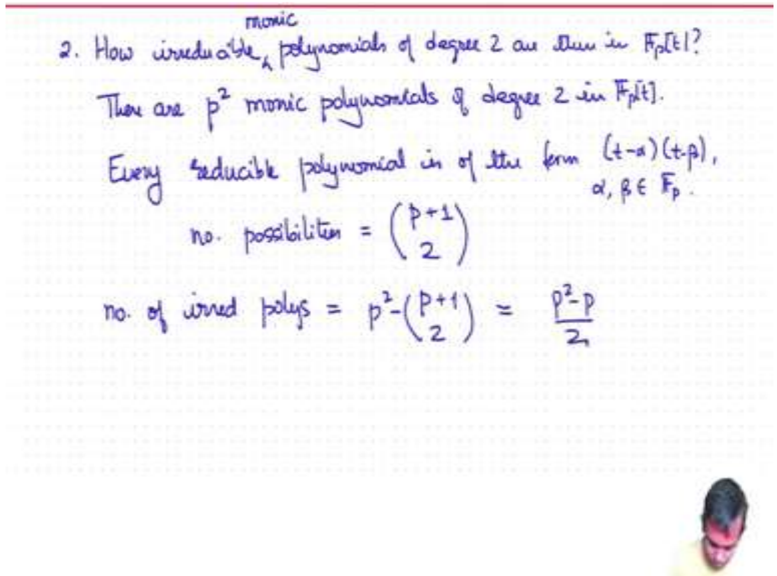
(Refer Slide Time: 00:15)



Let us solve some problems, the first problem list all the subfields of F729 By which I mean a finite field of order 729. So, 729 is 2 to the power 6 and 6 has factors 1, 2, 3 and 6. So, we have F729. It contains subfield of order 3 square, which is 9. It also contain subfield of order 27 which is 3 cubed. And both those contain a subfield of order 3.

The F 729 has exactly four subfields including itself F 729, F9, F27 and F3 these are the subfields of F729. It is exactly one of each of the. F9 consists of the root of the polynomial t to the 9 minus tF27 consists of the roots of the polynomial t to the 27 minus t and F cube consists of the root for the polynomial in the cube minus, okay. So, that was easy.

(Refer Slide Time: 01:48)



Let us look at problem two of how many irreducible polynomials of degree 2 are there in Fbt. So, I am asking this question about general Fpt. Let us see how the answer depends on p. That is another interesting point. So, now one way to calculate the number of irreducible polynomials, maybe let us just make this simple, irreducible monic polynomial, okay.

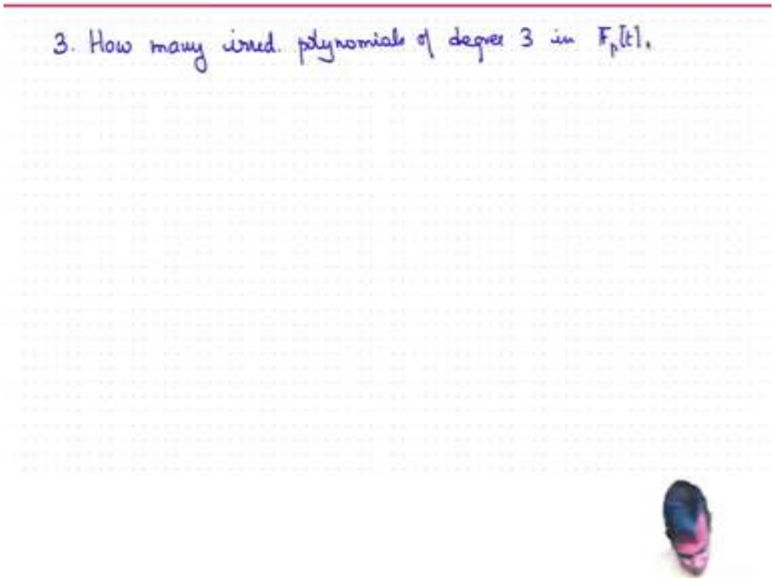
So, one way to find the irreducible polynomial, this is start with all polynomial. So, there are totally p squared irreducible polynomials, monic polynomial of degree 2 because each monic polynomial for t square plus at plus b, you have p choices for a and p choices for b. So, the total p square monic polynomials of degree 2 in Fpt, irreducible or not.

Now from this, let us remove the polynomial which are not reducible. So, every reducible polynomial or non-irreducible average is well, it must have two linear factors is of the form, t minus alpha into t minus beta where alpha and beta are in Fp. So, what we are looking is how many pairs, unordered pairs of possibly in repeated elements do I have in Fp.

