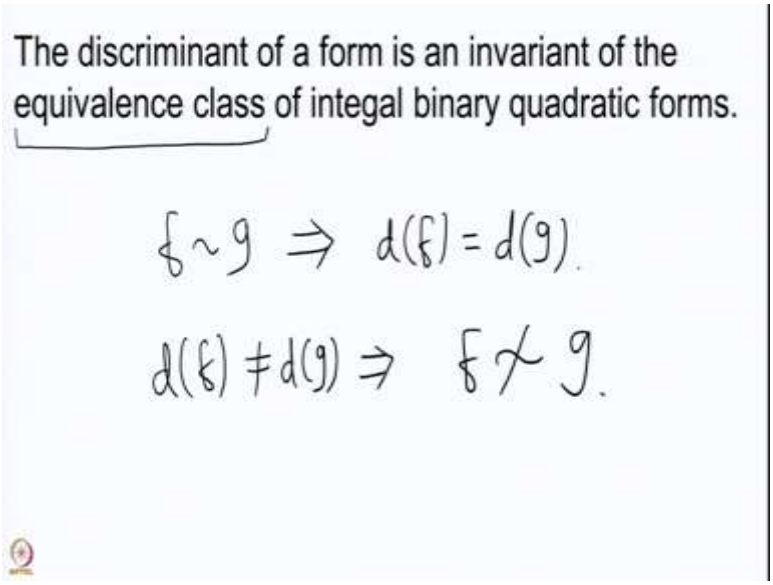
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 41
Reduction Theory of Integral Binary Quadratic Forms

Welcome back. We have defined discriminant of an integral binary quadratic form and we studied the discriminant at some length in our last lecture and the most important thing about the discriminant is that it does not change when we apply our transformations to the binary quadratic forms.

(Refer Slide Time: 00:42)



So this is in front of you that the discriminant is an invariant of the whole equivalence class of integral binary quadratic forms. That means if I have f equivalent to g then the discriminant of the form f is equal to the discriminant of the form g. We have introduced this equivalence in the hope that we could go from a difficult form to a simpler form and we saw also that value sets do not change. Now we also have that is result that a discriminant does not change.

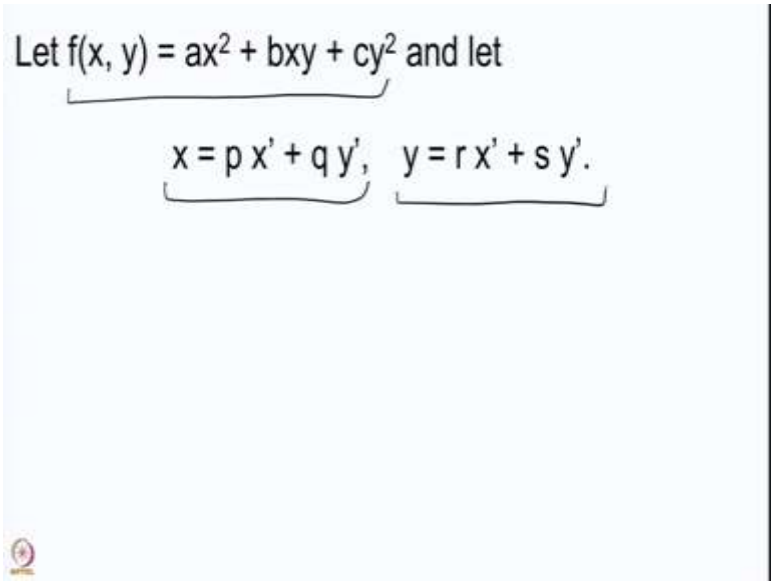
So later what we are going to do is that we are going to fix these discriminants and we would like to identify all integral binary forms of a given discriminant. Ofcourse, if you have two discriminants, if there are two integral binary quadratic forms and their discriminants are different then they cannot be equivalent because we have seen just now that discriminant is an

