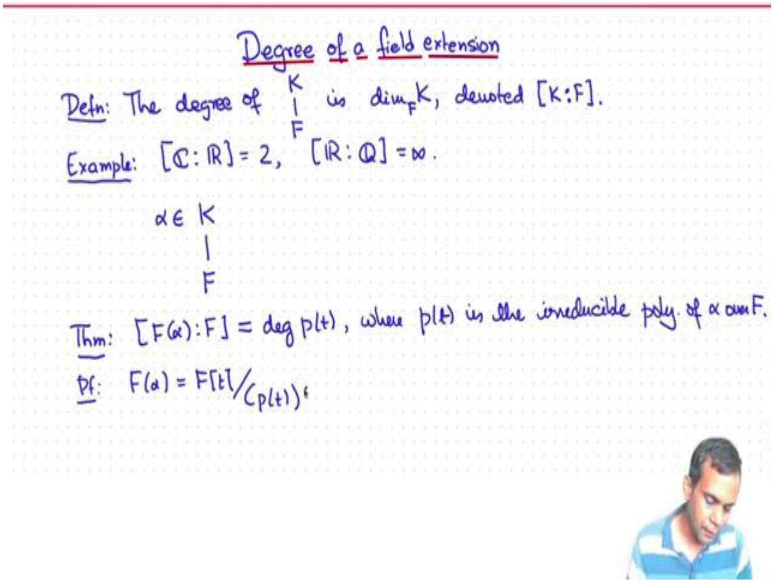
Algebra – II
Professor Amritanshu Prasad
Mathematics
The Institute of Mathematical Sciences
Lecture 4
Degree of an Extension

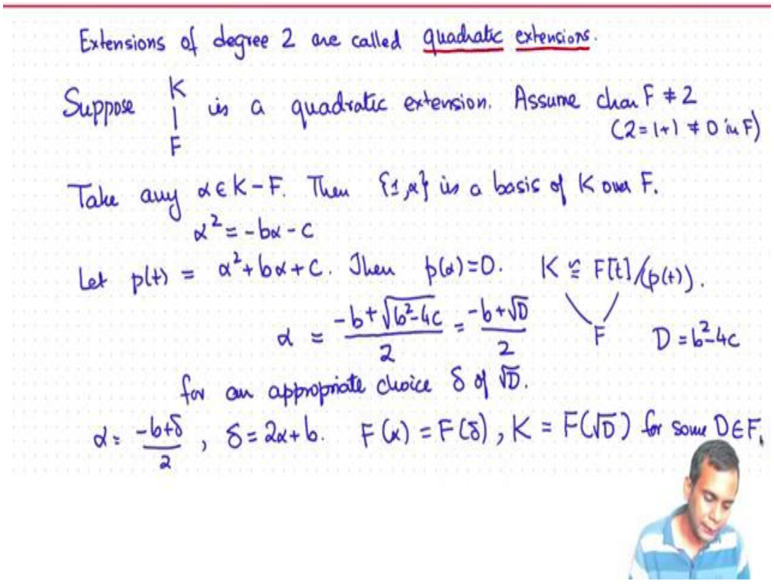
(Refer Slide Time: 00:14)



We define the degree of a field extension as the dimension of the larger field as a vector space over the smaller field. So, the degree of an extension F, K over F is the dimension of K over F, see F is a subring of K, and therefore, K becomes an F module. And in this case, F is a field. So, K is a vector space over F, it makes perfect sense to talk about the dimension of K over F. And the notation is K colon F. So, for example, the degree of C, over R is 2, but the degree of R over Q is infinity. So, degrees can be infinite as well. Now, what about the extensions generated by an element?

So, let us consider the situation where we have a field extension K over F and we have an element alpha. So, then we can ask what is the degree of F alpha over F? It turns out that it is just the degree of p t, where p t is the irreducible polynomial of alpha over F. And the proof is very simple, it is just that we know already that F alpha is F t mod the ideal generated by p t. And this F t mod p t, if p t is a polynomial of degree t, then 1t, t squared all the way up to t to the power t minus 1, form a basis of F t mod p t. So, the dimension of F alpha over F must be t.

