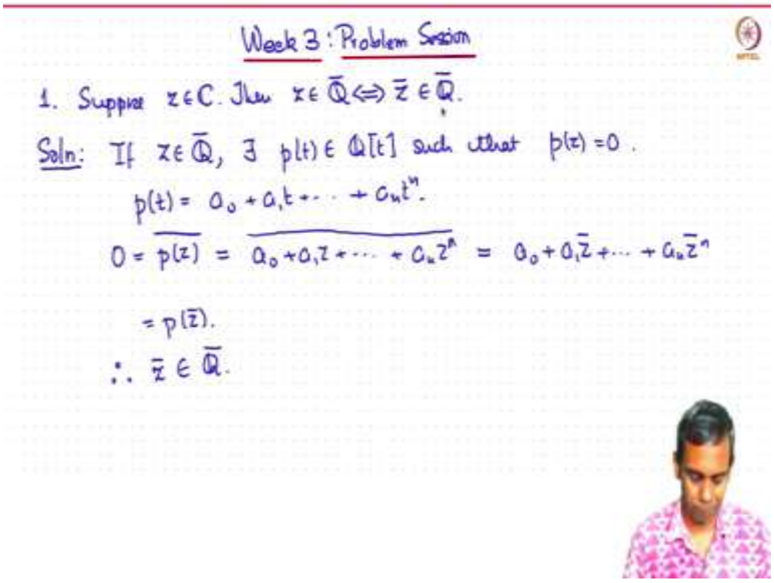
Algebra II
Professor – Amritanshu Prasad
The Institute of Mathematical Sciences
Solved Problems, part 1 (Week 3)

(Refer Slide Time: 00:16)



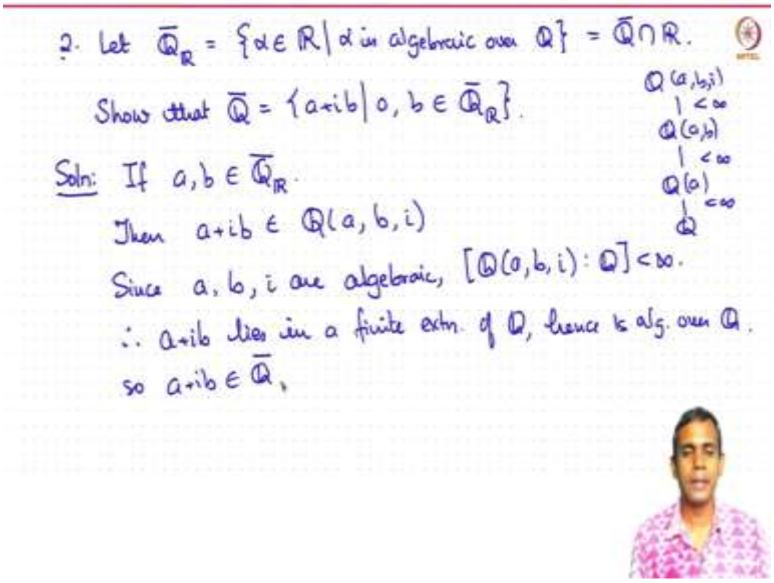
Let us solve some problems. For the first problem, recall that Q bar denotes a set of complex numbers that are algebraic over Q. And the problem states that suppose Z is a complex number, then Z belongs to Q bar, if and only if Z bar belongs to Q bar. Now, you can pause the video and try to solve it yourself. And if you cannot do it, then go ahead and watch me solve it. What does it mean for Z to be in Q bar.

So, if Z is in Q bar, then there exist a polynomial pt, in Qt such that pz is equal to 0. Now, let us look at this polynomial say pt is equal to a0 plus a1t plus an t to the power n. Now I claim that p of z bar is also 0. This is because well, 0 is p of z taking complex conjugates, we get that p of z the whole thing bar is 0. But this is a0 plus a1z plus an z to the n. And then we take bar of this whole, not z sub n, z to the power n, we take bar of this whole thing.

With these coefficients a0 a1 up to an are rational and therefore, they are in fact real numbers. So, I can write this as a0 plus a1z bar plus an z to the n bar. But this is nothing but p of z bar. So, if z satisfies a polynomial pt, then z bar also satisfies the same polynomial pt, if that polynomial has coefficients, which are real numbers. Since rational numbers are real numbers, z bar again satisfies this polynomial pt.

And that shows that if z is in Q bar, the other way is by symmetry, because z bar bar is equal to z. So, if z bar is in Q bar, then z bar bar, which is z is also in Q bar. So, you do not really need to do that separately.

