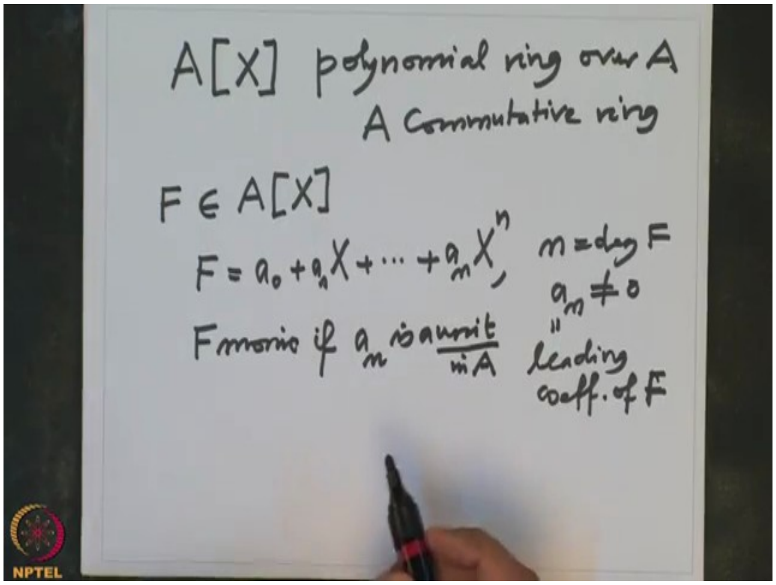
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 05 – Unit and unit groups

(Refer Slide Time: 0:46)



A[X] polynomial ring over A

A Commutative ring

$F \in A[X]$

$F = a_0 + a_1 X + \cdots + a_n X^n$, $n = \deg F$

$a_n \neq 0$

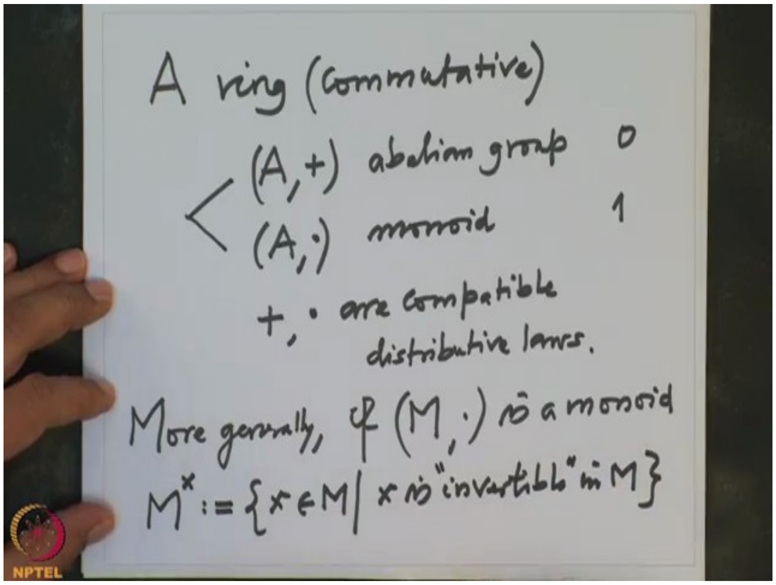
'' leading coeff. of F

F monic if a_n is a unit in A

In the last lecture we began our study with the polynomials, more precisely polynomials over a commutative ring. And the notation we have used is the set of polynomials with coefficients in the ring A is denoted by A[X]. This is, and we saw again that it is a ring and this ring is called a polynomial ring over A. And A was commutative ring. And we saw how to add two polynomials, how to multiply two polynomials. And with those binary operations, this is again a commutative ring with multiplicative identity and multiplicative identity is the constant polynomial one.