(Refer Slide Time: 02:55)



The smallest non-trivial extensions of what are called quadratic extensions. So, extensions of degree 2 are called quadratic extensions. That is because they come from a quadratic polynomials. It is very easy to describe quadratic extensions exactly what they are. So, now, suppose K over F is a quadratic extension, then take any element of K which is not in F. So, alpha is in K minus F, then we know that 1 comma alpha is a basis of K over F just because it is a linearly independent set of size 2.

And so, what we know is that alpha squared must be a linear combination of 1 and alpha. So, I can write alpha squared as b alpha plus c, but just for what is about to come, I will write as minus b alpha minus c does not matter, but the point is now, that let p t be the polynomial alpha square plus b alpha plus c. So, then p of alpha is 0. So, we can write down a polynomial, a quadratic polynomial such that K is isomorphic to F t mod p t. And this is an isomorphism over F.

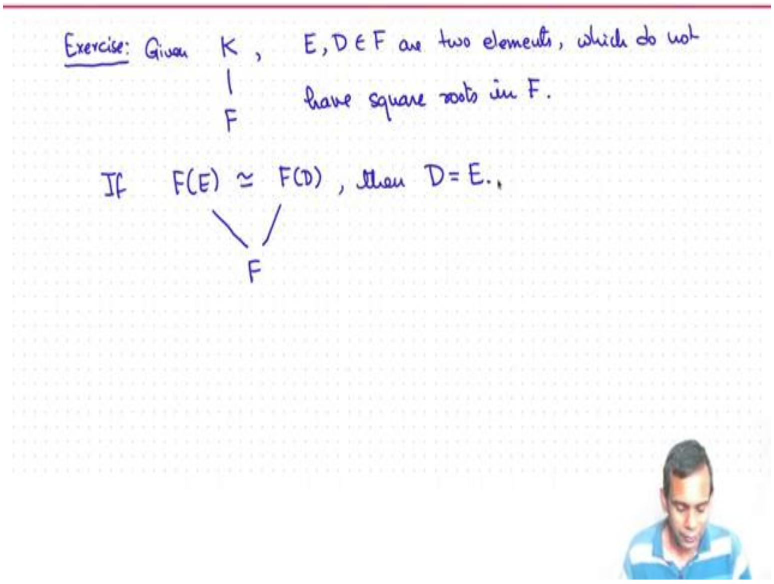
Now, we can simplify the situation further by trying to, so if we try to solve, so there are two roots of this polynomial, one of them is alpha and the other is something else. How are these roots given? So, know that the roots of p t are minus b plus or minus square root of b squared minus 4c, and we need to divide by 2. So, let us assume that F is not a field of characteristic 2. So, that means that 1 plus 1 is not equal to 0 in F. So, 2 is equal to 1 plus 1 is not equal to 0 in F with that assumption we can divide by 2, 2 is non-zero, so, we can divide by 2 and so we get that these are the roots and 1 of them is alpha.

So, there is anyway always a choice of square roots of b squared minus 4c. So, let us just write to choose a square root in such a way that this is alpha. So, let us say we have alpha equals 4 an appropriate choice, so let us call this thing D, b squared minus 4c. And so, this is minus b plus root D by 2 for an appropriate choice of root D, let us call it delta. So, what we have is that alpha is minus b plus delta by 2 and we can also write delta is 2 alpha plus b.

So, what these 2 identities mean is that Q alpha is equal to Q delta because, if a field contains alpha and not Q, I guess what I want to say is F alpha and F delta, this is general and this is because if a field contains alpha, and it contains F, then it must contain 2 alpha plus b because b is in F and 2 is in F, so, 2 alpha plus b must be in that field. So, that means the delta is in that field. So, F delta is contained in F alpha.

