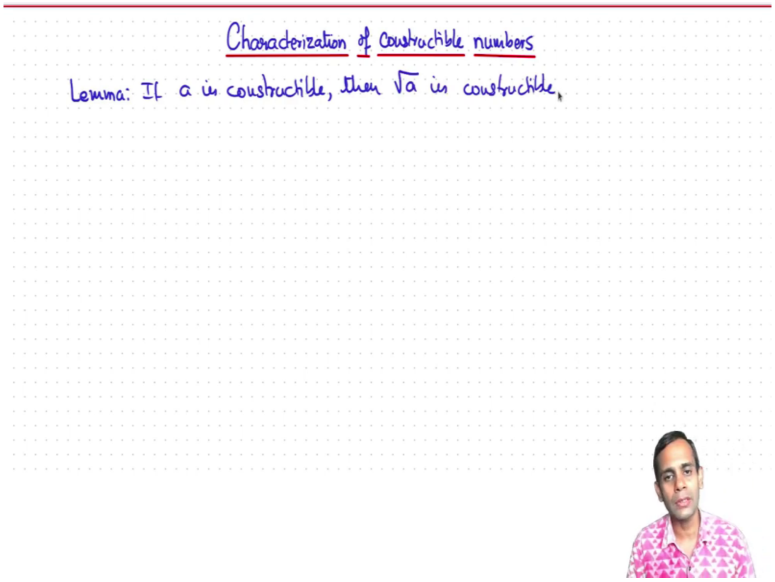
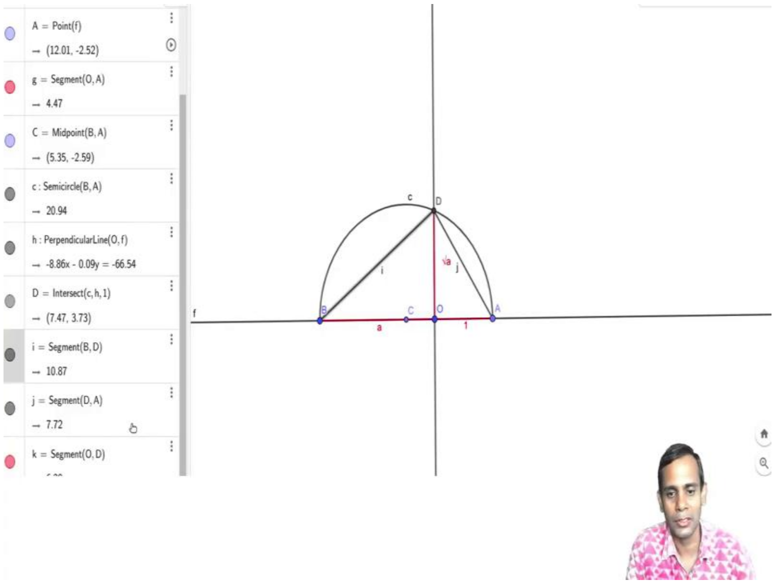
Alegbra - II
Professor Amritanshu Prasad
Mathematics
The Institute of Mathematical Sciences
Lecture 7
Characterization of Constructible Numbers

(Refer Slide Time: 0:15)



We are now ready to describe what all constructible numbers look like in terms of towers of field extensions. There is just one little construction we need before we can put all this into motion. And that is following that if you can construct a then square root, you can also construct square root of a. So let us call it a Lemma maybe, if a is constructible then square root a is constructible. And how does this construction work?

(Refer Slide Time: 1:06)