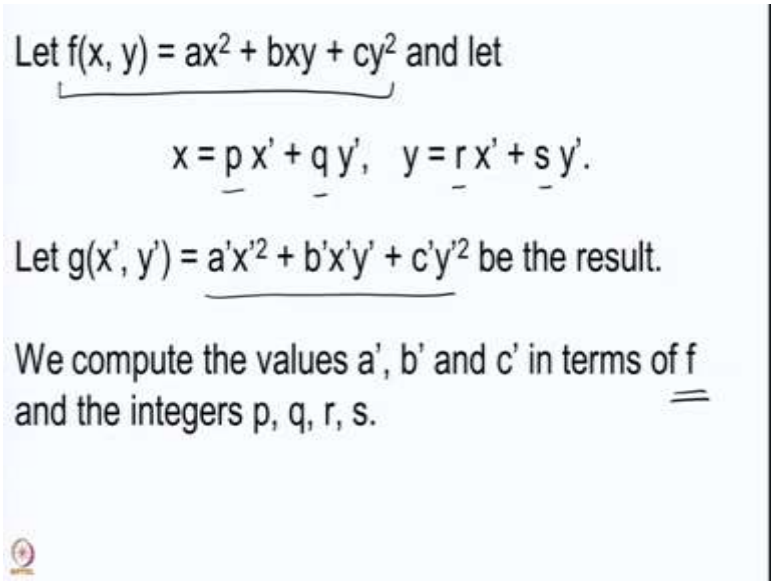
invariant for the equivalence class. So that is a very important statement when the discriminants happen to be different we get that the form f cannot be equivalent to the form g.

So the discriminant will help us in understanding the equivalence classes. It may happen that you may have two forms which are not equivalent, but they have the same discriminant. Therefore, we would like to understand the forms which have the same discriminants but are not equivalent. And so we will need to develop the theory of what is called a reduction of these integral binary quadratic forms.

But before that let us apply the transformations and see what is the change that happens for the coefficients. So because we had developed the matrix notation and many proofs were simple, we did not introduce this thing until now, but now we are going to do this.

(Refer Slide Time: 03:02)





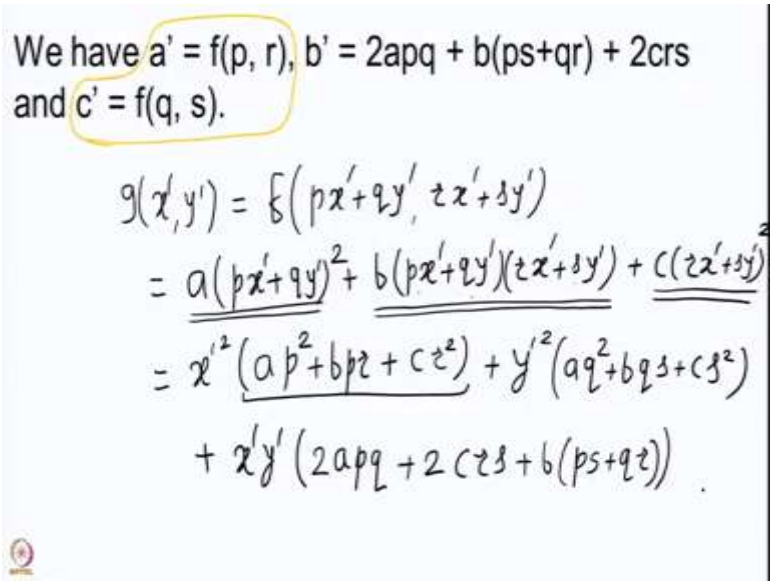
So we start with a, with an integral binary quadratic form ax square plus bxy plus cy square. We start with this form and we apply this transformation. We change x to x prime y prime with coefficients p and q, y goes to rx prime plus sy prime. So what is going to happen is that we will get a different integral binary quadratic form. We call it g, this is the form that you get. So we have different coefficients now, a prime b primer and c prime and we want to explicitly determine what happens to these coefficients.

How are they? How do they look? What is the value of these in terms of the earlier numbers that we have introduced? So we compute the values a prime, b prime and c prime in terms of the

numbers that we have. So we have the numbers a, b, c or in other words we have the form. So we have the form f which is the same thing to say that we have the numbers a b c and we have these p, q and r and s. So we have these 7 numbers. And ofcourse a prime, b prime, c prime should be polynomials in these 7 numbers in some way.

And we simply want to write the explicit description of a prime, b prime, c prime in terms of these numbers. But you know when we write this description, it is good to observe something. So for instance the a prime and c prime, the coefficient of x prime square and the coefficient of y prime square these have a nice form.