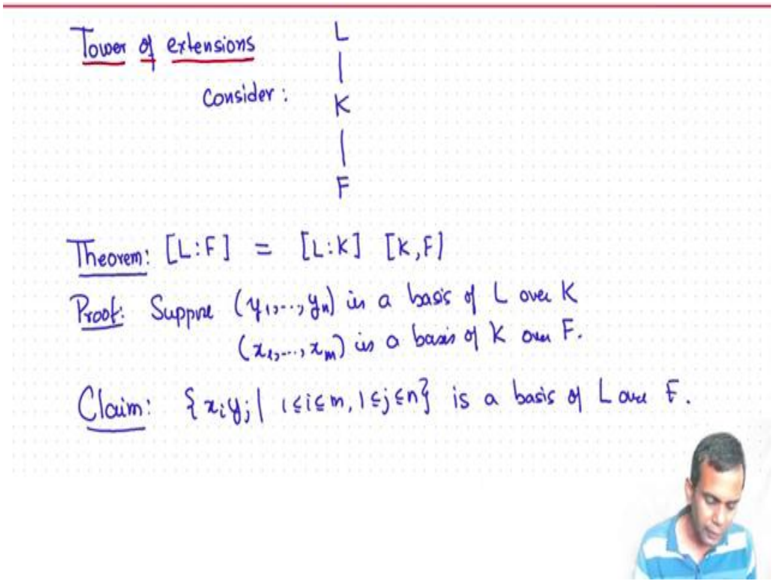
Conversely, if a field contains delta and it contains F then it must contain minus b plus delta by 2 which is alpha. So, F alpha is contained in F delta. So, we have that F alpha is equal to F delta. So, this field extension, this quadratic extension of degree 2 can be just written as it is the extension generated by the square root of some element D in K. So, it is F adjoint delta, or we can write F adjoint square root D for some D. So, every quadratic extension is of the form, well if you are working inside a larger field then it is of the form, it is generated by the square root of a single element in F. So, for some D, this D is in F for some D belonging to F.

(Refer Slide Time: 09:41)



Here is an exercise for you. So, suppose you have some field extension K over F and not necessarily quadratic and E and D belonging to F are two elements without square roots, so they belong to F, which do not have square roots in F. So, then you can talk about F E, and you can talk about F D. So, then F E is isomorphic to F D over F, show that D is equal to E. So, what is the saying is that all the quadratic extensions of F inside K correspond to elements of F, which are not square roots and which are not perfect squares in F itself.

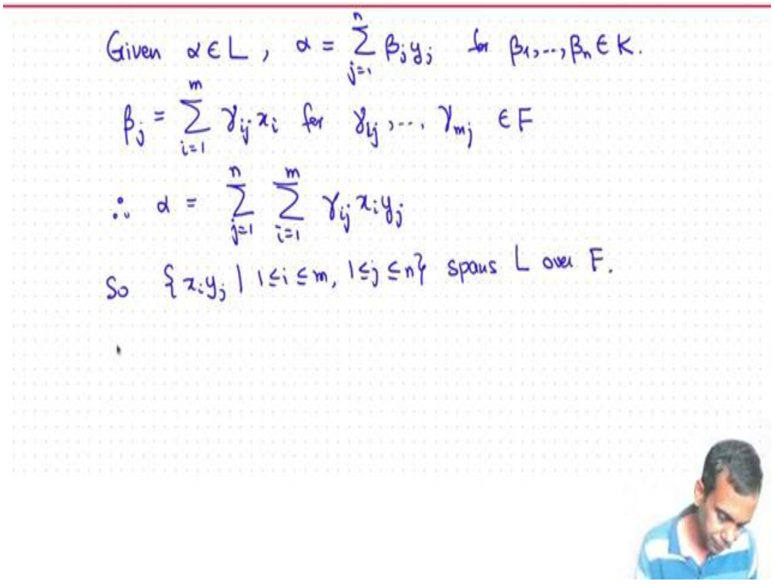
(Refer Slide Time: 11:08)