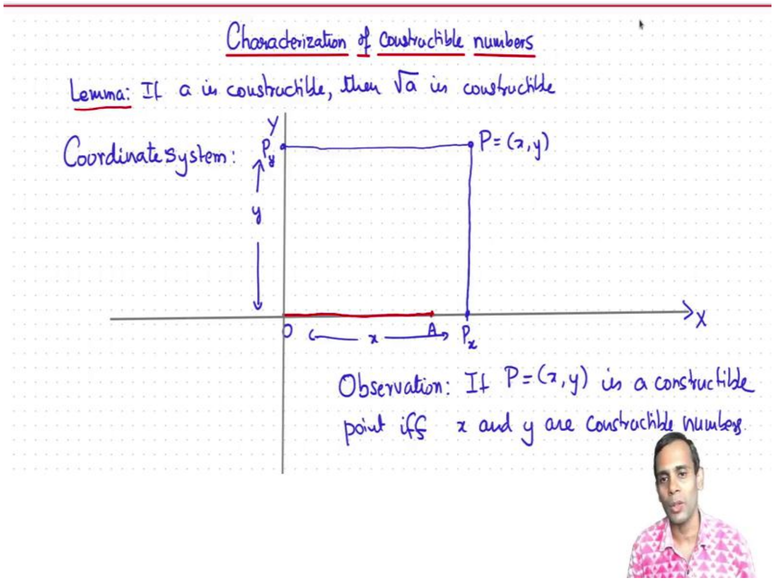


And let us use GeoGebra. So to start with I have this segment OA of length 1 and I mark off the left of O another segment of length A and now I am going to construct a segment of length square root A. So firstly what I do is I find the midpoint of A and B, let us call it C. So this we can do it again using straightedge and compass I already did this when we were trying to find a, construct square root of 2.

So we find the mid-point and then we draw a circle I am only drawing half of it here with center C passing through A and therefore also B because C is this midpoint of AB. So we construct the circle C and through O we construct a perpendicular to the line that passes through O A and B and then let us call the intersection of this new line with the circle D, with a circle C to be capital D. And now you look at, you join the line segments BD and you join the line segments BA, I do not really need to do this but I am doing it explain to you something.

So now you look at these 2 triangles ODB and a OAD in that order. These are similar triangles because I guess this is easy this angle here at B and this angle here at A they add up to 90 degrees and so that shows this angle here at B is the same as this angle ADO is same as the angle DBO. And so these 2 triangles are similar. Now since these 2 triangles are similar if I take this length OD and divide it by a that is the same as 1 divided by length OD. And so this length OD it cannot be anything but square root of a. It so having constructed a we can also construct square root of a as this construction shows.

(Refer Slide Time: 3:22)



So that is the proof of this Lemma and let us move on. So the other thing we need to do is to be able to construct a coordinate system. This will be convenient because right now what we have said is that a constructible number is the distance between 2 constructed points and you may have a lot of constructed points floating around it is difficult to keep track what are all the constructible numbers that you have created so far.

So we will create coordinate system and this we can do with straightedge and compass I will just do it by hand here. So you start with your lines segment OA and then you can draw a perpendicular to it using straightedge and compass. So firstly in fact maybe a given OA you can draw a line that is you know the x axis as just the infinite line that passes through O and A. I need to move it up a bit. So this would be my x axis.

And for my y axis I will draw a line, so let us just remember where OA was this is OA and for the y axis I will draw a line perpendicular to it. Which I can also construct by straightedge and compass. And now if I have any point Ps then I can draw a perpendicular from P to Y, to the y axis and I will call this a P subscript y or just little y and I can draw a perpendicular to the x axis and I will call this P subscript x.

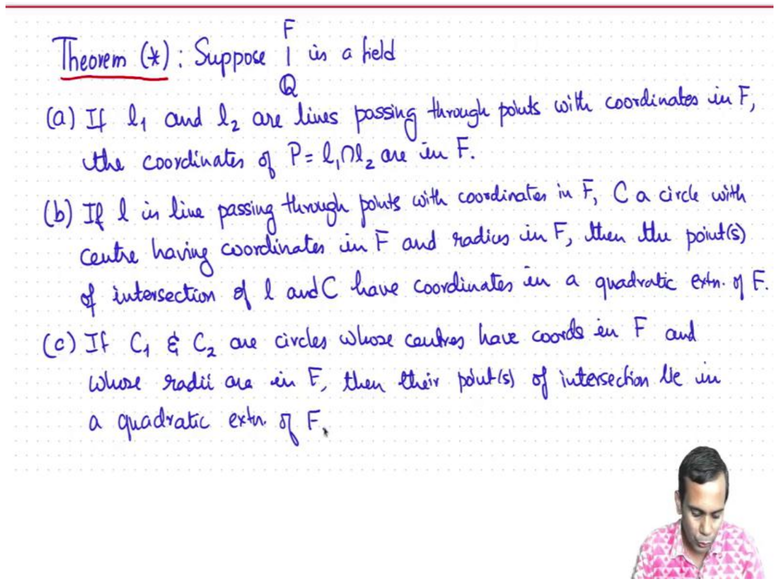
So we can always construct given a point we can the firstly given O and A which we were given at the beginning of our construction, we can construct the coordinate system the x axis is the line that passes through y ending the y axis is the line perpendicular to it and if we can construct the point P then by dropping perpendiculars we can construct the x coordinate and the y coordinate of the (()) (5:45).