(Refer Slide Time: 04:58)



And here we have them a prime is the earlier integral form evaluated on p and r and similarly c prime is also given by the same integral binary form evaluated at q and s. B prime has a slightly complicated expression but we will come to handling b prime also. So let us start doing competitions and let us see what we get. So we have that g of x prime y prime is f of px prime plus qy prime rx prime plus sy prime.

So we have a px prime plus qy prime whole square plus b px prime plus qy prime into rx prime plus sy prime. And finally we have c into rx prime plus sy prime square. So what are the terms for x prime square, let us compute. So for x prime square we are going to get coefficients from here, you will get a into p square. From here we will get no such further term for x prime square. The term for x prime square coming from here will be b into p into r.

And the term for y prime square coming from here will be c into s square. So we immediately observe that this is nothing but the form f p, r which is given by the integers a, b and c on ps comma r. We are looking at x prime square so we should get r square coming from here. So we immediately observe that this value is nothing but the earlier integral quadratic form evaluated on the integers p and r.

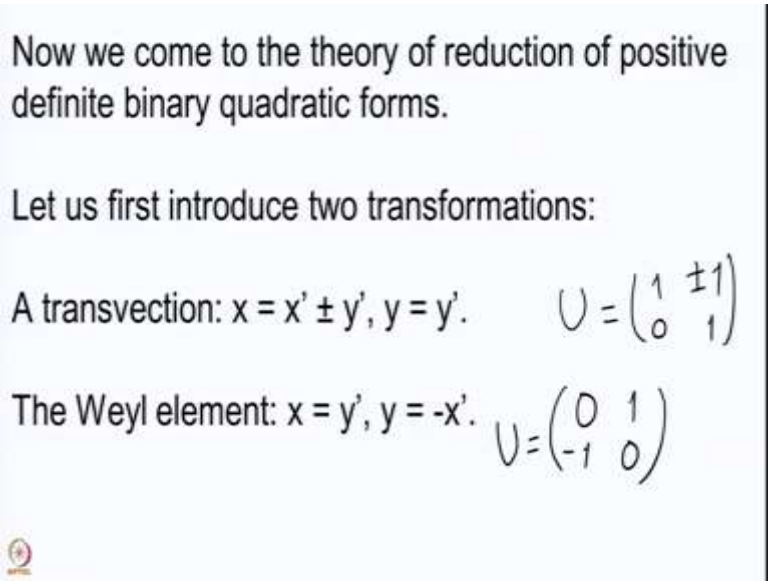
Similarly and I will not do this computation that y prime square is nothing but f of qs. So that is aq square plus bqs plus cs square. And now we need to compute the coefficient of x prime y prime. So the contribution from this term will be apq into 2. So we get two times a times pq. The contribution coming from here will be 2 times c times rs. So that accounts for these two terms already.

And now we get the contribution from this middle term which will be b in 2, I can have ps and I can have qr. So it gives me ps plus qr. So this completes the description. What we have done is to obtain the description for the coefficients of the equivalent form in terms of the earlier coefficients and the integers involved in the change of variables. The only important thing you should remember here is these things.

So these are the things that a prime, the next coefficient of x prime square is the earlier form evaluated on some pair of integers actually given by P and R, and the coefficient of y prime square is also the integral form that you started with, the form F evaluated on Q and S. These are the two important things that we are going to need. There is the formula for B prime is slightly complicated but B prime is something that we are going to handle in a different way later on.

So now we are going to look at the theory of transforming a form to a simpler form. So what is a simpler form? We have not made this concept very clear yet. We will give this concept also, but we are going to introduce two very important transformations.

(Refer Slide Time: 10:05)



So this is the theory which is called the theory of reduction of integral binary forms, but we are going to restrict ourselves to only positive definite forms. Remember our motivation was to study the forms like x square plus y square. We want to determine all natural numbers which are sums of two squares. We would like to determine all natural numbers which are sums of three squares, all natural numbers which are sums of four squares. Those are the things we want to do. So we would like to restrict ourselves to definite forms.

Now whether we take positive definite or negative definite, that is not a very difficult thing because once you have a negative definite form, you simply multiply all coefficients by minus 1. And you are going to get a positive definite from. Discriminant will remain the same, you will get a positive definite form because the value set which was earlier containing only negative values now it will contain only positive values and zero may be there that does not matter.

So negative definite form has been transformed to a positive definite form simply by multiplying all coefficients by minus 1, the values set would be obtained by multiplying by minus 1. So if you wanted to study definite forms, it is enough to study positive definite forms. So we restrict ourselves to positive definite forms that means if you are a is not zero, we will assume that a is positive.

