

**A Basic Course in Number Theory**  
**Professor. Shripad Garge**  
**Department of Mathematics**  
**Indian Institute of Technology, Bombay**  
**Lecture No. 59**  
**Some basic of algebraic number theory**

Welcome back, we are at into the final lec of our course, only a few lectures remain now, what we have done in our last lecture is that we described all the real numbers which are expressed by a continued fraction which is ultimately periodic, we actually proved this very interesting result that these are nothing but quadratic irrationals.

(Refer Slide Time: 00:41)

**Quadratic irrationals:** These are zeros of a polynomial

$$ax^2 + bx + c$$

where  $a, b, c \in \mathbb{Z}$ , the discriminant  $b^2 - 4ac \in \mathbb{N}$  is not a perfect square.

These are of the form  $x + y\sqrt{m}$  where  $m \in \mathbb{N}$  is not a square and  $x, y \in \mathbb{Q}$  with  $y \neq 0$ .



What are quadratic irrationals? Quadratic irrationals are these numbers which are solutions to  $ax^2 + bx + c = 0$  or which are also called the 0's of this degree 2 polynomial. Here we have that  $a, b, c$  are allowed to be any integers, but there is a small condition that  $b^2 - 4ac$  has to be a natural number, this is because we want all these roots, the 0's to be real numbers and further we also demand that this  $b^2 - 4ac$  be not a square, because we are looking at the numbers which are irrational, the numbers which are not rational numbers.

We have also noted that all these numbers can be written in the form  $x + y\sqrt{m}$ , where  $x$  and  $y$  are rationals, but  $y$  is non-zero, because we are looking at the numbers which are not the rational numbers, if  $y$  is 0, then any such number equals  $x$  which will then be a rational number.

So, we are looking at all these type of numbers and we prove that they are nothing but the ultimately periodic continued fractions where ultimately periodic is defined in the slide.

(Refer Slide Time: 02:10)

A continued fraction expansion  $[a_0; a_1, a_2, \dots]$  is called ultimately periodic if  $a_{m+n} = a_n$  for some  $m$  and for all  $n$  after some integer  $N$ .

**Theorem:** A real number  $\theta$  is represented by an ultimately periodic continued fraction expansion if and only if it is a quadratic irrational.

It means that after a stage the partial quotients keep repeating periodically, that means after this capital  $N$  some there is some capital  $N$  such that after this capital  $N$  you have a capital  $N$  plus 1 a capital  $N$  plus 2 dot dot dot a capital  $N$  plus  $m$  and that a capital  $N$  plus  $m$  happens to be the same as a capital  $N$  and so on, so the next ones keep repeating. So, this finite sequence of partial quotients is the sequence that keeps coming there periodically, this is what we mean by saying that it is an ultimately periodic continued fraction.

So, there is this word ultimately that is because the periodicity has started after some stage, if you remember we did the continued fraction expansion for root 2 in the last lecture and we noticed that it was 1 comma 22222, so the first integer  $a_0$ , the first partial quotient that we had obtained was 1, so we leave the  $a_0$ , but from  $a_1$  onwards we had periodicity and that period was 1. So, every integer that we obtain after that the every partial quotient was just equal to  $a_1$  which was 2.

So, we had 1 222222, so there the period the  $m$  is 1 and your capital  $N$  is also 1, The 0th 1 is not part of that periodically repeating set of partial quotients, that is what we had, but it may happen sometimes that your periodicity starts on the nose, if you look at 1 plus root 2, remember root 2 was 1 comma 2 bar the 2 was getting repeated. Therefore, if you add 1 to root 2, now the integral

part of 1 plus root 2 is going to be 2 and then you have 2222, so you have the periodicity right from the word go, you have the periodicity on the nose.

And then these are somewhat special periodic these are somewhat special periodic continued fractions and one may wonder whether you can describe these also in some certain way, are these off some special form and indeed that is true.

(Refer Slide Time: 04:40)

### Purely periodic continued fraction expansion:

**Theorem:** A real  $\theta$  has a purely periodic continued fraction expansion if and only if  $\theta > 1$  and  $-1 < \theta' < 0$  where  $\theta'$  is the conjugate of  $\theta$ .

If  $\theta$  satisfies  $ax^2 + bx + c = 0$  then we have  $(x - \theta)(x - \theta') = ax^2 + bx + c$  for some  $\theta' \in \mathbb{R}$ .  
 $\theta = a + b\sqrt{d}$  then  $\theta' = a - b\sqrt{d}$ .