So we can mark off a distance equal to the x coordinate of P and a distance equal to y coordinate of the P along the x and y axis respectively. So what we observe here is that maybe I will just call it in observation. If P equals x comma y is a constructible point then x and y are constructible numbers. But also if we can construct these distances x and y then we can mark them off along the x and y axis and draw perpendicular lines.

We can draw a line perpendicular to the y axis through this Y coordinate and a line perpendicular to x axis through this x coordinate and they will intersect in the point P. So also we can construct x and y we can the point P and with coordinates x comma y is constructible. So what I will do is I can change this from one-way implication to and if and only if. So point P is constructible if and only if its x and y coordinates are constructible numbers.

Now let us see what happens at each stage of a construction. So what at each stage of the construction you constructed at certain set of points and their coordinates would be a constructible numbers and now we can add a new point the new points we allow to add are either intersection of lines passing through the constructed points or intersection of circles with center at the constructed points and radius which is constructible or a circle and a line. So in each of this cases let us see what are the new constructible numbers we get as x and y coordinates of constructible points.

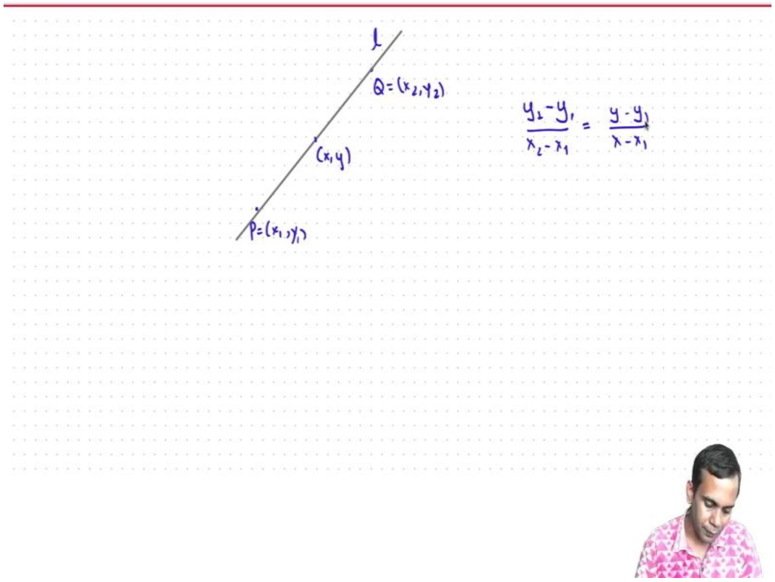
(Refer Slide Time: 8:11)



So here is a theorem I will call it theorem star it going to use it later, it is going to be important in what follows. So the theorem says that suppose I have a field extension F over Q is a field. Now we look at three cases if l1 and l2 are lines passing through points with coordinates in F. Then the coordinates of l1 intersection l2 are in F. We do not even need to go to an extension. And b if l is a line passing through points with coordinates in F. and C is a circle with center having coordinates in F and radius having coordinates in F.

So maybe I should say center and well radius in F center having coordinates in F and radius in F, then the points of intersection of l and C they could be only one if l is tangential have coordinates in a quadratic extension of F. And the last case is where you have if C1 and C2 are circles whose centers have coordinates in F and radii are in F then their points of intersection again they could be just one point but they are tangential their points of intersection lie in a quadratic extension of F.

(Refer Slide Time: 12:17)