So if F is a polynomial with coefficients in A, so F we can write it as $a_0+a_1X+...+a_nX^n$. This n is the degree F, where a n is the last non-zero coefficient. This a n is also called leading coefficient of F. And we call F monic if a_n is a unit in A. Now let me recall little bit. Since I said unit, let me recall few facts about this. So in general, this we will need it later also. So I would prefer that we get acquainted from the beginning.

(Refer Slide Time: 2:59)



A ring (commutative)

$(A,+)$ abelian group 0

$(A,\cdot)$ monoid 1

$+, \cdot$ are compatible distributive laws.

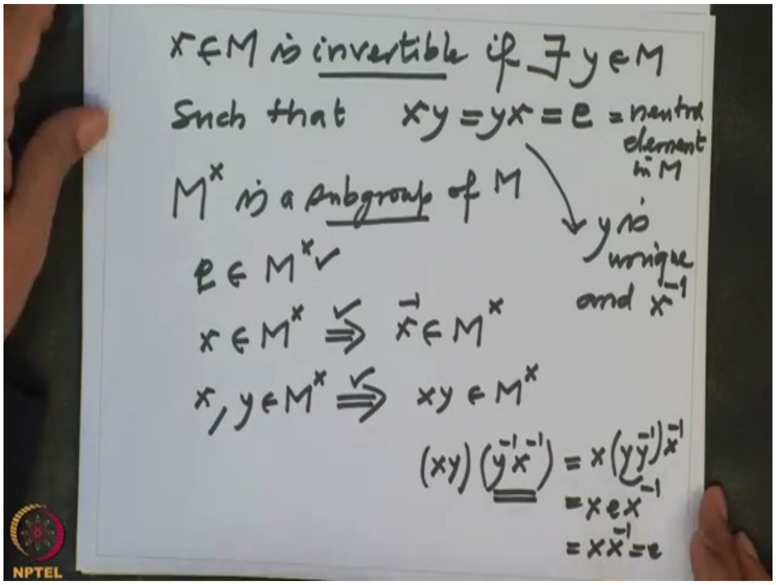
More generally, if $(M,\cdot)$ is a monoid

$M^{\times} := \{x \in M \mid x \text{ is "invertible" in } M\}$

So whenever I have a ring A, remember ring for us is always commutative, so I will not keep saying all. Throughout this course, we will consider commutative rings. That means what? That means (A,+) is an Abelian group and (A,.) is monoid. And plus and multiplication are compatible. That means distributive laws, they satisfy distributive laws. So the neutral element with respect to addition is 0 and neutral element with respect to multiplication is 1. That is how we have noted.

So I am going to make efforts to write 0_A and 1_A . So this means they are identity element with the respective binary operations in A. Now this monoid, A dot, see this is an Abelian group, so every element is an inverse. So in this monoid, some elements are invertible, some elements are not invertible. Now what is invertible means? So more generally, when, if (M,.) is a monoid, monoid means it is a binary operation, associative binary operation and there is an neutral element with respect to that binary operation. Then I will denote by M^x , all elements x of M such that x is invertible in M.

(Refer Slide Time: 5:39)