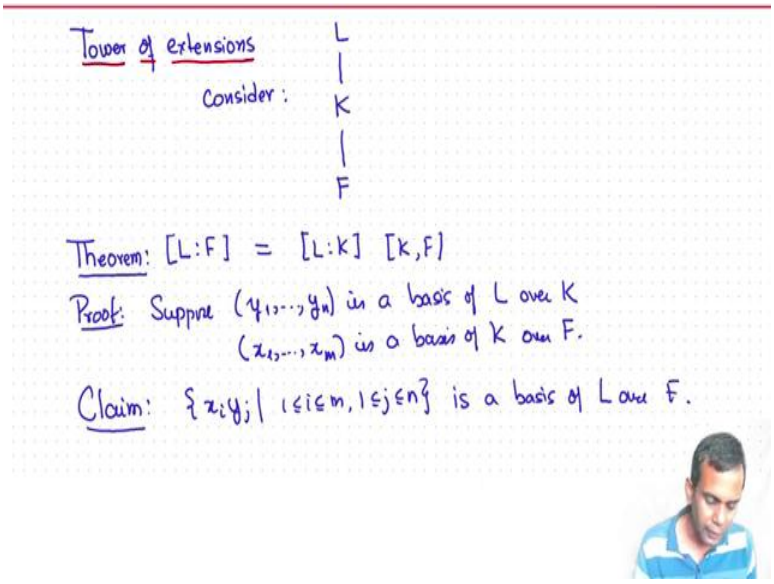


Now, we will talk about the degree of a tower of extensions, this is a very important result. So, by a tower here, not a very tall tower in this case of extensions, I mean 3 fields L containing K containing F, so you consider such a tower of 3 fields. And so, then the question is what is the relationship between the degree of L over F and the degree of L over K and the degree of K over F. And it turns out that the degree of L over F is precisely the product of the degree of L over K and the degree of K over F. This is not a very difficult theorem to prove, if you just think about it, you will probably come up with a proof very similar to what I am going to give here.

So, you can try pausing the video and trying to come up with the proof or you can watch a little bit and then try to finish the proof. So, what we will do is, we will construct a basis of L over F from a basis of L over K and a basis of K over F. So, suppose we have y1, y2, yn is a basis of L over K, and x1. So, these are all elements of L x1, x2, xm, is basis of K over F. My claim is that you look at the set xi, yj, where i goes from 1 to m and j goes from 1 to n, then this is a basis of L over F. You can try to prove this as an exercise, just pause the video and try to do it. If you cannot do it, then watch.

(Refer Slide Time: 13:41)

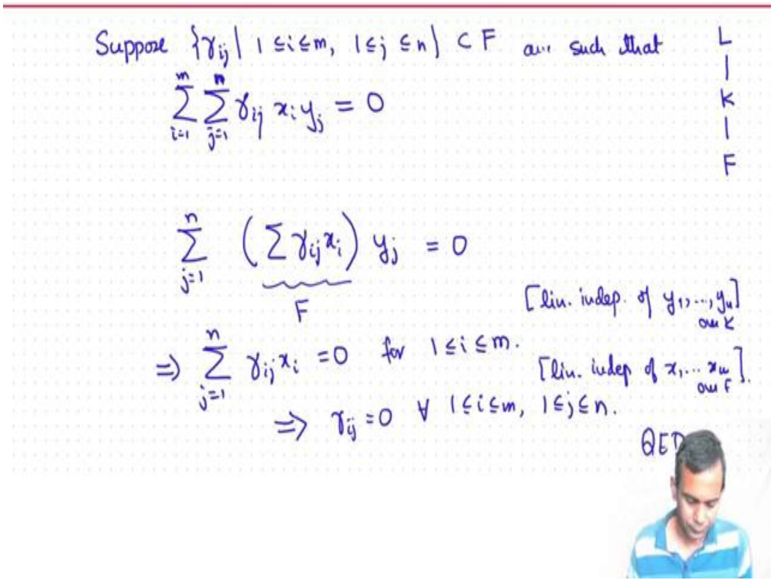


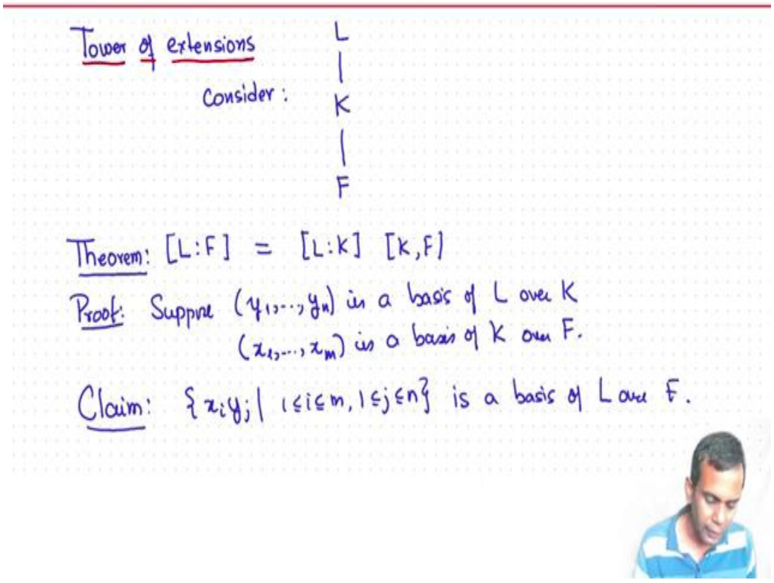


So, we need to show 2 things we need to show firstly, that L is spanned by the set. So, let us do that. So, given alpha in L. So, alpha is an element of L and we have a basis of L over K. So, we can write alpha in terms of the y1, y2, and yL with coefficients yn, with coefficients in K. So, alpha is equal to summation j goes from 1 to n, beta j, yl for some elements beta 1, beta n in the intermediate field K, but now this beta 1, beta 2, beta 3, and so on, these are all elements of K.