These are what are called purely periodic continued fraction expansions and there is this very nice result that a real theta has a purely periodic continued fraction expansion if and only if there are 2 conditions, condition 1 says that your number has to be bigger than 1, so the number theta has to be bigger than 1 if the theta has to have a purely periodic continued fraction expansion, it should be bigger than 1 and minus 1 less than theta prime less than 0, where theta prime is the conjugate of theta.

So, let us understand this result first, we are saying that we have this theta whose continued fraction expansion is purely periodic, that means it is starting from the word go from  $a_0$  we have the periodicity. So,  $a_0$  has to be equal to one of the  $a_n$ 's appearing later and therefore,  $a_0$  has to be a positive number,  $a_0$  cannot be negative and  $a_0$  cannot be 0. So,  $a_0$  has to be 1 or more. So, this condition that theta has to be bigger than 1 that is very easy to see.

The second condition is that the conjugate, now what is a conjugate? We have that our theta if it has a purely periodic continued fraction expansion it has an ultimately periodic continued

fraction expansion, it just happens that the periodicity starts from the word go, so this  $\theta$  satisfies the condition in the previous result. And therefore this  $\theta$  has to be a quadratic irrational, at least that much we have beyond quadratic irrationals this theorem does not make sense. So,  $\theta$  has to be a quadratic irrational, therefore the  $\theta$  should satisfy a degree 2 polynomial.

So, if  $\theta$  satisfies say  $ax^2 + bx + c = 0$ , then we have  $x - \theta$  into  $x - \theta'$  equal to this  $ax^2 + bx + c$  for some  $\theta'$ . This is easy to see and I will not do this in this course, so we can actually factorize this degree 2 polynomial, over reals where 1 root is of course  $\theta$ , because  $\theta$  does satisfy this, when you put  $x$  equal to  $\theta$  you are going to get 0. So, 1 root is  $\theta$  and then there is one more root  $\theta'$ , this  $\theta'$  is called the conjugate to the  $\theta$  that we started with.

So, if  $\theta$  has the form  $a + b\sqrt{d}$ , then  $\theta'$  is of the form  $a - b\sqrt{d}$ . So, if you know how your  $\theta$  is written in the form  $a + b\sqrt{d}$ , then computing this  $\theta'$  is not difficult. But the condition now says that your  $\theta$  is bigger than 1 and then this  $\theta'$  has to be negative number, but it cannot be a very large negative number, it should be between 0 and minus 1. And it should not be equal to any of these two, it is a irrational number, so, of course it will not be equal to any of these two, so it should be between minus 1 and 0, this is the condition.

So, the condition is that the quadratic irrational that you start with, if it is bigger than 1 and its conjugate  $\theta'$  is between minus 1 and 0, then the  $\theta$  has a continued fraction expansion which is purely periodic. And similarly, in the converse would say that if you have a purely periodic continued fraction expansion for your  $\theta$ , then  $\theta$  should satisfy these two conditions.

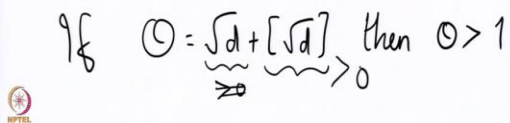
We are not going to prove this theorem in this course, but we will use it, we would like to see that there are some certain real numbers which have purely periodic continued fraction expansions and whenever we want mod to have that we need to only check that these two conditions are satisfied. So, we give some examples of such real numbers.

(Refer Slide Time: 09:34)

### Purely periodic continued fraction expansion:

**Theorem:** A real  $\theta$  has a purely periodic continued fraction expansion if and only if  $\theta > 1$  and  $-1 < \theta' < 0$  where  $\theta'$  is the conjugate of  $\theta$ .

The numbers  $\sqrt{d} + [\sqrt{d}]$  and  $1/(\sqrt{d} - [\sqrt{d}])$  are some examples of such real numbers.


$$\theta = \sqrt{d} + [\sqrt{d}] \text{ then } \theta > 1$$

The numbers  $\sqrt{d} + [\sqrt{d}]$  and  $1/(\sqrt{d} - [\sqrt{d}])$  are some examples of such real numbers. So, in fact if you are  $\theta$  is  $\sqrt{d} + [\sqrt{d}]$ , then of course  $\theta$  has to be bigger than 1, here  $d$  is not a negative number we are looking at real numbers, so we are looking at a plus  $b\sqrt{d}$ , where  $d$  is positive. So,  $d$  is of course real, therefore this is the when we talk about square root  $d$ , note that square root actually may mean positive or negative.