$x \in M$ is invertible if $\exists\, y \in M$

Such that $xy = yx = e$ = neutral element in M

$M^{\times}$ is a subgroup of M

y is unique and x^{-1}

$e \in M^{\times}$ ✓

$x \in M^{\times} \overset{\checkmark}{\Rightarrow} x^{-1} \in M^{\times}$

$x, y \in M^{\times} \overset{\checkmark}{\Rightarrow} xy \in M^{\times}$

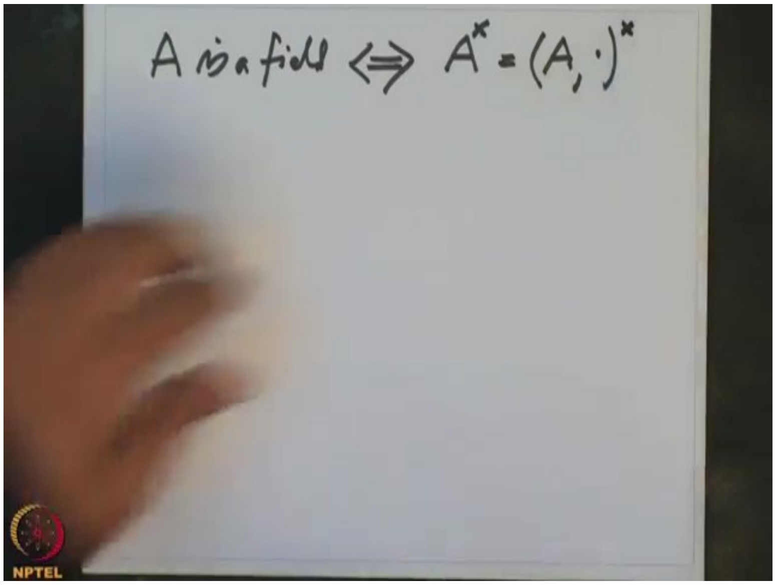
$$(xy)(\underline{y^{-1}x^{-1}}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$$

What does invertible mean? So that means, so invertible means an element x in M is invertible if there exist an element y in M such that $x.y=y.x=e$. So this e is the neutral element in M. Such an element is called a neutral invertible element in M. And the set of invertible elements is denoted by M^x . So it is clear that this M cross is a subgroup of M. So what does that mean?

That means the binary, the same binary operation of M induce a binary operation on this set M^x . And with respect to that binary operation it is a group. So that is obvious because, so what do I have to check for this? We have to check that the neutral element belong to M^x which is clear. Also, if x is in M^x , then the inverse is the unique element that y. See, this y unique and then y is called the inverse of M. So then the inverse of, so that this y is called, y is unique and it is denoted by x^{-1} .

So this is in the multiplicative notation. When you are using an additive notation, then the inverse will be denoted by -x. So this is also in M^x . Two elements, if x and y are in M^x , then x, y is also in M cross. So what will be the inverse of xy? $x^{-1}y^{-1}$ will be, inverse of xy will be precisely $xyy^{-1}x^{-1}=e$. So this will be the inverse of this, so that check this. This is obvious. This is also clear. So this is a subgroup of M^x .

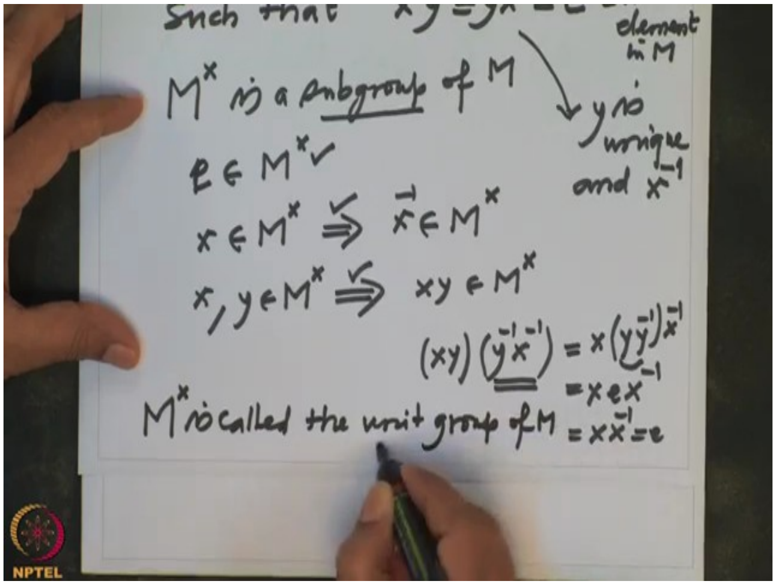
(Refer Slide Time: 8:39)



A is a field $\Longleftrightarrow A^{\times} = (A, \cdot)^{\times}$

So this, so how do we test some ring is a field or not? So now it has become easier to state A is a field if and only if this A^x , the unit group of, this is called a unit group of A is $(A,.)^x = A \setminus \{0\}$. So A, dot and then the cross. This monoid, and take the cross of that.