So, we can expand them in terms of this basis x1, x2, xm of F. So, we have beta j is of the form i goes from 1 to n, gamma ij, xi for gamma i 1j gamma mj in and these are going to be elements of F and just because x1, x2, xm is the basis for K and so now combining these you can write summation j goes from 1 to n, summation i goes from 1 to m gamma ij xi yj and so this set xi, yj spans L and as a vector space over F, it remains to prove our linear independence.

(Refer Slide Time: 16:23)





So, now, for linear independence. Suppose, we have scalars gamma ij 1 less than or equal to i less than or equal to m, 1 less than or equal to j, less than or equal to n. These are elements of F the smallest field here such that summation gamma ij, i equals 1 to m, j goes from 1 to n, gamma ij xi yj is equal to 0, we need to show that each of the gamma ij is equal to 0. So, now firstly, so just to recall we have L and then that sitting over K and that sitting over F. So, firstly, we will use the fact that the y1, y2, up to yn are linearly independent over K. So, this sum can be written as summation j goes from 1 to n.

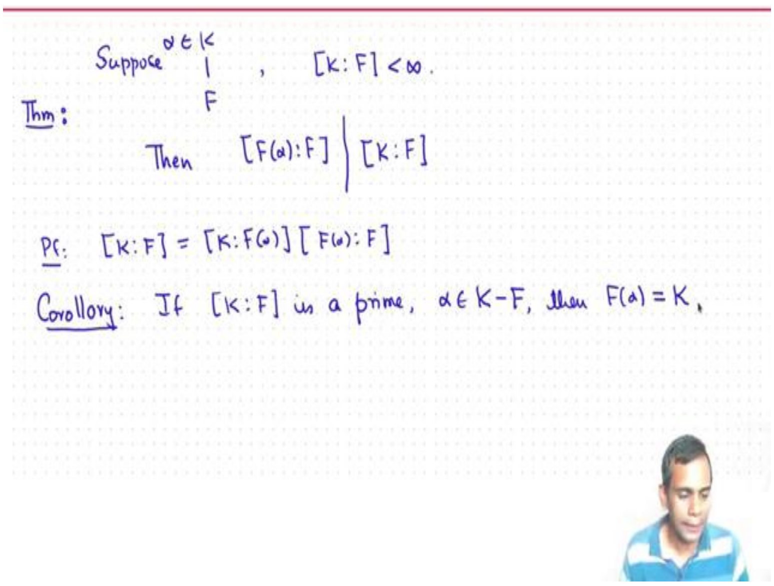
And then we have gamma, let us write like this summation gamma ij, xi and then over yj. So, what we have is this sum is equal to 0. And where do these elements live? Well, this gamma ij is live in F and this yj is live in K. So, this thing lives in F and so, these are in F and this is a basis of L over K. So, since this is the basis of L over K, this implies that summation j goes from 1 to n, gamma ij, xi is equal to 0 for every i between 1 and m.

But that because the x1, x2, xn form a basis of K over F, that would mean that each of these gamma ij is also equal to 0. Just from the linear independence of the xi's So, this step is by the linear independence of y1, yn and this step is the linear independence of, by the linear independence of y1, yn over K and this is of x1, xm over F. And that is completes the proof.

In the statement of this theorem, nowhere to dimension that the degree of a L over K is finite or the degree of K over F is finite. So, but in the proof, I assume the degree of L over K is finite and the degree of K over F is finite. But this theorem actually holds. In general, even if the degree of L over F is infinite, or the degree of L over K is infinite, or the degree of K over F is infinite. So, a product of infinity and any finite number is to be taken as infinity. And the product of infinity and infinity is, of course, taken to be infinity.

And the same proof goes through except that instead of finite basis, you may have to take infinite or maybe even uncountable bases. And you would still have this basis of L over F, which would be infinite. And so, this theorem also holds in the case of infinite extensions. Now, this theorem has some very, it is a simple theorem and the proof as you saw was not very difficult, but it has some very interesting consequences.

