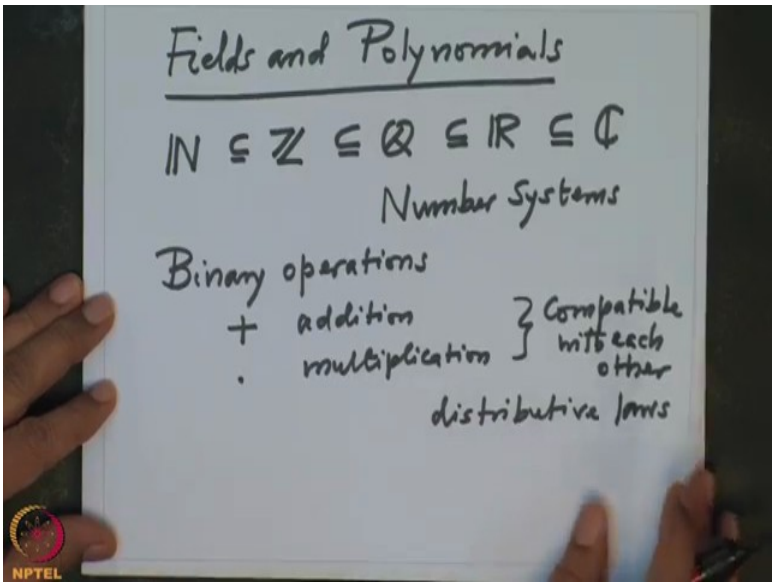
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 02 – Examples of Fields

I come back to this continuation of the last lecture. Now I will be more formal writing definitions more precisely et cetera. So first one or two lectures I will spend on the preliminaries, on fields and polynomials.

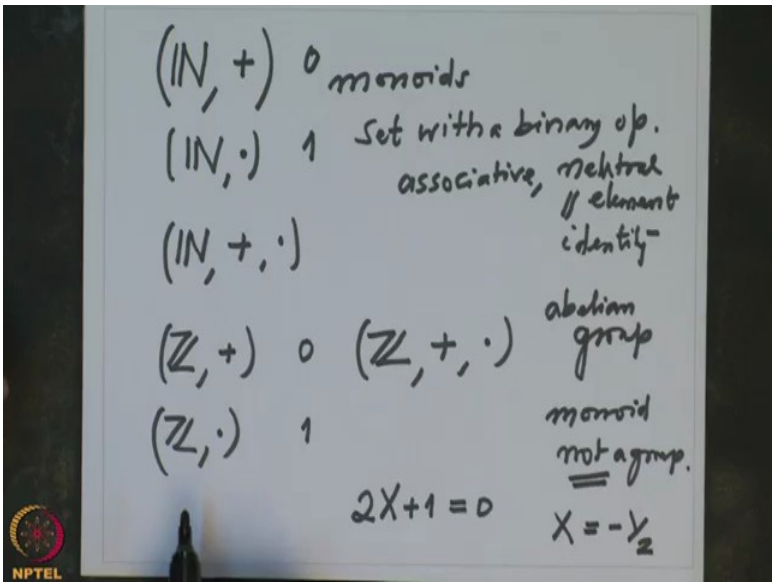
(Refer Slide Time: 0:51)



So first about the field, so first as we just mentioned for the completeness our notation is $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. I will assume that the participants are familiar with these number systems. This I will keep referring them as number systems. Each one of them has two binary operations, one is addition and the other is multiplication. And both these operations are compatible with each other.

That means they satisfy the so called distributive laws. I will not go into the details because all the participants in this course have studied such systems. And in fact, originally they were defined for natural numbers and then they were extended to integers and then they were extended to rational numbers and they were extended to real numbers and they were extended to complex numbers. So this was what the mathematics progress up to 19^{th} century. And let me note the properties here and how it has improved over time.