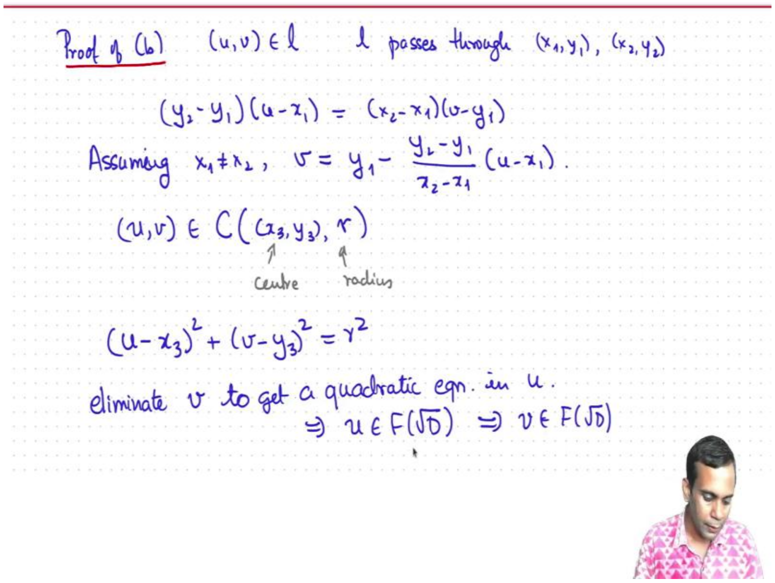


So part a is rather simple what you have to do is if you have two points P equals x1 y1 and Q equals x2 y2 then this line l that passes through them, this line l that passes through them its points will be given by an equation like you know if you have a point x comma y here then what we know is that y2 minus y divided by, so we can assume that either x1 is not equal to x2 or y1 is not equal to y2.

And now if I assume that x1 is not equal to x2 then I can write this like this y2 minus y1 divided by x2 minus x1 is equal to y minus y1 x minus x1. If you want, you can move this to the other side and write it in form like this does not involve any division. And so not have to worry about x equals x1 or x equals x2 equals x1.

And then from this you can show that if you have two such lines then their point of intersection will lie in the same field that it will just you can construct it by addition and multiplication of coordinates of x1 y1 and x2 y2. So you will have this kind of conditions for two lines, I am going to leave this as an exercise for you and move on to the slightly more interesting cases of a circle and line and 2 circles.

(Refer Slide Time: 14:15)

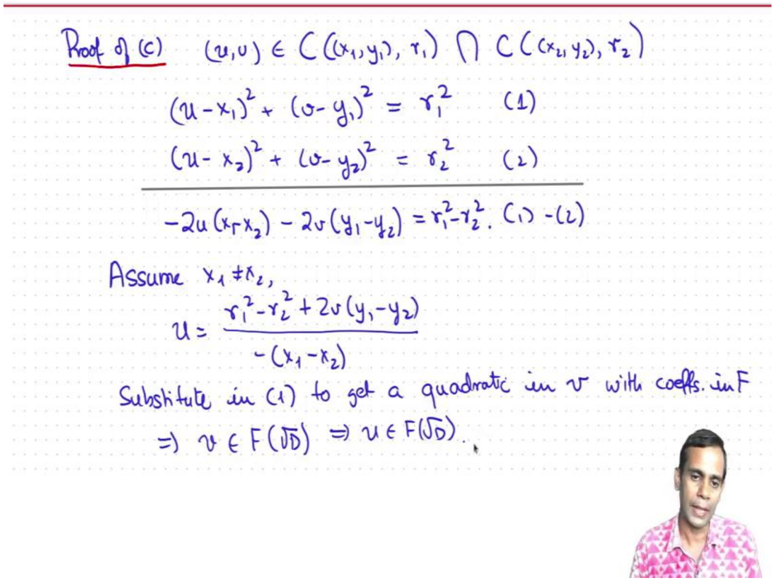


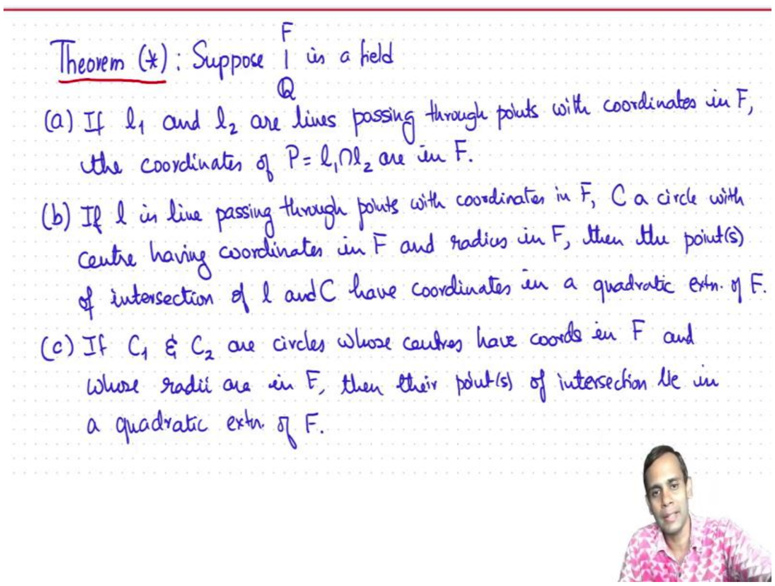
So let us go to the proof of part b. So we have a point u, v in the line l where l is the line passing through x1 y1, x2 y2 and as I already explained the condition for the point to lie on this line is that y2 minus y1 into u minus x1 is equal to x2 minus x1 equals into v minus y1. And if we assume that, so we have to assume that this points x1 y1 and x2 y2 are un, are not the same. So assuming that for example x1 is not equal to x2, if they are equal then we have use the fact that y1 will not be equal to y2.