For instance, square root of 4 is the number 2 and also the number minus 2. So, let me just take a minute to explain this symbol for you, whenever we have a symbol, I may have told you initially that the number of  $p$  by  $q$ , that is an expression to write some certain number and that expression means that its particular number which when multiplied by  $q$  gives you the number  $p$ . So,  $p$  by  $q$  is that number where when you multiply by  $q$  you get  $p$ . So,  $1$  by  $2$  is one particular point one particular dot on the real line which lies exactly halfway from 0 to 1 and we call that  $1$  by  $2$  we are giving the name  $1$  by  $2$  to this number, because this number has the property that when you multiply that number by 2, you are going to get the answer to be 1.

Now, ideally whenever we want to write a number in this way, there should be a unique number, it should not happen that there are if you use some certain way to write denote a number, but some another number is also possibly expressed in the same way, we would like to try and avoid

such situations, because if there are such multiple possible numbers which can be written in the same way, then it leads to confusion.

So, if you talk about root of  $d$ , then ideally it is the number whose square equals  $d$ , that is what we mean by a root  $d$ , but there are two such numbers, whenever your  $d$  is not 0 and let us say we are taking positive because we do not want to go into the realm of complex numbers, whenever you take  $d$  to be positive, let us say if your  $d$  is 4, then square root of 4 can be 2 and it can also be minus 2. Because both plus and minus 2 have the property that their squares will give you 4.

So, when you mean when you write square root of 4, you should actually tell what you mean by this and I am sorry for not having explained this earlier, but luckily I realized it now and so I would like to emphasize here that whenever we put a root we always mean the positive number. Note again, that  $d$  is positive, so we are within the real numbers and therefore it is clear what is a positive root and what is a negative root, we do not talk about positivity and negativity when we have the  $d$  to be imaginary, because that would lead to further complications let us not go into that.

So, now our root  $d$  is positive, by convention this is bigger than 0 and of course we have the integral part of root  $d$ , since root is bigger than 0 and if your  $d$  happens to be non-square that would mean that anyway  $d$  is an integer and so root  $d$  will be 1 or bigger. Therefore, the integral part is also 1 or bigger, so both these quantities would certainly add up and give you that you have something which is bigger than 0, in fact you have something which is bigger than 1.

(Refer Slide Time: 13:43)

### Purely periodic continued fraction expansion:

**Theorem:** A real  $\theta$  has a purely periodic continued fraction expansion if and only if  $\theta > 1$  and  $-1 < \theta' < 0$  where  $\theta'$  is the conjugate of  $\theta$ .

The numbers  $\sqrt{d} + [\sqrt{d}]$  and  $1/(\sqrt{d} - [\sqrt{d}])$  are some examples of such real numbers.

$$\text{If } \theta = \sqrt{d} + [\sqrt{d}] \text{ then } \theta > 1. \quad \theta' = [\sqrt{d}] - \sqrt{d} \\ -1 < \theta' < 0.$$

So, this number theta which is root d plus integral part of root d that is bigger than 1. So, we are done with this. Now, we consider theta prime. So, I told you that if your theta is of the form a plus b root d, then the prime the conjugate is a minus b root d. So, here the conjugate would be integral part of root d which is simply an integer minus root d. Now, integral part of any number is less than or equal to that number and if you add 1 to the integral part then you would have gone beyond the number.

So, when you remove the integral part from any number what you get is the fractional part and we have noticed that the fractional part can be 0 or it can be something which is less than 1. Here we are taking the negative of the fractional part, because we are taking the integral part and remove the number from that, root d is our number and we are looking at integral part of root d minus root d. So, here we get some number which is negative of the fractional part, so it is going to be between minus 1 and 0 and being an irrational number it is not going to be equal to any of these two.

So, we have that your theta prime is negative and it lands between minus 1 to 0. So, the number theta equal to d root d plus integral part of root d satisfies both these definitions. So, it has to be a purely periodic continued fraction expansion, we will remember this and we are going to use this that root d plus integral part of root d is always a purely periodic continued fraction expansion.

So, we are done with these quadratic irrationals and expressing them as continued fractions for the time being, now what we are going to do is to consider a little bit of very basic algebraic number theory, this is something that we are going to use in solving the Brahmagupta equations.