And so the number of possibilities is the number of sub multi sets of a set of size p plus 1 off sites 2 which is p plus 2 minus 1 choose 2, another way to see this is okay if they have to be distinct. Then you get p choose 2 possibilities for alpha and beta. And if they have to be the same, then you get p possibilities for alpha, which is repeated root 2 times.

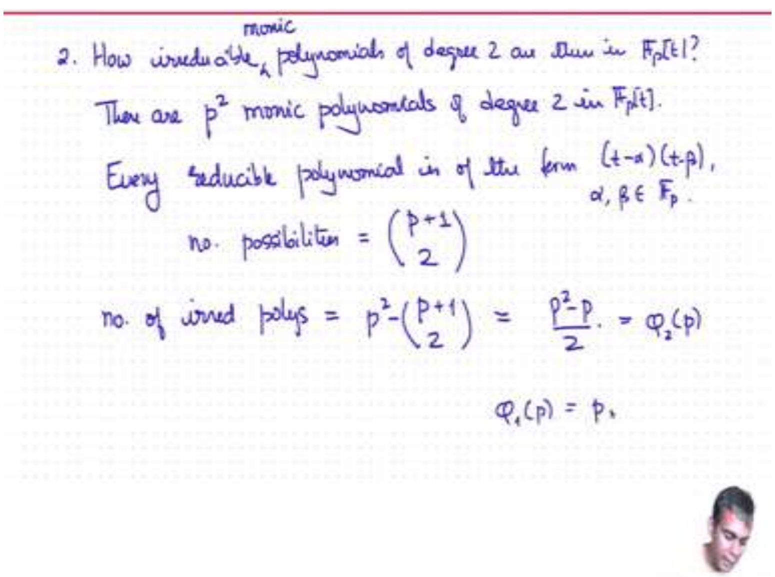
So, p choose 2 plus p, which is the same as p plus 1 choose 2. So, number of irreducible polynomials is p square minus p plus 1 choose 2 which is just p square minus p by 2, okay.

(Refer Slide Time: 04:46)



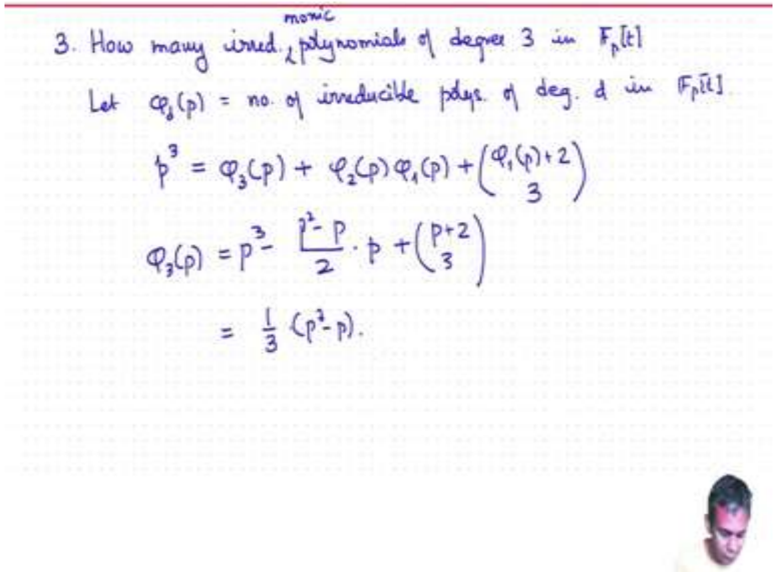
Let us try a slightly harder one. How many irreducible polynomials of degree 3? Actually, here p need not be a primary could also take p to be a prime power, all the uses of the cardinality, the field (())(5:17).

(Refer Slide Time: 5:17)



So, note that let us call this polynomial phi 2 p it is a polynomial p which is itself quite a nice thing. You do not need to calculate it separately for each Prime p, its dependence on p is just polynomial. And phi 1 p let us say, is the number of irreducible polynomial of degree 1.