(Refer Slide Time: 3:35)

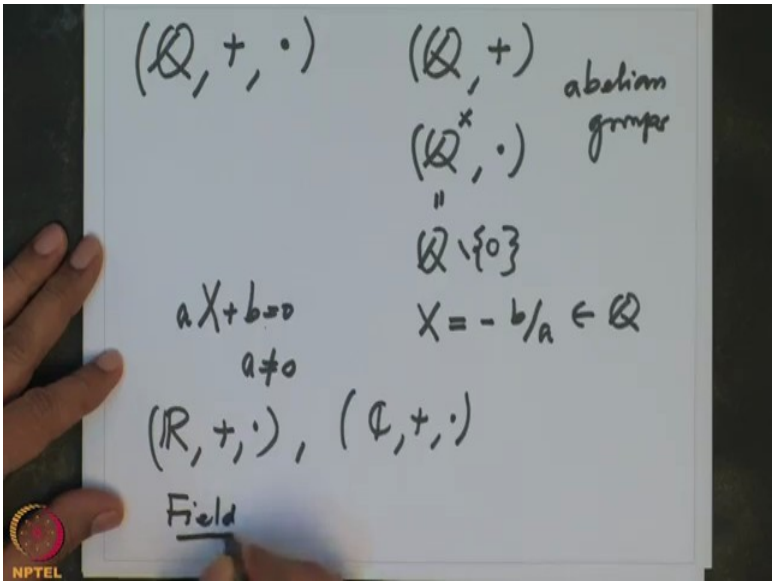


So for example, ($\mathbb{N}$,+) and ($\mathbb{N}$,.) are monoids. Monoid mean a binary set with a binary operation which is associative and has a neutral element. Similarly N, dot is also monoid. The neutral element for ($\mathbb{N}$,+) is 0, and neutral element for ($\mathbb{N}$,.) is 1. And together ($\mathbb{N}$,+,.) is a number system. This is natural numbers and these two operations are compatible with each other.

So the identity of the monoid ($\mathbb{Z}$,+) is 0, the identity of the monoid ($\mathbb{Z}$,+) is 1. Identity or neutral element, I will keep interchanging the words. So here it is better now. This ($\mathbb{Z}$,+) is not only a monoid but it is a group, it is an Abelian group. Abelian means it is commutative, these operations are also commutative. All the operations in our number system are commutative.

($\mathbb{Z}$,.) is not a group but it is just a monoid. Monoid, not a group. So because it is not a group, we have a problem in solving such equations. 2X+1=0 is a linear equation, coefficients are in $\mathbb{Z}$ but the solution is not integral solution, solution is minus- half. So we cannot divide it by 2. 2 does not inverse in, with respect to multiplication. That is why this equation does not have a solution in $\mathbb{Z}$. So not only we need to be precise to say where the coefficients are, but also we need to be precise to ask questions where are we looking for solutions. If you are looking for solutions in $\mathbb{Z}$, this equation does not have solution in Z. So with this kind of problem rational number is better.

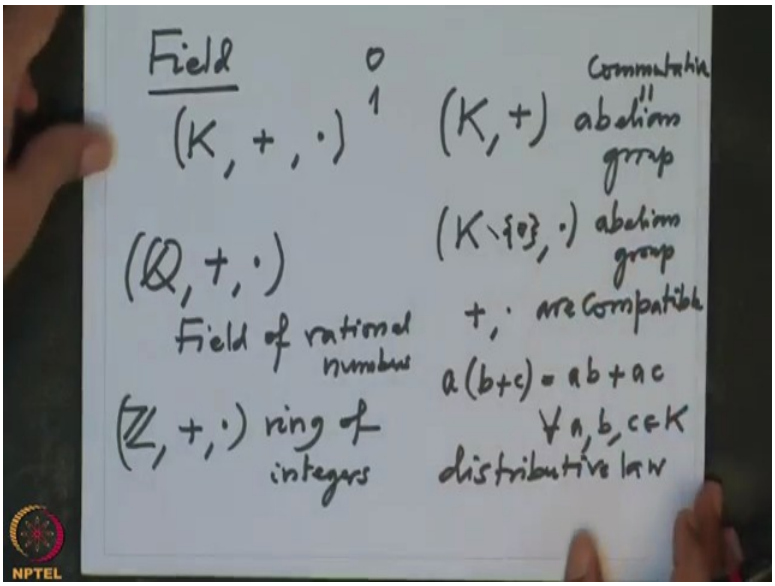
(Refer Slide Time: 6:35)



So ($\mathbb{Q}$,+) and ($\mathbb{Q}^x = \mathbb{Q}\setminus\{0\}$,.) are Abelian groups. So when the linear equation, now if I take any linear equation like this, aX+b=0, the solution makes sense. The equation is linear; therefore a cannot be 0. Then the solution is $\frac{-b}{a} \in \mathbb{Q}$.

And even if a and b are rational, b by a is also rational. So therefore, a linear equation or $\mathbb{Q}$ has a solution. Similar work for real numbers and complex numbers. So such a thing is called a field. So what is the formal definition?