We can solve this and write v in terms of u. So v is going to be y1 minus y2 minus y1 divided by x2 minus x1 into u minus x1. And now if u v belongs to the circle with center let say at x3 comma y3 and radius r. So this is the center and this is the radius that is my notation. Then what we know is that u minus x3 squared plus v minus y3 squared equals r squared. So what we get is that we can eliminate now, we can eliminate from this equation u, we can eliminate from this equation v using v equals this expression for v in terms of u.

So eliminate v to get a quadratic equation in u and so as we have seen, whenever you have a quadratic equation its solutions lie in the extension of the field in which the coefficients lie by the square root of the discriminate. So u v which implies that u belongs to F adjoints square root D where D is already in F and this implies that also v belongs to F square root D. Because v can be written in terms of u by this equation here. So u and v both lie in F square root D.

(Refer Slide Time: 17:38)





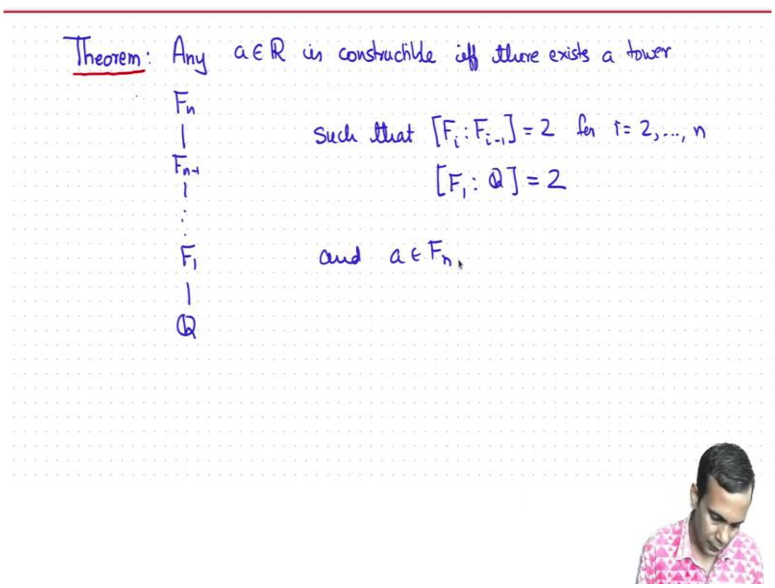
Now let us move on to the prove of c. We have a point that lies on two circles. So let us say u v the circles are the first one is with radius x center x1 y1 and radius r1 and also it lies in the circle with center x2 y2 and radius r2. Then what we have is that this point u and v satisfy the equations u minus x1 squared plus v minus y1 squared equals r1 square. This is equation 1 and u minus x2 squared plus v minus y2 squared equals r2 square, this is equation 2.

So now let us just add these equations or rather maybe subtract these equations. So we take equation 1 minus equation 2 then this quadratic terms will cancel out and we will get a linear equation involving u and v. So what we get is a minus 2u x1 minus x2 minus 2v y1 minus y2 is equal to r1 square minus r2 square. So using this we can eliminate let say assume that x1 is not equal to x2 then we can write u as r1 square minus r2 square plus 2v y1 minus y2 to whole divided by x1, negative of x1 minus x2.

And so you can eliminate u from either of this equations and solve for v. So substitute in 1 to get a quadratic equation in v and with coefficients in F. And so this implies that v belongs to F square root D but then u can be recovered from v using this function here. So which also imply that u belongs to F square root D. And so u and v lie in a quadratic extension over F.