(Refer Slide Time: 05:39)

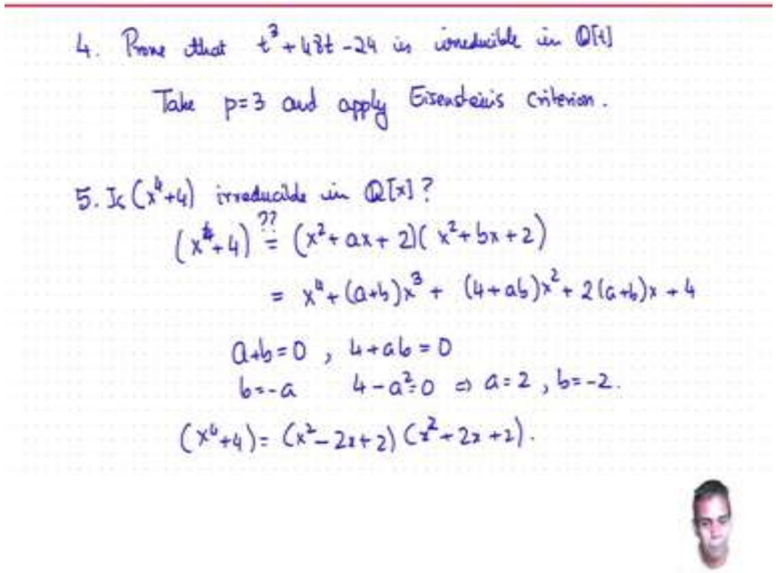


So, we have phi 1 p each polynomial from p minus alpha. This is just and phi 3p is so let phi dp be the number of irreducible polynomial of degree d in Fpt, what we get is p cubed is the total number of irreducible polynomials is a total number of again, I want to say monic polynomials. So, p cubed is the total number of monic polynomial the degree 3.

And so this consists of, okay, you can have the irreducible polynomials, which is phi 3p then you can have polynomials which have one irreducible factor of degree 2 and 1 and irreducible factor of degree 1. So, that phi 2 p time's phi 1 p and then you can have polynomials with 3 irreducible factors of degree 1. Now those factors could be repeated. And so what you get is phi 1 p plus 2 choose 3, the number of sub multi sets of a set of size phi 1 p of size 3.

If you want, you can work through different cases and see these two are the same and so on. I let you figure this part out. So, now we know the values of phi 2 and phi 1. So, we can compute phi 3 from that. So, what we get is phi 3 p is p cubed, minus now phi 2 is p squared minus p by 2 into p plus. And then this is just p plus 2 choose 3. And if you expand it all out, I believe you will get 1 by 3 p cube minus p.

(Refer Slide Time: 08:12)



The next exercise is a fairly straightforward application of Eisenstein's criteria. Prove that t cubed plus 48t minus 24 is irreducible in Qt. Now, this would be you just have to find a prime p with which we can apply Eisenstein's criterion. So, you look at the factors of 24, 24 has two prime factors, 2 and 3, but it is divisible by 4. So, you cannot use p equals 2 however you can use p equals it is just divisible by 3, but it is not divisible by 9. So, just take p equals 3 and apply Eisenstein's criterion, okay.

And let us look at problem five, which is another irreducibility problem is x to the 4 x, x to the 4, x to the 4 plus 4 irreducible in Qx. Now it would be tempting to see that Eisenstein's criterion does not apply to this polynomial because the only P I can take is 2, but p square divides 4 so the only. So, Eisenstein's criterion does not apply to this polynomial and therefore it is not irreducible.

But that is not correct. Eisenstein's criterion only gives a sufficient condition for a polynomial to be irreducible. If Eisenstein's criterion does not hold that is not automatically mean that the polynomial is not irreducible. So, we need to work a little further and try to examine this.

Now note that x to the power 4 plus 4 does not have any linear factors because x to the power 4 plus 4 does not have any rational roots. So, we would be looking for a factorization into two quadratic factors. So, let us try and we should have x square plus, x to the power 4 plus 4 should be a product of two quadratic factors. And we know that we can choose they have to be integer polynomial by gauss's lemma.

So, there were must be of the form x square plus so you can have ax plus 2 into x square plus bx plus 2 you can have x square plus ax plus 4 into x square plus bx plus 1. But let us just try this and see we can find a and b. But if you can expand this out so we do not know for sure that we have a factorization like this. So, let us just try so we expand this out you get x to the power 4 plus a plus b x cubed plus 4, 2 here and 2 here so 4. We want x square 4 plus ab x square plus 2 into a plus bx plus 4.

So, that is the thing what we must have is that a plus b is equal to 0. And 4 plus ab is equal to 0. And so this means that b is equal to minus a. which means that 4 minus a square equal 0 which imply a equals 2, b equals minus 2. So, we have a factorization x power 4 plus 4 is x square minus 2x plus 2 into x square plus 2x plus 2.

Well if you were little observe and you may have notice that this is the x to the power 4. So, this is an a plus b into a minus b forms. So, x square plus 2 minus 2x into x square plus 2 plus 2x. So, this is can also be solved in that way by gauss. So, x to the power 4 is not a irreducible Qx. Eisenstein's criterion does not applied but that is not enough you actually need to show that it is reducible.