(Refer Slide Time: 02:58)



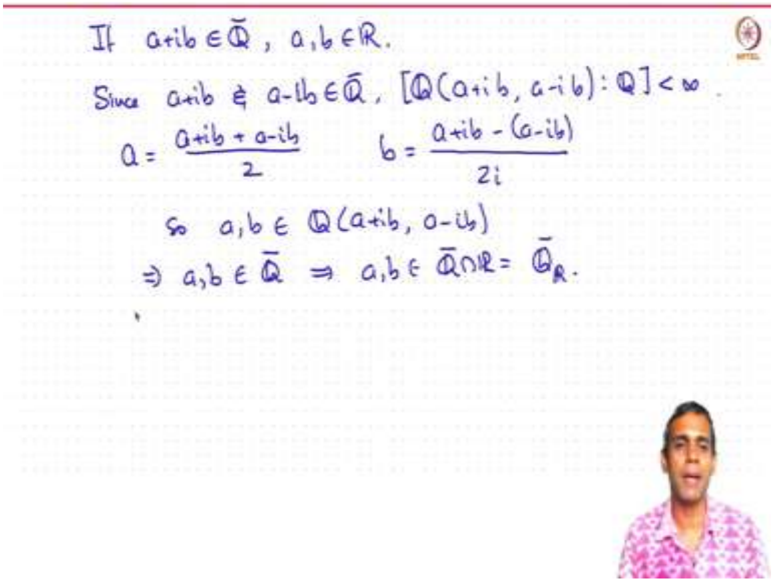
Now let us move on to problem two. So, for this problem, let us define a subfield of QR. Let, I will call it Q bar subscript R. It is the set of complex numbers C, well, no, I would say the set of real numbers alpha such that alpha is algebraic over Q. So, this is nothing but Q bar intersect the real numbers. And the problem is show that Q bar is equal to a plus ib, where a and b belong to Q bar R.

Now you can pause the video and try to solve this yourself. If you cannot, then I will solve it for you. So firstly, what we will show is that if so, so we need to show that if a and b are in QR bar, then a plus ib is in Q bar. And conversely, if a plus ib is in Q bar, then a and b are in QR bar. So, let us start with the assumption that a and b are in QR bar and we want to show that a plus ib is in Q bar.

So, then a plus ib belongs to the field generated by Q, a, b and i. But a, b and i are all algebraic. So, this is a finite extension of of Q. So, a and b are algebraic, because they are in QR bar, i is algebraic because i squared is minus 1. If you are not sure why this is true, I would suggest you work it out. You can show it by looking at a tower of fields Q a, b, i then Q a, b and then Q a and then Q and showing that each of these extensions is finite.

Basically, you can bound the extension of Q, a degree of Q a, b, i over Q a, b by the degree of Q i over Q i over Q. We have seen these kinds of arguments before in the lecture. So, this extension being generated by algebraic elements is algebraic. And therefore, a plus ib, since it lies in an algebraic in a finite extension, hence is algebraic over Q. So, a plus ib belongs to Q bar. The other way is a little more involved.

(Refer Slide Time: 06:32)

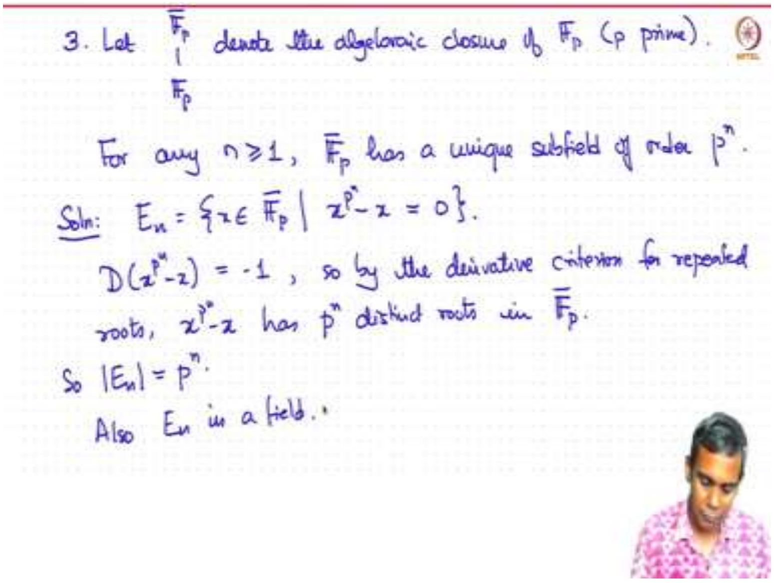


Now, if a plus ib belongs to Q bar, we want to show that a and b are, where a and b are real numbers. We want to show that a and b lie in Q bar R. Now a plus ib belongs to Q bar. No, let us let us not do it like that. So so first we will use the, we will use problem one. Problem one says that if a plus ib belongs to Q bar, then a minus ib also belongs to Q bar.