(Refer Slide Time: 9:06)



Such that $xy = yx = e$

element in M

y is unique and x^{-1}

$M^{\times}$ is a subgroup of M

$e \in M^{\times}$ ✓

$x \in M^{\times} \Rightarrow x^{-1} \in M^{\times}$ ✓

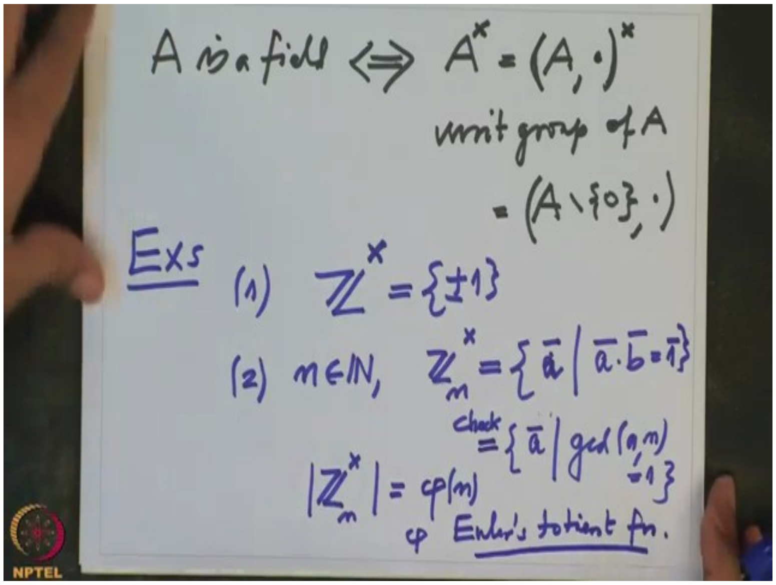
$x, y \in M^{\times} \Rightarrow xy \in M^{\times}$ ✓

$(xy)(\underline{y^{-1}x^{-1}}) = x(\underbrace{yy^{-1}})x^{-1} = xex^{-1} = xx^{-1} = e$

$M^{\times}$ is called the unit group of M

Just let me, I want to just say it here that this M cross is called the unit group of M. So when you have a ring, you have two binary operations, addition and multiplication. And with respect to addition, it is already Abelian group, so we do not have to worry, every element has invertible. With respect to multiplication is the only complication. Because if the elements are not invertible, we cannot cancel them easily. For example, in ring of integers only two elements have multiplicative inverses, $\{ \pm 1 \}$.

(Refer Slide Time: 9:53)



A is a field $\Leftrightarrow$ $A^\times = (A, \cdot)^\times$

unit group of A

$= (A \setminus \{0\}, \cdot)$

Exs

(1) $\mathbb{Z}^\times = \{\pm 1\}$

(2) $n \in \mathbb{N}$, $\mathbb{Z}_n^\times = \{\bar{a} \mid \bar{a} \cdot \bar{b} = \bar{1}\}$

$\overset{\text{check}}{=} \{\bar{a} \mid \gcd(a, n) = 1\}$

$|\mathbb{Z}_n^\times| = \varphi(n)$

φ Euler's totient fn.