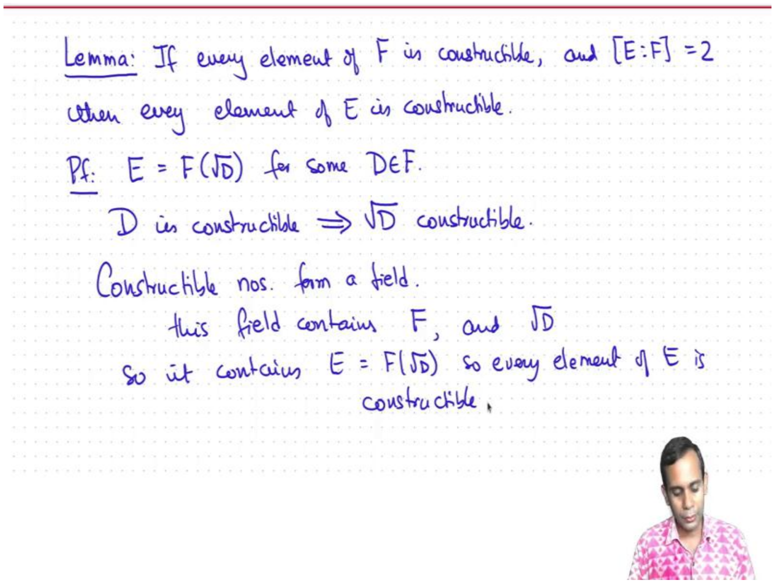
So we have shown with theorem star, we have proved theorem star which basically says that if some stage of our construction, all the points that we have constructed their x and y coordinates lie in some field F. Then any new point that we introduce at this stage of our construction its coordinates will lie in a quadratic extension of F or in F itself in case we are constructing a new point by intersecting 2 lines. But if it is a circle is involved, then it would probably lie in a quadratic extension of F.

(Refer Slide Time: 21:30)



And now with this you can kind a guess where all the constructible points come from, this is the statement a beautiful theorem now ready to prove. So a real number is constructible if and only if there exist a tower, Fn containing Fn minus 1 going to F1 containing Q such that Fi index Fi minus 1 is 2 for i equals 2 to n and also we assume that F1 in Q degree of F1 over Q is 2. And a number a belongs to Fn. So basically we are saying that constructible numbers are numbers that live in towers of quadratic extension.

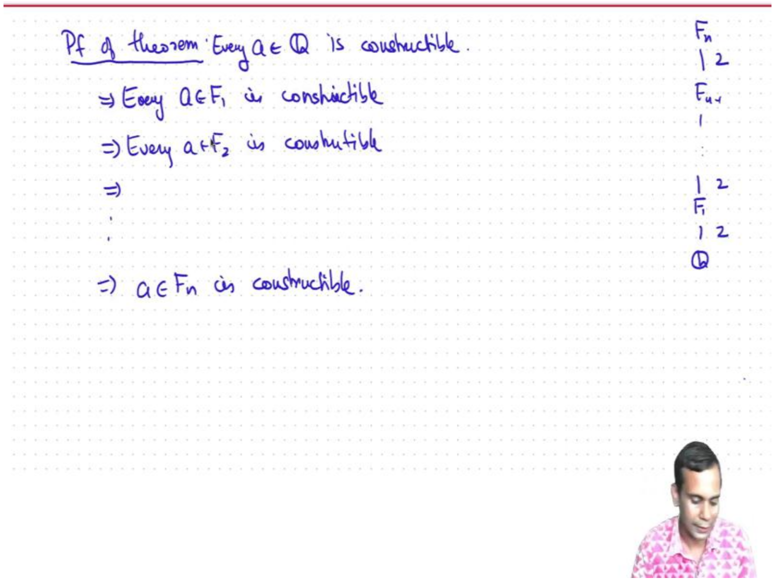
(Refer Slide Time: 23:05)

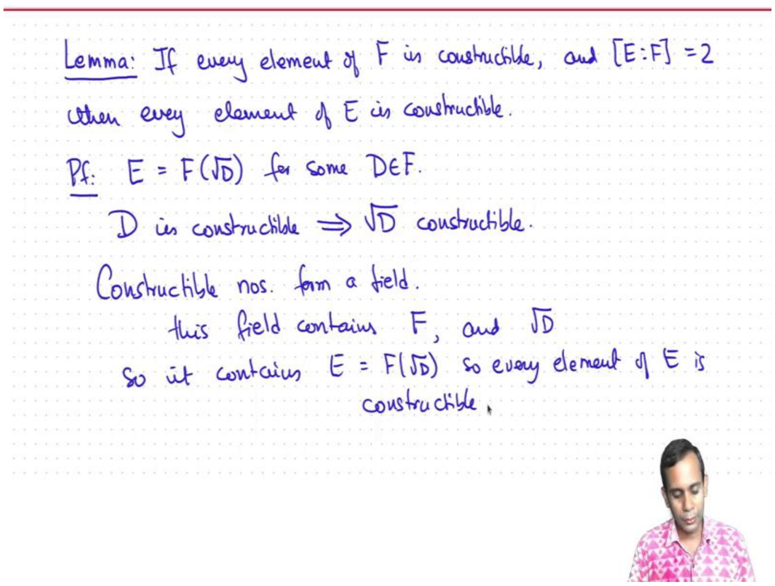


So let us see how to prove this. So firstly to prove it we will have a we will first state a simple Lemma which will make the prove easier to understand that if every element of a field F is constructible and E is an extension of F with degree 2 then every element of E is constructible. So this is taking care of one step of our tower. And proof, well we have already seen that if E is a quadratic extension of F, E is of the form F square root D for some D in F.