(Refer Slide Time: 16:01)

Consider a square-free  $d \in \mathbb{Z}$  and consider the set

$$\mathbb{Q}[\sqrt{d}] := \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}.$$

$$x + y\sqrt{8} = x + 2y\sqrt{2}, \quad a + b\sqrt{2} = a + \frac{b}{2}\sqrt{8}$$

$$\mathbb{Q}[\sqrt{8}] \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{8}].$$

So, what we do here is the following, we take a square free  $d$ , square free means that there is no square which divides  $d$ , earlier we were looking at non square  $d$ , so for instance 8 is a non-square  $d$ , because 8 is not square of any natural number, but 8 is not square free because 4 divides 8. So, when we are writing the corresponding this is called  $\mathbb{Q}$  root  $d$ , when we are writing this  $\mathbb{Q}$  root  $d$ , we will consider only this square free  $d$ , the reason being that, if I have  $x$  plus  $y$  root 8, then this can also be written as  $x$  plus 2  $y$  root 2.

So, the number of elements which are in  $\mathbb{Q}$  root 8, the elements which are in  $\mathbb{Q}$  root 8 are contained in the elements which are in  $\mathbb{Q}$  root 2. And of course we are allowing rational coefficients  $x$  and  $y$  are rational, so if you have  $a$  plus  $b$  root 2, this is  $a$  plus  $b$  by 2 root 8, so we have that this is also contained in  $\mathbb{Q}$  root 8. So, these are the same sets, we have defined a set  $\mathbb{Q}$  root  $d$  by this way, so this is our definition, it is of the form  $x$  plus  $y$  or  $d$  where  $x$  and  $y$  are rational numbers, then it is enough to take the corresponding  $d$  to be a square free  $d$ . So, we will stick with this particular convention that our  $d$  is always a square free  $d$ .



(Refer Slide Time: 17:54)

Consider a square-free  $d \in \mathbb{Z}$  and consider the set

$$\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}.$$

$$(x_1 + y_1\sqrt{d}) + (x_2 + y_2\sqrt{d}) = (x_1 + x_2) + (y_1 + y_2)\sqrt{d}.$$

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = \underbrace{(x_1x_2 + y_1y_2d)}_{\in \mathbb{Q}} + \underbrace{(x_1y_2 + x_2y_1)}_{\in \mathbb{Q}}\sqrt{d}.$$

What can we do with this set, if I take any  $x_1$  plus  $y_1$  root  $d$  and add it to another search  $x_2$  plus  $y_2$  root  $d$ , we will get  $x_1$  plus  $x_2$  plus  $y_1$  plus  $y_2$  root  $d$ . So, this set  $\mathbb{Q} \text{ rot } d$  is actually closed with respect to addition, if you take addition of any two such numbers in the set, then the sum is again in the set. So,  $\mathbb{Q} \text{ root } d$  is closed under addition, there is the 0 which can be written as 0 plus 0 root  $d$ . Therefore, this  $\mathbb{Q} \text{ root } d$  has the additive identity and it also has the additive inverse  $x$  plus  $y$  root  $d$  plus minus  $x$  plus minus  $y$  root  $d$  is going to give you 0 plus 0 root  $d$ .

So,  $\mathbb{Q} \text{ root } d$  is a group with respect to addition, you also have the multiplication defined on it, we can write  $x_1$  plus  $y_1$  root  $d$  into  $x_2$  plus  $y_2$  root  $d$  as we have  $x_1 x_2$  plus  $y_1 y_2 d$  plus now the coefficient for root  $d$  that is  $x_1 y_2$  plus  $x_2 y_1$  root  $d$ . Because  $x_i$  are rationals,  $y_i$  are rationals, we see that these two numbers are rationals. So, the set is closed under multiplication also, you have rational coefficients and you are taking the sum and product and you again have rational coefficients. There is the element 1 which is 1 plus 0 root  $d$ . So, you have that there is multiplicative identity, we of course have the associativity for both addition and multiplication.

So, to check whether we have group structure the question that we should ask is whether we can divide by every such  $x$  plus  $y$  root  $d$  and remain in  $x$  plus  $y$  root  $d$ , this is something which is very important, in the very first few lectures we have talked about divisibility in natural numbers and the important thing for us was that whenever you divide a natural by another natural, we do not want to go outside the natural numbers, we want it to be in the same set, so here also we are

asking whether we have one particular element of  $\mathbb{Q}[\sqrt{d}]$  another such element and let us assume that the element that we are dividing by is non-zero.