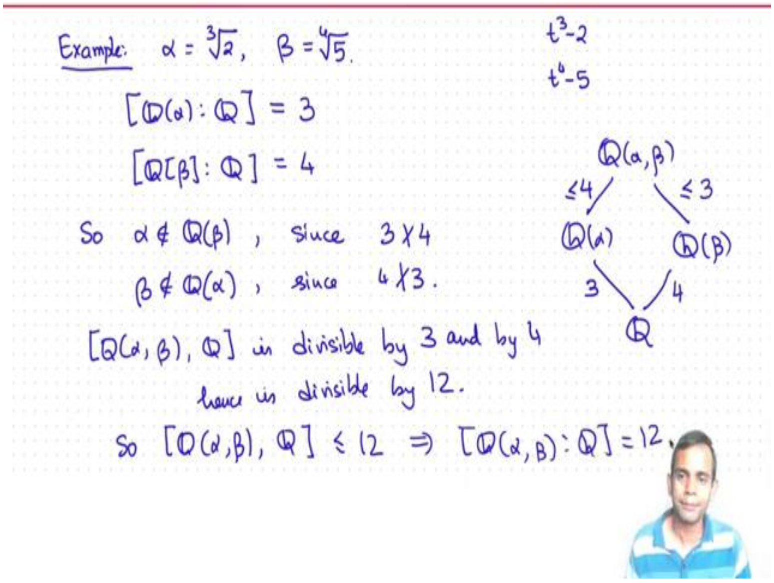
(Refer Slide Time: 21:05)



So, one is, so let us suppose that we have an extension, let us just call it K over F. And we have alpha here. And the index of K over F is finite. So, if it is infinite, this really will not say anything, then what we know is that the index of F alpha over F is going to divide the index of K over F, so this is a theorem. Why? Well, because the index of K over F is just the index of K over F alpha times the index of F alpha over F.

So, the index of F alpha over F better divide the index of K over F. A very surprising consequence of this is the following that if the index of K over F is a prime and alpha belongs to K but is not in F, then F alpha must be equal to K because F alpha is clearly larger than K. So, the degree of F alpha over F would be some divisor of p but only divisor of p are p and 1 itself the index cannot be 1 because F alpha is larger, strictly larger than K. So, it has to be p, it is also kind of useful in analysing certain extensions, let us look at an example.

(Refer Slide Time: 23:08)



So, let us take work over the rational numbers. So, let us take alpha to be cube root of 2 and data to be 4th root of 5 for example, then we know that Q alpha over Q, this should have degree 3 because alpha satisfies the polynomial t cube minus 2 equals 0 which is of degree 3 and this is irreducible over Q. And we also know that Q beta over Q is 4 because beta satisfies the polynomial t to the power 4 minus 5.

So, this means that alpha cannot lie in Q beta. Because if alpha was in Q beta, then q alpha would be a subfield of Q beta and its degree would divide the degree of Q beta, but 3 does not divide 4. So, so we can see since 3 does not divide 4, and similarly beta does not belong to Q alpha, maybe I should just write the standard notation round brackets beta Q, beta does not belong to Q alpha, since 4 does not divide 3 of course.

And what can we say about the field generated by both the elements Q alpha Q beta, so we know that Q alpha, so we have this field generated by Q alpha-beta, it contains the field Q alpha, it also contains the field Q beta and they both contain the field Q. So, this is the, it is called a diamond of fields. And so, what we know is that the degree of this by, so here the degree is 3, here the degree is 4. So, the degree of Q alpha-beta over Q is divisible by 3 and 4, and by 4, hence, it is divisible by 12.

But we also know that the degree of Q alpha-beta over Q beta, this has to be less than or equal to 3, because alpha satisfies the equation t cube minus 2, which is an equation with coefficients in Q, but it is also an equation with coefficients in Q beta. So, alpha satisfies a polynomial of degree 3 over Q beta.

And so, it is irreducible polynomial must be of degree less than or equal to 3. So, we know that the degree of Q alpha-beta, Q beta is less than or equal to 3. Similarly, you could argue that the degree over here must be less than or equal to 4. And so, what we get is Q alpha-beta over Q is less than or equal to 12 times, is less than or equal to 12, 4 into 3, which means that since we know that it is divisible by 12, it has to be exactly 12.