Now if we know that D is constructible which implies that square root D is constructible. Now constructible numbers form a field and what we have seen is that this field contains F and root D. So it contains a smallest field containing both F and root D. So it contains E equals F root D. So every element of E is constructible. And that is the proof, so now we can prove a this theorem in one direction and which is that suppose a lies in a tower of quadratic extensions.

(Refer Slide Time: 25:34)





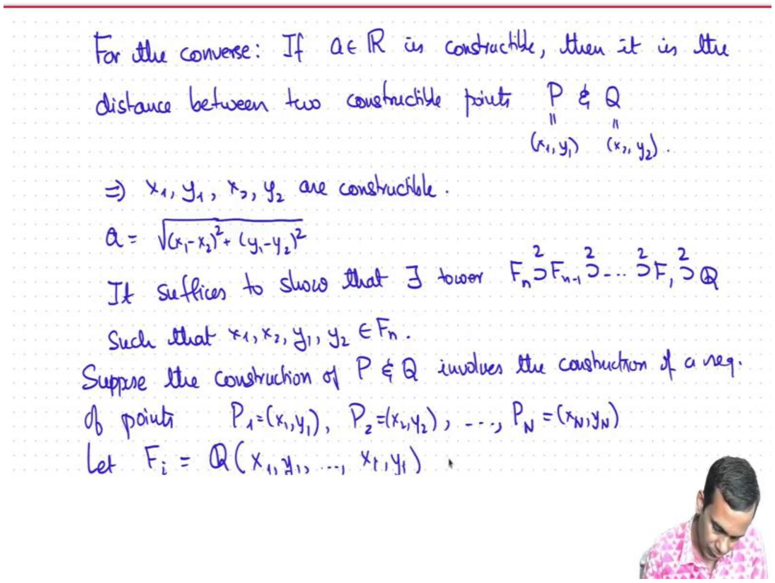
So now suppose proof of theorem if so firstly a in Q can be constructed a belong to Q is constructible. Why is this? Every rational number is constructible because 1 is constructible and constructible numbers from a field. Now any so if 1 is in a field then all rational numbers are in that field. So every element of Q is constructible and now applying this Lemma. So we have this you know we have this extension Fn Fn minus 1 F1 over Q.

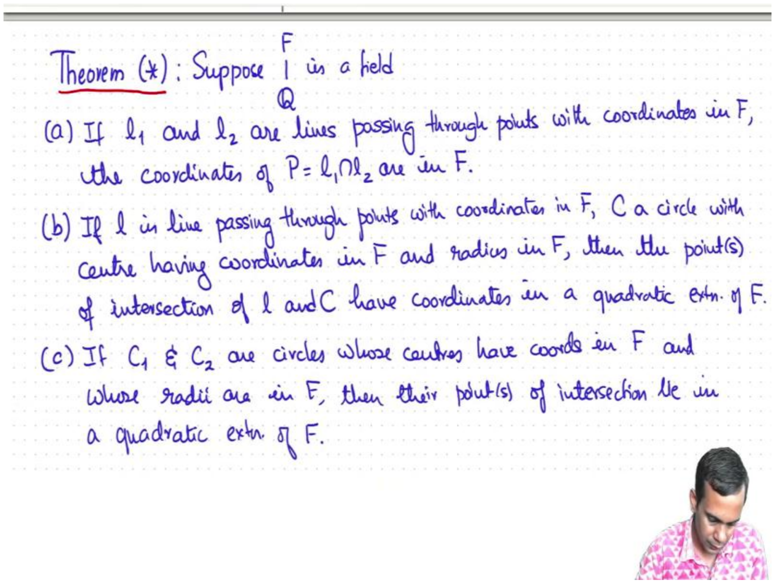
And each of this is a degree 2, each of this extension is of degree 2. So now every element in Q is constructible by this Lemma. This implies that a belongs to F1 is constructible. So maybe I should say every a in Q is constructible implies that every a in F1 is constructible by this

Lemma. And that implies that every a in F2 is constructible again applying that Lemma and so on, which means that every a in Fn is constructible.