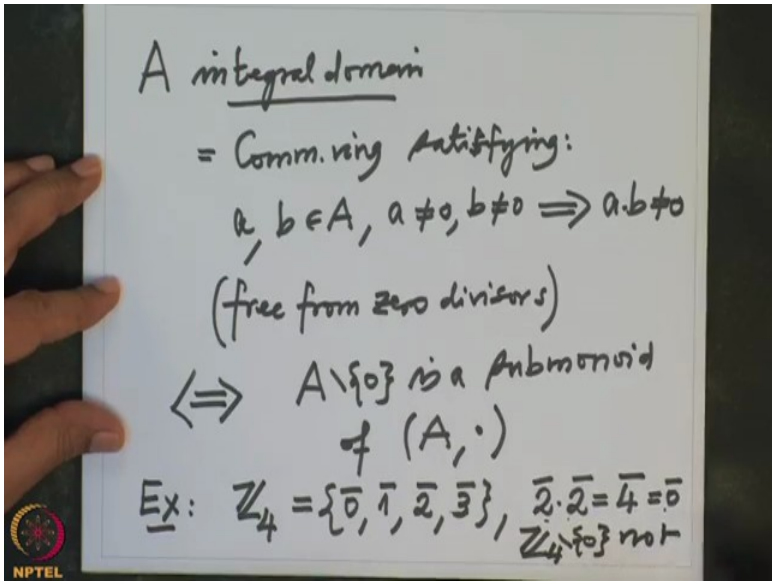
So it is very important to study a monoid, multiplicative monoid of the ring and take the invertible elements in that and that is a subgroup under multiplication of M. This subgroup is called unit group of A. So when it is a field, this unit group is a maximum possible. That means this one has to be equal to all non-zero elements, then only it is a field. Because this means that every non-zero element is invertible.

And remember that 0, you cannot hope to have inverse as 0. 0 is, it is additive identity, so you cannot hope to have inverse. So these are the maximum possible. So for example, let us see some examples. For example, if you take ring of integers, if I take ring of integers and take the unit group, so I do not have to assume now, I do not have to write in the notation that I am talking about a unit group with respect to multiplication. Because with respect to addition, everybody is invertible, so the question does not arise. So these are precisely $\{ \pm 1 \}$.

It is a nice exercise for you to find out for any n, natural number n, what is the unit group. $\mathbb{Z}_n^x$. These are precisely all those remainders. So all those $\bar{a}$ such that $\bar{a}\bar{b}$ is $\bar{1}$. But we will easily see that these are precisely all those, these we can identify this side, all those a bar such that gcd of a and n is 1. I want you to check this. So therefore, order of the unit group in the first example is 2. Order of this unit group order, that is cardinality of $\mathbb{Z}_n^x$, these are precisely all those integers between 0 and n, which are relatively prime to n.

And you know that is precisely $\phi(n)$. This phi of n is called, ϕ is called Euler's totient function. So field, to study equations, solving equations over an arbitrary ring is as I have shown you in last lecture that when there are elements in the ring which are not invertible with respect to multiplication, they cause lot of problem because we cannot cancel immediately. Therefore we are going to concentrate only when the coefficient ring is a field. And last time I gave some examples of field and I will give you still more examples. But today I will continue our study of polynomials still more.

(Refer Slide Time: 13:46)



A integral domain

= Comm. ring satisfying:

$a, b \in A, a \neq 0, b \neq 0 \Rightarrow a.b \neq 0$

(free from zero divisors)

$\Longleftrightarrow$ $A\setminus\{0\}$ is a submonoid of $(A, \cdot)$

Ex: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, $\bar{2}\cdot\bar{2} = \bar{4} = \bar{0}$