(Refer Slide Time: 8:10)



Field: Field is a set, K, it has two binary operations, plus and multiplication. With respect to plus, it is Abelian group. Abelian means commutative. Abelian is same as commutative. Abel was the first to consider such an operation, so it is usually called Abelian. It is named after Abelian. And remove 0, the additive identity for K, so 0 and 1 are usually denoted by, depending on the context they are not, of course this 0 and 1 is also notation for the natural numbers.

But in this context now 0 is the neutral element or identity element with respect to the binary operation plus. And 1 is neutral element with respect to the operation multiplication. Also the word used multiplication, is used because of the standard examples. So $K\setminus\{0\}$ with dot, this is also an Abelian group. And of course, the operations are compatible. Compatible just means they are connected by the distributive law. That is, let me write at least once, a.(b+c) = ab + ac for all a, b, c in the field K. And obviously the other side also.

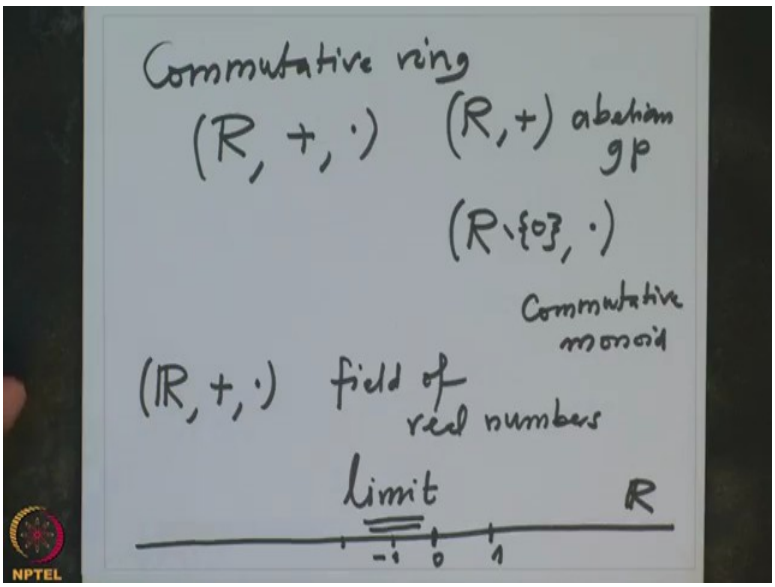
But I will not write other side because now our operations are commutative, so we do not need to. But if you are studying non-commutative ring theory or some such subject, then we need to mention that. So this is called a distributive law.

So this is very important because if this was not there, then different people will get different answers and the world will not be compatible with each other. So these are very important part of the definitions. So such a thing is called a field. Then the examples of fields are $\mathbb{Q}$ with a

natural addition and natural multiplication. This is a field, therefore this is called a field of rational numbers.

With the similar thing, one would call this $\mathbb{Z}$ plus, dot; this is ring of integers. It is not a field but it is a ring. And now what should be ring? Ring, only condition you drop is with respect to the multiplication, tt may not be a group but it is certainly a monoid. Such a thing is called a ring, commutative ring. One does not say Abelian group or Abelian field. One calls it a commutative ring. So in general, we have a concept of commutative ring.

(Refer Slide Time: 12:22)

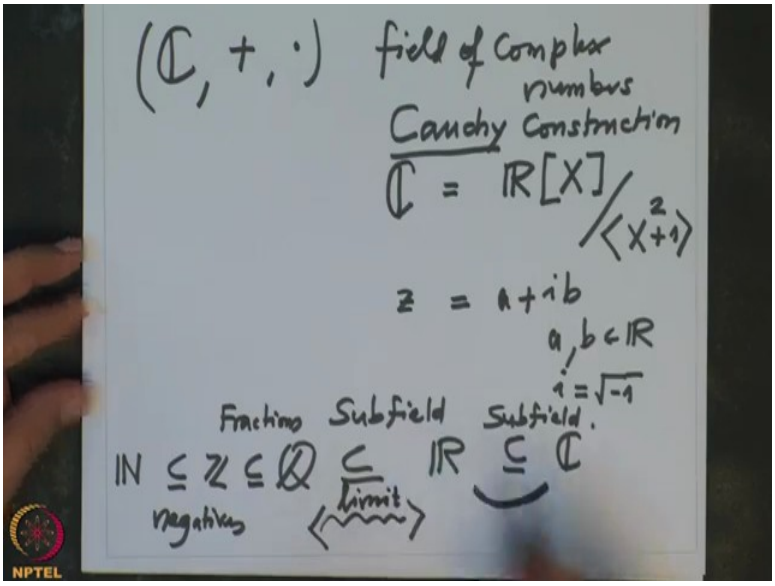


That is a ring, the set R which has two binary operations. And R, plus is Abelian group. And if you remove identity for plus, that is denoted by 0, with respect to multiplication, it is a commutative monoid. That means it has neutral element with respect to this. A typical example of a commutative ring is the ring of integers. Some more examples of field: real numbers with usual addition and multiplication, that is a field of real numbers.