So you apply this Lemma n times to show that every element of Fn is constructible. Now for the converse we will have to use theorem star. So this shows that every element of Fn is constructible. Now we want to show that if we have a constructible number then we can find a tower of quadratic extensions, so that lives in one of the fields in that tower.

(Refer Slide Time: 27:57)





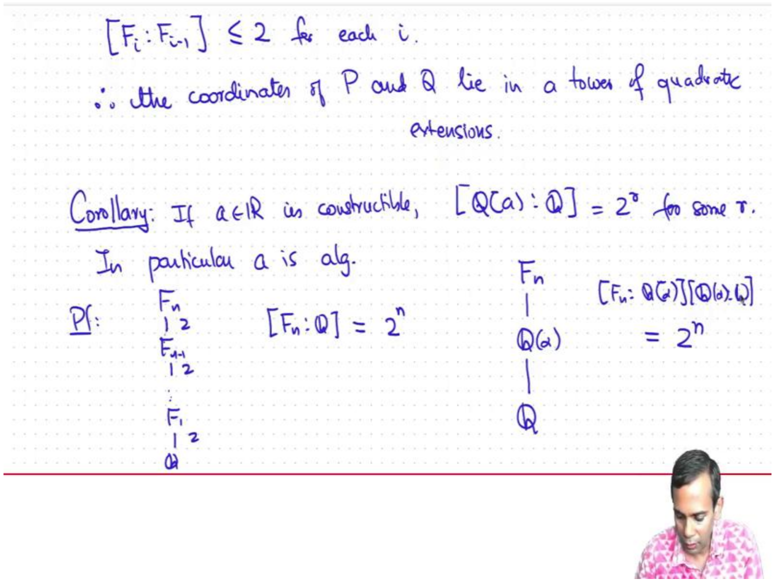
So for the converse, so if a in R is constructible then it is the distance between two constructible points. Let us call them P and Q so let say P is x1 y1 and Q is x2 y2. So this means that the coordinates x1 y1 x2 y2 are constructible. So it which and so now this distance between P and Q a is equal to square root of x1 minus x2 square y1 minus y2 square. So this is in a quadratic extension contained in these points.

So this means that of course if these are constructible then a is constructible. So it suffice to show, so a is a quadratic extension containing the field containing x1 y1 and x2 y2. So it suffice to show that there exist a tower now to just save space I will write my tower horizontally Fn contains Fn minus 1 contains F1 contain in Q and each of these of degree 2 of quadratic extensions, such that x1 x2 y1 and y2 are Fn.

So now let us, so these point P and Q are constructible. So let us say that the construction of the points P and Q takes place through several steps. So suppose the construction of P and Q involves the construction of a sequence of a points, let say P1, P2, Pn in this order such that each Pi is constructed by joining either two lines in the previous step of the construction or a circle and a line in the previous step of the construction or two circles in previous step of the construction.

Then what we have is that let Fi be the field extension of Q containing let us say that maybe I will just say P1 is x1 comma y1, P2 is x2 comma y2, Pn xn comma yn. Then if you look at this F which is x1 y1 up to xi yi for i goes from 1 to n. Then by theorem star which we have here, so each of these points is constructed by intersecting two lines at the previous step or intersecting a circle and a line at the previous step or intersecting 2 circles at the previous step.

(Refer Slide Time: 33:01)



So theorem start will tell us that, theorem star will now tell us that Fi index Fi minus 1 is either 1 or 2. And therefore we have that coordinates of P and Q lie in a tower of quadratic extensions as claimed. A very interesting corollary of this is the following. If a number a is constructible then you look at the degree of the extension Q a over Q, this has to be a power of 2. Some non-negative integer r, in particular a algebraic of course.

This is because we have a tower Fn Fn minus 1 F1 Q and each of these extension is of degree 2 the degree of Fn over Q is going to be 2 to the power n, it is going to be the product of these extensions. And now what we have is, if our element is constructible then it lies inside in some Fn like that. So Q alpha is an extension that is between Q and Fn and so Fn Q alpha, Q alpha Q this is 2 to the power n. So the only possibility for Q alpha the index the degree of Q alpha over Q is that it has to be the 2 to the power r for some r less than or equal to n.