If a is zero, then C will have to be non-zero and we will assume that c is positive, a and c are both zero then there discriminant is b square, which is positive and that is not definite. Positive

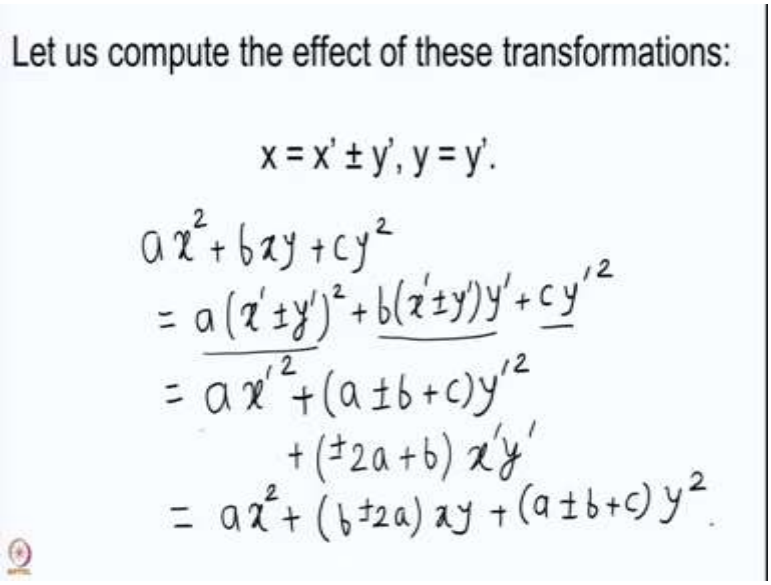
discriminant is an indefinite case which we are not taking so one of the a and c has to be non-zero. And since we are looking at positive definite forms that a or c is a positive number. These are the things that we have with us.

So we are going to obtain the theory of reduction. We are going to start from our given positive definite form and we will apply suitable transformations to obtain a simpler looking form. And this is how we do it. So we introduce these two transformations. They have special names. This is called a transvection. So if you write this in terms of the matrix notation this will correspond to the matrix U is 1, plus minus 1, 0 and 1.

You may obtain writing x in terms of (U x prime) x prime where U is this and you will see quickly that exceeds x prime plus or minus y prime and y remains the same. It is equal to y prime. These matrix elements are called transvections. So we call this a transvection. It can be plus or minus. There are two possibilities. And the second transformation that we want to introduce for want of a better name, I will call it the Weyl element.

So this is written as 0, 1 minus 1, 0 the corresponding U is this matrix, and you will see that this matrix has determinant equal to 1, the earlier matrix that we had for our transvection that also had determinant 1. So these are the two very important (transvection) transformations that we are going to study. Let us see what happens when we apply these two transformations to a positive definite integral quadratic form.

(Refer Slide Time: 14:27)



Let us see what is the effect of these two transformations on our forms, so we will study first the effect of a transvection and if your form was earlier ax squared plus bxy plus cy square this will now become ax prime plus or minus y prime whole square plus bx prime plus or minus y prime into y prime plus cy prime square. So once again, if you count the terms which are coming from x prime square you will get only this thing.

Because there is no x prime square coming from the remaining terms plus y prime squares so that will be a plus or minus b plus c. So these are easily obtained, these also as we have seen in the general, such transformations these are simply given by taking p and r and applying our first quadratic form at p and r, and that would give us the value a because p is 1 and r is 0. And then this is the value obtained for Q and S.