Because we know that we are not going to divide by 0 in and then if you divide by 0 you will not remain in this set, you will get something called infinity, let us not go into that, let us remain in our finite world, so we are dividing by a non-zero number and the question is, can you divide by a non-zero number. And that is true, you can actually divide by a non-zero number and you can you will remain in the set  $\mathbb{Q}[\sqrt{d}]$ , this is something that we have already seen when we have computed the continued fraction expansion for  $\sqrt{2}$ ,  $\sqrt{3}$  and so on.

There were instances when we had  $1/\sqrt{3} - 1$ , for instance and we need to multiply both sides by  $\sqrt{3} + 1$  and we obtain some rational combination of 1 and  $\sqrt{3}$ . So, this is indeed true that you can divide by a non-zero element in  $\mathbb{Q}[\sqrt{d}]$ .

(Refer Slide Time: 21:54)

Consider a square-free  $d \in \mathbb{Z}$  and consider the set

$$\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}.$$

This set is equipped with addition and multiplication.



So, the set is first of all equipped with addition and multiplication and with respect to addition it is a group, with respect to multiplication all the non-zero numbers for a group, there is another way to see this.

(Refer Slide Time: 22:05)

We have the norm map defined on  $\mathbb{Q}[\sqrt{d}]$ ,

$$\begin{aligned} N(x + y\sqrt{d}) &= \underbrace{x^2 - dy^2} \in \mathbb{Q}. \\ &\parallel \\ &\underbrace{(x + y\sqrt{d})(x - y\sqrt{d})} \\ \text{If } xy \neq 0 \text{ then } N(x + y\sqrt{d}) &\neq 0. \\ \text{then } \frac{1}{x + y\sqrt{d}} &= \frac{x - y\sqrt{d}}{\underbrace{N(x + y\sqrt{d})}} \in \mathbb{Q}[\sqrt{d}]. \end{aligned}$$

We have this norm map defined on  $\mathbb{Q} \sqrt{d}$ , what does the norm map do? Note, that this is nothing but  $x$  plus  $y$  root  $d$  into  $x$  minus  $y$  root  $d$ . If you take the product  $x$  plus  $y$  root  $d$  into  $x$  minus  $y$  root  $d$ , we get  $x$  square minus  $dy$  square which is what we have and the coefficient of root  $d$  happens to be  $x$  into minus  $y$  plus  $y$  into  $x$ , so it is  $xy$  minus  $xy$  and that becomes 0. So, we have that this norm is always a rational number,  $x$  square minus  $dy$  square and if you have  $x$  and  $y$  non-zero,  $xy$  is not 0, if you have that the product is non-zero, then norm of  $x$  plus  $y$  root  $d$  is also not-zero.

This is because if you have any rationals giving us 0 solution for  $x$  square minus  $dy$  square, that would mean that  $d$  is of the form  $x$  square by square and we have taken  $d$  to be an integer which is not a square. In fact, we have taken  $d$  to be square free, it is not a square and it is not even divisible by any square other than 1 of course. So, this  $d$  cannot be square off some integer it also cannot be square of any rational number I told you in some of the last lectures that this is going to use the fundamental theorem of arithmetic that if you have a non-square, then its square root is not a rational number.

So, you are not going to get solutions to  $x$  square minus  $dy$  square equal to 0, where one of the  $x$  and  $y$  is non-zero. Of course, if you have  $y$  to be 0, you get  $x$  square equal to 0 and so  $x$  is 0, if  $x$  is 0 you get  $dy$  by square equal to 0 and then  $y$  is 0, so if any one of them is 0 other is also 0 and you have no solutions when none of them is 0, that would mean that the norm  $x$  plus  $y$  root  $d$  is 0

would imply that  $x$  is 0 and  $y$  is 0. And in fact turning it in the other way, if you have that if any of them is non-zero, your norm cannot be 0.

So, if you are  $x$  plus  $y$  root  $d$  is a number where the product is not 0, then  $1$  upon  $x$  plus  $y$  root  $d$  is nothing but  $x$  minus  $y$  root  $d$  upon norm  $x$  plus  $y$  root  $d$ , we have noticed that this is a rational number of course  $x$  square minus  $dy$  square and it is not 0 so you can divide by rational number, you can always divide by rational number and be in the set of rational numbers. So, you will divide by this rational  $2x$  you will get a rational you will divide by that  $2y$  and you get a rational, so ultimately this number is again in  $\mathbb{Q}$  root  $d$ .