I will not dare to define this in this course. I will assume that all of you know how do you construct field of real numbers from the field of rational numbers. I will only say that you need concept of limit. So what was roughly was? If you try to see rational numbers, it had gaps. And if one want to fill up the gaps and try to draw picture of real line like a horizontal line, then we get the field of real numbers.

So usually the convention, standard convention which inherited to us from physics was when you go on the left side, it is negative and when you go on to the right side, it is positive. And this is also related to our Indian philosophy, methodology that when you go on the right side, it is more positive. So that is field of real numbers.

(Refer Slide Time: 14:45)



And one more example is (ℂ ,+,.). This is a field of complex numbers. So again if one looks at the historical perspective, till Steinitz people were not very clear about complex numbers. But after Steinitz's paper came many things became more and more clear. And for example, I will just mention here that, just mention but we will prove it sometime later. This complex number, one of the construction that Cauchy gave of complex numbers was $\mathbb{C} = \mathbb{R}[X] / \langle X^2+1 \rangle$

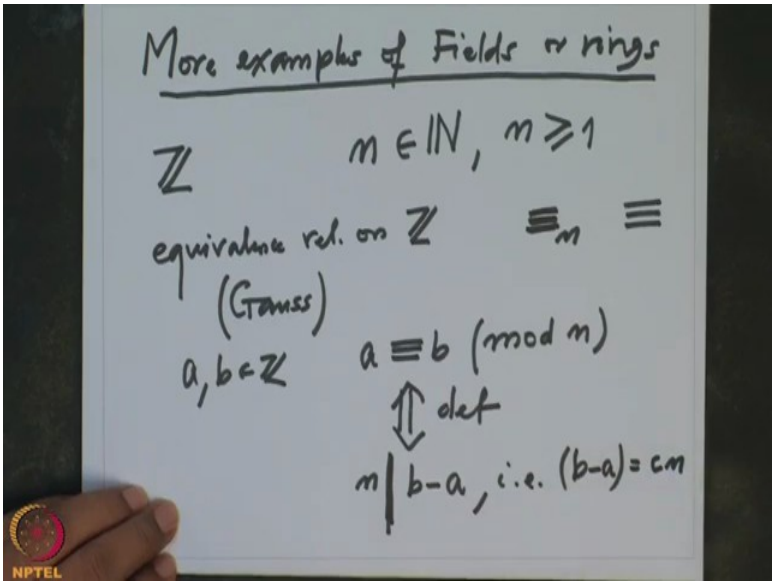
This is still not very clear but I will make it soon clear. This quotient ring is a field and that field is called complex numbers. And that field is called complex numbers and there you see then every complex number z can be uniquely written as a+ib, where a, b are real numbers and i is a complex, imaginary complex number which is square root of -1. So writing this is not very good. It is still sloppy. So I want to improve all this.

So first of all one has to explain what is the polynomial ring and how do I write this and so on. But this soon I will do. This is Cauchy's construction of complex numbers. So you see in this hierarchy, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, these are fields. And one also say that this $\mathbb{Q}$ is a field of real

numbers, subfield. Means the binary operations are same and $\mathbb{Q}$ is in its own right a field. Similarly, $\mathbb{R}$ is a subfield of complex numbers.

In this hierarchy up to $\mathbb{Q}$, definition of $\mathbb{Q}$ from natural numbers is not too bad. It is algebraic definition only because from $\mathbb{N}$ to $\mathbb{Z}$, you provide negative numbers and from $\mathbb{Z}$ to $\mathbb{Q}$ you provide fractions. So there you provide negatives. And here you provide fractions. And $\mathbb{R}$ to $\mathbb{C}$ is also not so bad. This is also easy. If you want, this is a vector space of dimension 2. 1 and i is a basis, that is one explanation. Or this explanation is also algebraic. But from $\mathbb{Q}$ to $\mathbb{R}$ there is a big gap which cannot be explained without limit. So definition of real numbers is more complicated than one thinks. But on the other hand, it is a very practical definition.