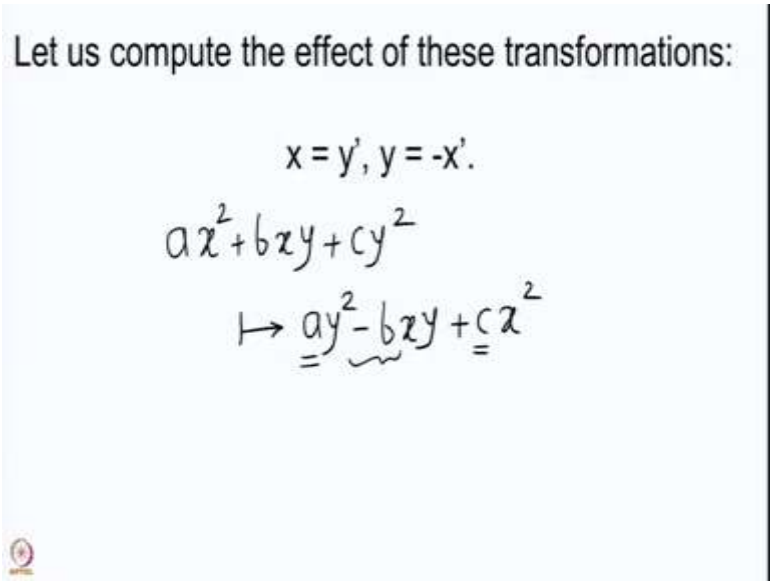
So Q is 1 or minus 1 and therefore you get a plus or minus b plus c and also obtain the coefficient of x prime and y, x prime y prime that would come from here. You would get minus 2a x prime y prime coming from this part, x prime y prime coming from here is plus b and there is no x prime y prime coming from here. So if I write it again in terms of my x and y ignoring the prime, then I get.

So there is a sizable change in the coefficient of y square that had changed from c to c plus a plus minus b. There is a change happening by a plus minus b, there is a change for b, but the change for b is happening only with respect to a. We are looking at b plus or minus 2 a. So the change

happening in b is b plus or minus 2a and a remains as it is, there is no change for a. This is one very nice thing.

If I apply this transvection, I can make the change in b, c will ofcourse change quite a lot, but we will see what to do to c. The coefficient of y square but b can be transformed with respect to a that is something that we can do.

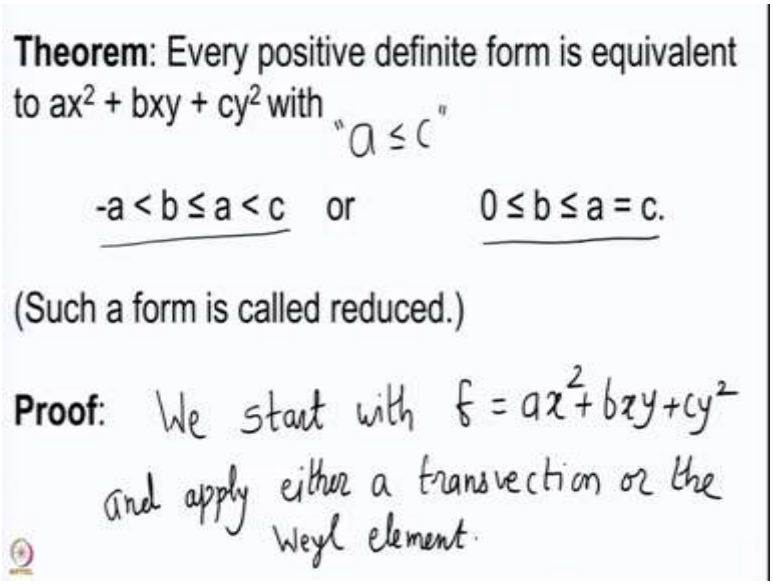
(Refer Slide Time: 17:55)



And now let us look at what happens when we apply the Weyl element to an integral form. This is very simple. So my form was ax square plus bxy plus cy square. This has now changed to I will use this sign and not write the primes. So x is actually now y, so I get ay square y is Y and y is minus x. So I am going to get minus bxy plus cx square. So my new a prime is c. The coefficient of Y square has now become coefficient of X square. The coefficient of x square has now become the coefficient of y square because a has gone towards y prime, y square. And there is a small change for the coefficient of x y. You have just got a sign change.

So you can switch the coefficients of x square and y square by this transformation. This is a very useful transformation. The coefficient of X square and Y square can be changed, but that results in a sign change for B, that is the only thing you should always keep in mind. The earlier transformation, the transvection would allow you to change B with respect to A and this allows you to switch a and c with a sign change at b. Having these two transformations in our kit, let us go and prove one very nice result.