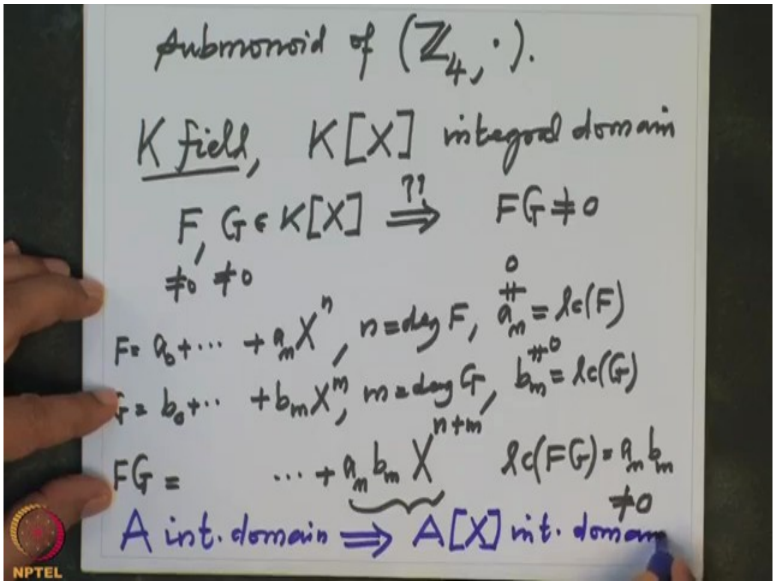
$\mathbb{Z}_4\setminus\{0\}$ not

So let me formally also define when you say integral domain, that means it is a commutative ring and satisfying a property that whenever I have two non-zero elements in the ring A; a, b, both non-zero, then their product should be non-zero. So this means also, this is also said free from zero divisors. Then you call it an integral domain. That you can test it again by using the multiplicative monoid very easily.

This is equivalent to saying, if you take $A\setminus\{0\}$, this is a submonoid of a multiplicative monoid (A,.). Under the multiplication it is a submonoid. So that is because if I have two non-zero elements, their product is again here. So it is a closure property that is very important. In general, this is not a submonoid. For example, if you take $\mathbb{Z}_4$ ={ $\bar{0},\bar{1},\bar{2},\bar{3}$ }.

Because these are precisely the remainders, possible remainders after dividing by 4. And in this $\bar{2}\bar{2}=\bar{0}$. So when I remove 0 from $\mathbb{Z}_4$, it is not closed under the multiplication. Therefore, $\mathbb{Z}_4\setminus\{0\}$ is not a submonoid, not submonoid of ($\mathbb{Z}_4$,.) .

(Refer Slide Time: 16:18)



Submonoid of $(\mathbb{Z}_4, \cdot)$.

K field, $K[X]$ integral domain

$\underset{\neq 0}{F}, \underset{\neq 0}{G} \in K[X] \overset{??}{\Longrightarrow} FG \neq 0$

$F = a_0 + \cdots + a_m X^n$, $n = \deg F$, $\overset{0}{\overset{\#}{a_m}} = lc(F)$

$G = b_0 + \cdots + b_m X^m$, $m = \deg G$, $\overset{\neq 0}{b_m} = lc(G)$

$FG = \cdots + \underbrace{a_m b_m X^{n+m}}$ $lc(FG) = \underset{\neq 0}{a_m b_m}$

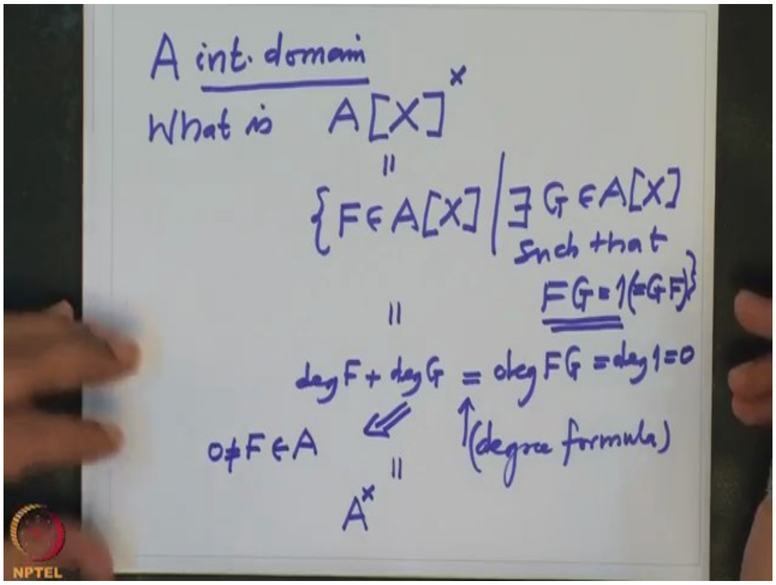
A int. domain $\Longrightarrow$ A[X] int. domain

And then you can write down many examples like this. So remember our example. We are going to concentrate on, I will have a field K, K is a field and we will take all polynomials with coefficients in K, that is K[X]. And this is clearly an integral domain. So to check this, what do I have to check? If I have two non-zero polynomials, both non-zero, then the product also should be non-zero. This is what we need to check to justify that it is an integral domain.