(Refer Slide Time: 19:02)



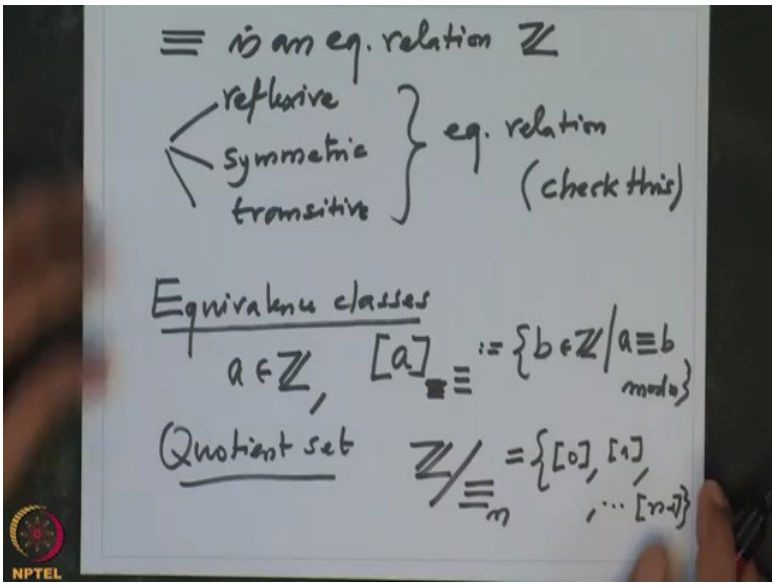
Now more examples of field, and also I want to make this clear. So before I go on, so how can one construct more fields? There are two ways. Or how do you construct more rings? So, you can ask more examples of fields or rings. And usually nowadays there are, at every stage there are courses like rings, group rings and fields. So more and more examples. And it is more appropriate to construct examples from the given examples.

And now the only example we have are these: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. So from these I will construct more examples of ring as well as fields. So the only examples of a ring so far are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. But the first thing is ring of integer, $\mathbb{Z}$, from this I am going to construct many rings. So

given any integer n, any natural number in fact, n bigger equal to 1, I am going to define an equivalence relation on the set $\mathbb{Z}$, equivalence relation on $\mathbb{Z}$ which will be denoted by $a \equiv_n b$.

But I will drop this n and fix our n, so I will just write this. And this symbol is very important, this was introduced by Gauss, and that created revolution at that time in the simplification of notation. So what is it? So we will say that a, and b are integers and $a \equiv b \pmod{n}$ (read a congruent to b mod n) if n divides b-a. Or in other words, b-a is a multiple of n.

(Refer Slide Time: 21:54)

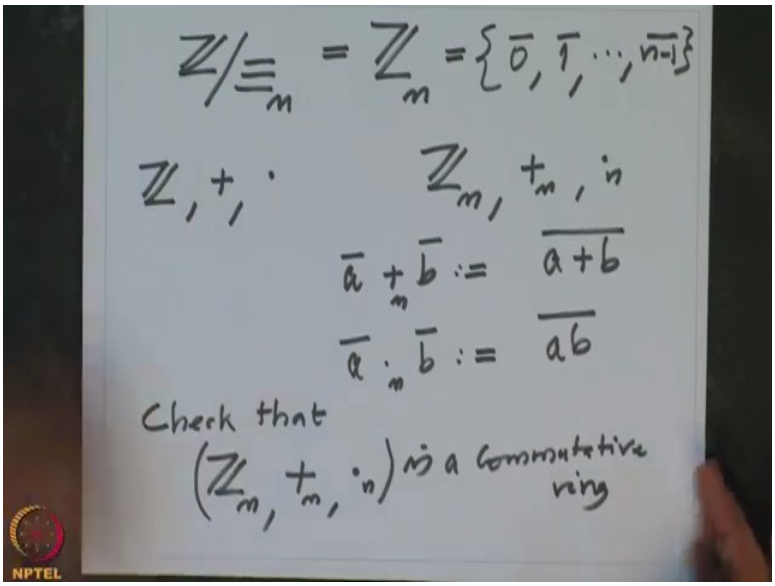


So we have a relation on the integers and I want to check that this is an equivalence relation $\mathbb{Z}$. So what should we check? We should check that it is reflexive, symmetric and transitive. These three things together, it is called an equivalence relation. And I will leave it for you to check that this is an equivalence relation. So I will just mention here, 'check this'. Once you have an equivalence relation, we can talk about the equivalence classes and quotient set.