(Refer Slide Time: 19:33)

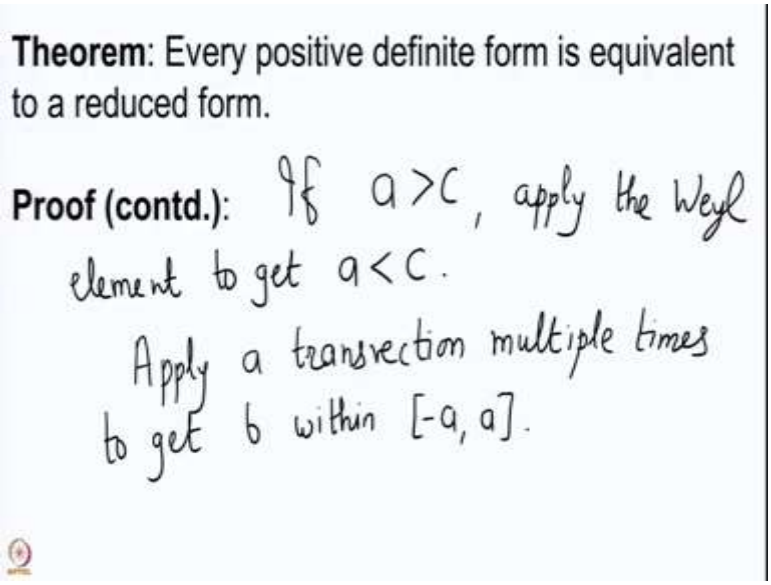


This result says that every positive definite form is equivalent to one satisfying these two very important conditions. So the conditions depend on the behavior of a and c. If you have a equal to c then b will be only between 0 and a, b is always positive and it is between 0 and a. Further if a is less than c then b has a slightly more relaxed behavior.

It can take negative values, but it will not go beyond minus a, it will not even take minus a. So one thing which is hidden in this is that a is always less than or equal to c. So we have a form where a, the coefficient of x square is always less than or equal to the coefficient of y square and moreover depending on whether a is equal to c or a is strictly less than c we have two different behaviors for the integer b.

So the theorem says that every positive definite form is equivalent to one such form and these forms are called reduced forms. These are the simpler forms that we were talking about earlier. So let us go about and prove this statement. So we start with f given by the same coefficients and apply either a transvection or the Weyl element. So this is what we are going to do. Let us start with the possibility that a may not be less than or equal to c.

(Refer Slide Time: 22:11)



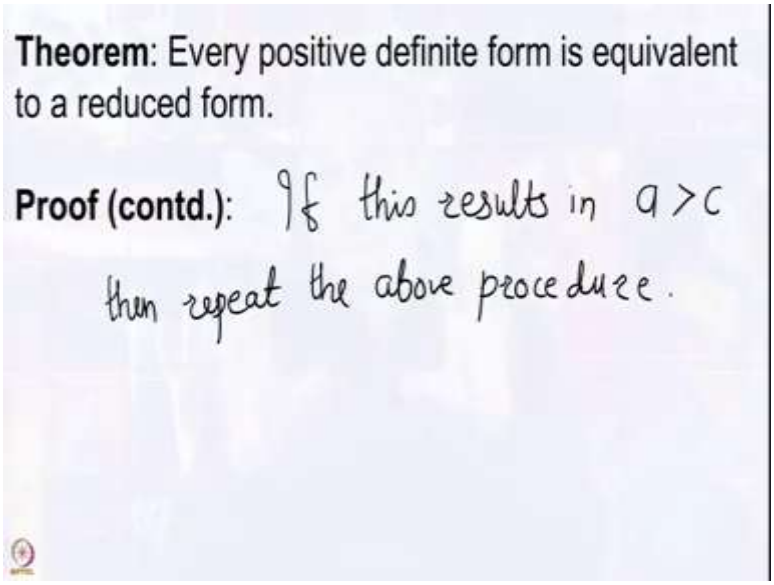
So if a is bigger than c apply the Weyl element to get a less than c. If your a is equal to c you do not have to apply Weyl element, but if a is bigger than c, then apply Weyl element. Remember Weyl element allows you to switch the coefficients of X square and Y square by applying a sign at b also but you can switch these two elements.

So you can just apply Weyl element and have the a and c replaced with each other. So now the new a is less than the new c. So this is one thing that we have obtained very easily. Now we have our a. There will be some b, remember with respect to a, we want to have some condition on b, namely that b should be between minus a and a. But b can be anywhere in the set of integers.

Then we apply the transvection, apply a transvection multiple times to get b within minus a and a. Remember application of the transvection would change b to b plus or minus 2a. So if your b was negative then you can add multiples of 2a to get it towards your minus a, a. If b was very large you can subtract a suitable multiple of 2a to get it between minus a and . Applying a transvection will have no change on a.