But that is because you see here F is non-zero polynomial, so it has a leading coefficient, the degree is n, degree may be 0. The constant polynomials precisely have degree 0. G is also looking like this: $b_0+...+b_m X^m$, where m is the degree of G. And this a_n is a leading coefficient, lc of F. And this _ m is lc of G. And what will be our multiplication will tell us? That F times G, the top degree term will be precisely $a_n b_m X^{n+m}$ + the lower degree terms.

So this is the highest degree term. So leading coefficient of F times G is precisely a n times b m. And because we are in a field, K is a field, if I take two non-zero elements, this is non-zero, this is also non-zero, two non-zero elements, then the product cannot be 0, because we are in a field. Fields are integral domains. So therefore, this cannot happen. In fact, we do not even need, for this we do not even need K to be field. It is enough that it is an integral domain, that is what we have used. So in fact, we know A integral domain. Then what we have proved is A[X] is also integral domain. Then what about the, in this case what about the unit group? That is also very easy now.

(Refer Slide Time: 19:24)



A int. domain

What is $A[X]^{\times}$

$\|$

$\{F \in A[X] \mid \exists\, G \in A[X]$ such that $\underline{FG = 1}\,(= GF)\}$

$\|$

$\deg F + \deg G = \deg FG = \deg 1 = 0$

$\Leftarrow$ $\uparrow$ (degree formula)

$0 \neq F \in A$

$\|$

$A^{\times}$

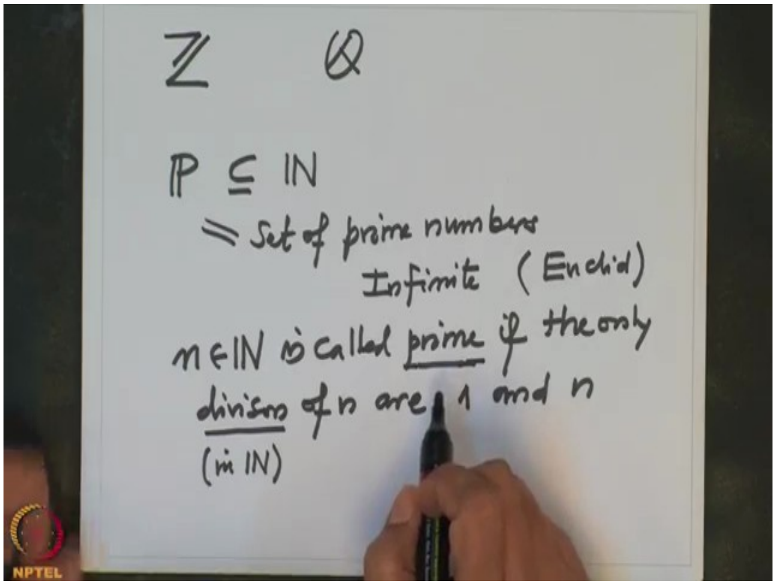
So just let us check that if A integral domain, then what will be the, what is A polynomial X and then the unit group $A[X]^x$? That means what? What is this set? This set is precisely all those polynomials with coefficients in A such that this F is a unit in A[X]. That means there exists G in X such that F times G equal to the multiplicative identity in this polynomial ring which is the constant polynomial 1. And which is, we will not write this. No need to write this. So I will write in a bracket that is also G times F.

Because our operations are commutative, so we do not have to bother about this. So all those polynomial, we want to know what are all polynomials with coefficients in A for which there is another polynomial G so that F times G is 1. But it is clear that this is precisely, this condition will force what? If I compare the degrees, degree of F times G equal to degree of 1 which is 0, degree of 1 is 0, it is a constant polynomial.