So equivalence classes, they are, that means given any a in integers, we are collecting all the elements which are equivalent to a, under this. So this is by definition, all those integers b in $\mathbb{Z}$ such that a is congruent to b mod n. And we know then these are the equivalence classes. And we know that the equivalence classes, they are disjoint or they are equivalent. And then the quotient set, that is usually denoted by Z modulo =.

And this has obviously how many elements? This has precisely n elements. Namely, they are equivalence classes of 0, 1, ..., up to n-1. These are precisely the integers. When I divide by n, I get 0. These are precisely the integers. When I divide by n, remainder is 1 and so on.

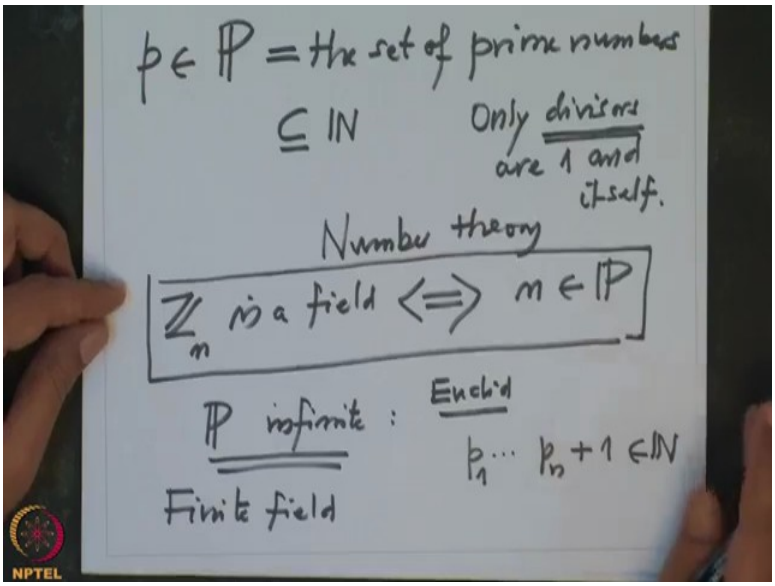
(Refer Slide Time: 24:26)



So on the quotient, so these are also denoted by, so we will usually denote these equivalence $\mathbb{Z}_n$. And the elements of this instead of writing the brackets, [0], [1],... we will write $\bar{0}, \bar{1}, \ldots, \overline{n-1}$, . And now I want to say that the binary operations on Z, namely the natural addition and multiplication, they will induce a binary operations on this new set.

And how are they defined? We define $\bar{a}+\bar{b}=\overline{a+b}, \bar{a}.\bar{b}=\overline{a.b}$ I will only write here, check that $\mathbb{Z}_n$ with these operations is commutative. So we have many rings now. As many as natural numbers, we have many commutative rings. So I will not check this.

(Refer Slide Time: 26:18)



Moreover, I will also mention here, this is an important observation. If I take a prime number p, p is prime number. This P is called the set of prime numbers. So P is considered as subset of $\mathbb{N}$. And what is the prime number? Those natural numbers whose only divisors are 1 and itself, these are called prime numbers. Again when I say only divisors, that means I am only taking divisors in natural number. These are called prime numbers.

And it is now very important topic: study prime numbers, how they are, how many they are? How often, what is their distribution and so on? This is a very big subject. Very, very important subject nowadays. It is called number theory. Number theory study the prime numbers, study of prime numbers. So anyway, so $\mathbb{Z}_n$, this is a field if and only if n is a prime number. This is very very important observation and I want you to check this.

So that way we get lots of examples of fields. We have, we know that the set of prime numbers is infinite. This is a famous proof by Euclid that if they are only finitely primes, p_1 to p_n then look at their product and add 1. And we know that this is again a natural number. And we know that, next time I will recall this precisely what I want to recall, that this is again a natural number. So it has a prime factor and that prime factor cannot be one of the p_1 to p_n Therefore you get a new prime factor, that is why, that is a contradiction.

So this was Euclid's proof that P is an infinite set. So we have now infinite examples of fields. The only difference between the earlier fields and these fields, all these fields are finite fields. Finite means the underlying sets are finite sets. In the other examples, $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, they

were all infinite sets. So next time I want to still give more examples of rings and then we will start studying polynomials over field. And then we will set up our dictionary correctly. What does one mean by solutions? What does one mean by polynomials and so on? Thank you.