So, this tells you that you can always divide by a non-zero element of  $\mathbb{Q}$  root  $d$  and remain in the set  $\mathbb{Q}$  root  $d$ . This is all encoded in this sentence that the set  $\mathbb{Q}$  root  $d$  is actually a field.

(Refer Slide Time: 25:53)

We have the norm map defined on  $\mathbb{Q}[\sqrt{d}]$ ,

$$N(x + y\sqrt{d}) = x^2 - dy^2.$$

The set  $\mathbb{Q}[\sqrt{d}]$  is actually a field.

$$m + n\sqrt{d} \in \mathbb{Q}[\sqrt{d}] \text{ is a root of } \text{satisfies a poly.}$$

$$= ax^2 + bx + c, \quad a, b, c \in \mathbb{Z}.$$



Just like we have seen the notion of a group, there is also the notion of a ring and here we have that there is a notion of a field, whatever it means it just says that the  $d$  you can divide by non-zero numbers and of course you can add and subtract and multiply by any number and you will remain in the set  $\mathbb{Q}$  root  $d$ .

Now, we noticed that any number which is here in  $\mathbb{Q}$  root  $d$ , suppose it is of the form  $m$  plus  $n$  root  $d$  which is here in  $\mathbb{Q}$  root  $d$  this satisfies a polynomial  $ax$  square plus  $bx$  plus  $c$  is satisfies means it is a 0 of or root of this polynomial  $ax$  square plus  $bx$  plus  $c$ , where  $a, b, c$  are integers. This a need not always be equal to 1, because you know for instance we have the element  $1$  by  $2$

which is there in the rational numbers, so it is there in  $\mathbb{Q}[\sqrt{d}]$  also and the polynomial satisfied by 1 by 2 over integers. If you want  $a, b, c$  in integers, then the only polynomial satisfied by 1 by 2 is  $2x$  minus 1, you cannot have a polynomial of the form  $x$  minus  $\alpha$  satisfied by 1 by 2 where  $\alpha$  is also an integer.

Similarly, if you have any higher degree polynomial satisfied by 1 by 2 over integers, then the leading coefficient the coefficient of the highest possible degree that cannot be 1, this is something which use a slightly advanced mathematics, but that was only for an example. So, what we have is that if you have a number in  $\mathbb{Q}[\sqrt{d}]$ , this number  $a$  need not always be 1. But we would like to take numbers where this  $a$  is also equal to 1, we call such numbers to be algebraic integers.

(Refer Slide Time: 28:23)

**Algebraic integers in  $\mathbb{Q}[\sqrt{d}]$ :** These are the elements

$m+n\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$  that satisfy

$$x^2 + bx + c = 0, \quad b, c \in \mathbb{Z}.$$

So, these are the elements  $m$  plus and root  $d$  in  $\mathbb{Q}[\sqrt{d}]$  that satisfy  $x$  square plus  $bx$  plus  $c$  equal to 0 with  $b$  and  $c$  being integers. So, for instance if you are looking at rational numbers which satisfy such polynomials, it will turn out that those are nothing but integers. So, these algebraic integers we are calling them integers, algebraic integers for the reason that when you consider the field of rational numbers the algebraic integers in rational numbers are the ordinary integers, that explains the nomenclature.

What happens later is that all these elements form a ring, you can add such elements you can subtract 0 is there associativity of course holds in the whole complex number, so we will not

keep mentioning it again and again, so the set of algebraic integers is a group under addition, you can multiply by two algebraic integers and get an algebraic integer, of course the element 1 is there, but we have problem when we come to division.

Of course, 1 and 2 these are algebraic integers, because these are ordinary integers, but you cannot divide 1 by 2 and get an algebraic integer, 1 by 2 is not an integer, any algebraic integer which is a rational number has to be an integer, so you cannot divide by them, but you can definitely multiply by them and therefore, it is an interesting question to determine all the elements by which you can divide within the set of algebraic integers.

These elements are called units and we will see a very nice way using continued fractions to describe the set of all units in a given  $\mathbb{Q}(\sqrt{d})$  and it will also lead us to what is known as the Brahmagupta equation. So, this is something that we are going to conclude our course with, I hope to see that you will stick until then, thank you very much.