So, what we have is since a plus ib and a minus ib belong to Q bar, we have Q of a plus ib a minus ib is a finite extension of Q and so because again, by the same argument, it is generated by two algebraic elements. But a can be written as a plus ib plus a minus ib by 2 and b can be written as a plus ib minus a minus ib by 2i.

So, a and b lie in this field Q a plus ib, a minus ib, which is extension of finite degree. Therefore, a and b belong to Q bar, which implies that a and b belong to Q bar intersect R, which is Q bar R, just by definition of Q bar R, we assume that a and b are real numbers. So here is the thing that if a plus ib is algebraic, then it is real part a and it is imaginary part b are algebraic real numbers.

(Refer Slide Time: 08:47)



Let us move on to problem three, which concerns the algebraic closure of a field of positive characteristic. So, let Fp bar over Fp. So, your Fp denotes the field with p elements, where p is a prime number. Then for any integer n, any positive integer n, maybe I should say n greater than 1. No, I can take n equals 1. So, for any integer positive integer n, Fp bar has a unique sub field of order p to the n.

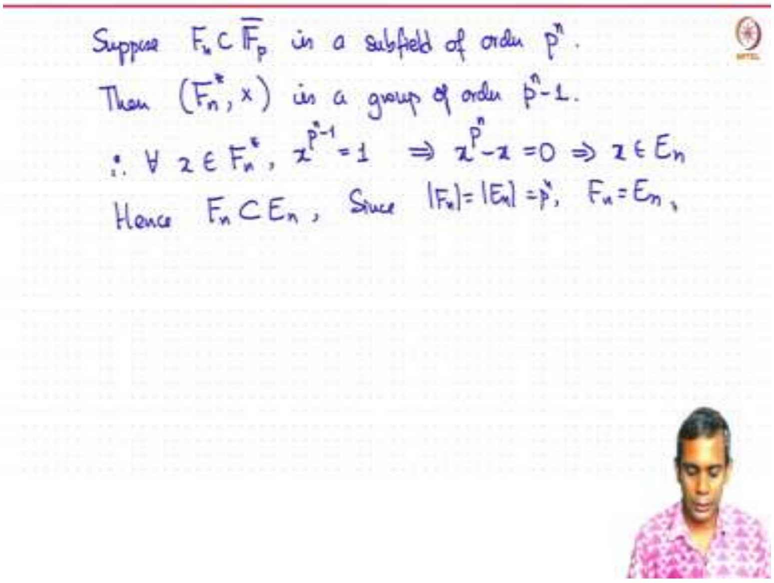
This is quite similar to the analysis we did when we looked at, we looked at the classification of finite fields and when one finite field contains the other, so you can try solving it yourself. And if not, can watch me solve it. So here is the solution. So, just define En to be the set of all elements x in Fp bar, such that x to the p to the n minus x is equal to 0.

Then note that if we take this polynomial x p to the n minus x, D of this polynomial is equal to minus 1 because p to the n is 0 in a field of characteristic p. So, by the derivative criterion for repeated roots, x to the p to the n minus x has p to the power n distinct roots and all of them lie in Fp bar because Fp bar is the algebraic closure of Fp.

So, it has p to the n distinct roots in Fp bar. And so, cardinality of E to the n of En is p to the power n. Also, En is a field. I will not work out the detailed solution of this, we have already seen it when we were classifying finite fields. So, you just have to show that if x and y are roots of this polynomial, then x plus y and xy are also roots of this polynomial.

And the interesting case is for x plus y where you use the binomial theorem, but when you use the binomial theorem with the power of p, then all but two terms will become 0, because those all the binomial coefficients except for the first and the last one will be divisible by 0. So, using that you can show that En is a field. So, what we see, we see here is that Fp bar has a field of order p to the n. So En is a field, sub field of Fp bar of order p to the n.

(Refer Slide Time: 12:45)



Now, we want to show that this is the only subfield of order p to the n. So now suppose Fn, well, maybe this notation is a bit ambiguous. So, but okay, I am not using bold letters. So Fn subset of Fp bar is a subfield of order p to the n. Then you can look at the nonzero elements of Fn. And you can look at them under multiplication is group of order p to the n minus 1, we just removed 0.

So, therefore, for every x in Fn star, x to the power p to the n minus 1 is equal to 1, which implies that x to the power p to the n minus x is equal to 0, which is just saying that x belongs to the field En, that we had considered earlier. And hence, Fn is contained in En, of course, 0 is in En too and every nonzero element of Fn is in En. But since Fn and En have the same order. We have Fn is equal to En, So En which consists of solutions of the equation x to the power p to the n minus x is the only subfield of Fp bar of order p to the power n.