You have made c smaller already but it may have a change on c. So you what we did in the beginning was that we made a smaller than c. If a was bigger than c we apply the Weyl element and we made a smaller than c. Then we made changes in the b, so that b was in the correct interval. But that may change c and now c might even become smaller than a. If that happens, we apply the Weyl group element once again.

(Refer Slide Time: 25:05)



If this results in a bigger than c then repeat the above procedure. So let us look at what happens to a and c. We had a and c positive, a was bigger than c, therefore we applied the Weyl element to make a smaller than c. And now we have a to be a smaller number. We made a change in b that resulted in c being smaller than a. But remember that c is again positive, c is not going to be negative.

We have a form which is positive definite and if you put X equal to 0, the value that you are going to get is cy square. If c becomes negative, you will get a negative value. So c has to be positive. So after c becomes smaller than a it will have only finitely many values. But you again switch and make a to be that smaller value. So the value of a has decreased after applying the transvection a few more times, you bring b within this smaller interval now.

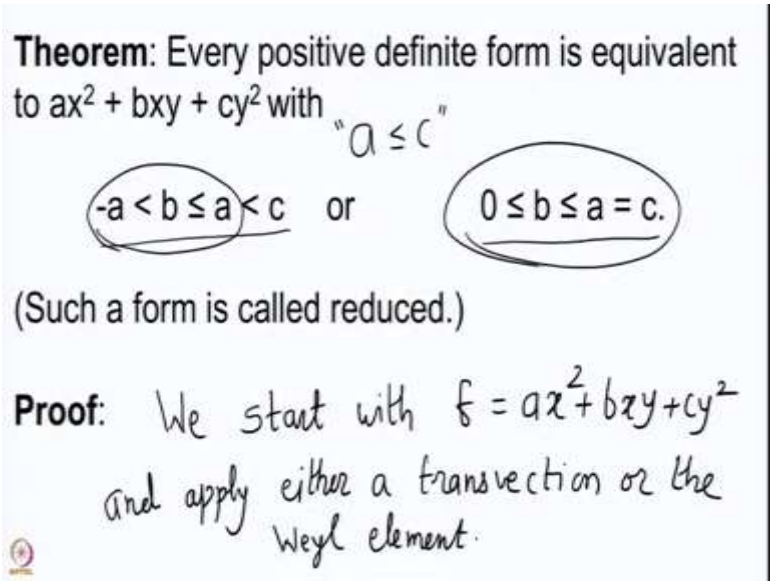
But even after having done this the c becomes even further smaller. You again apply the Weyl element. So by doing this a few number of times you will have to stop because the positive numbers just cannot go indefinitely and become smaller than each other. The process will have to stop at some place. This is what is called the principle of mathematical induction that a non-empty set of integers, positive integers is bounded below.

So the natural numbers is bounded below by 1. So ultimately you will have to hit some number where this process has to stop which means that you have some value for a which remains less than or equal to c. And after applying the transvection your b is now between minus a and a.

Now if you remember we had more specific behavior for b. We did not allow b to take the value minus a.

If your b takes the value minus a, you can apply transvection once again and get it value 2a and when you apply this particular transvection, there is no change in c.

(Refer Slide Time: 27:51)



So for this value whenever, so let us go to the previous term. So we are looking at the reduced forms and reduced forms mean that your b should have this behavior not just should the b be between minus a and a should not take the value minus a.

So that you can easily arrange by the transvection once again if the value of b is minus a, you can apply the transvection once again and get the value to be a without changing c. Further if your a and c are the same and b takes negative value. So we are in this case a and c are the same, but b takes negative value, then apply the Weyl element for one final time.

Weyl element allows you to change the coefficients a and c. Here they are same. So the changing will not make any difference. They will remain the same but remember that the Weyl element changes the sign of b. So if you are b was a negative number by applying the Weyl element you keep the same a and same c, but b has now become positive. So every positive definite integral quadratic form is equivalent to a reduced such form.

And what we have done we will actually see some examples in the next lecture and we would like to classify reduced forms of a given discriminant. We have obtained this reduced form by allow by applying the allowed transformations. So our discriminants have not changed. So these will have the same discriminant. We will actually prove some nice theorem depending on the discriminant and the corresponding reduced form. Stay tuned for more interesting things. Thank you very much.