On the other hand, we know that degree of the product is degree F + degree G, because the leading coefficient of this product polynomial is precisely the leading coefficient of this. So therefore, this is called the degree formula. And that equality happens because of our assumption, A is an integral domain. So therefore, but then which, if the degrees are 0, then that means F is also, should be constant polynomial. Not only constant but the non-zero constant. So therefore, this is precisely, set is precisely A^x .

So this will mean, this means F is non-zero constant. F is in A and F is non-zero. So therefore, the unit group will not change if you take polynomials. So that is same as unit group of A. And we will, as the course progresses, you will see the information which comes from unit group is very very important to deduce many consequences for the good results. Now the most important thing that we have been using in our school days, I want to recall couple of things about that.

(Refer Slide Time: 22:35)



$\mathbb{Z}$ $\mathbb{Q}$

$\mathbb{P} \subseteq \mathbb{N}$

= Set of prime numbers

Infinite (Euclid)

$n \in \mathbb{N}$ is called prime if the only divisors of n are 1 and n

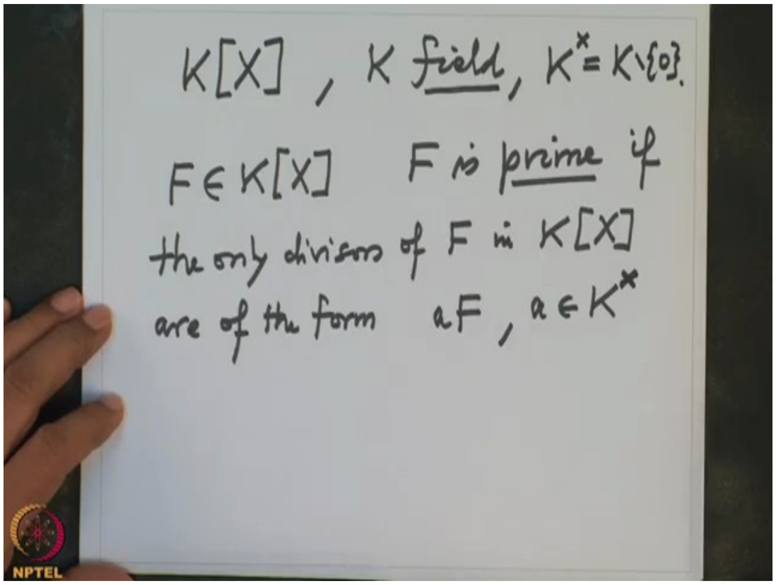
(in $\mathbb{N}$)

So for example, in the ring $\mathbb{Z}$ of integers I have defined you what are the prime numbers. P is the set of prime numbers and P we are considering a subset of $\mathbb{N}$. That simply means, when we say prime number, that means by definition we assume them they are positive. So this is the set of prime numbers. And we have seen that they are infinitely many. This set is infinite, that we have seen Euclid’s proof that there are infinitely many prime numbers.

We know that, so what was the definition of prime number? The only divisors are, so a number n, positive number n, so that is a natural number n is called prime if the only divisors of n are 1 and n. And when I say divisors, we should better write in $\mathbb{N}$. This is very important writing like this because you see - n is also divisor of n if you allow me to go divisors in $\mathbb{Z}$. Or if you allow me, if I go in rational numbers, then anybody will divide n, because I am allowed to do the denominators. 1 by n will also divide.

So therefore it is very important to say where you are taking the divisors. So that is a definition of a prime number. This was told to us in a school. This is not very, this is correct, this is not wrong definition, but it is not good for the future opening. It is not more general definition. So soon I will define it more general than the definition this which will work in general ring. This works only in the $\mathbb{Z}$. And not only in $\mathbb{Z}$, it only works in a positive.

(Refer Slide Time: 25:17)



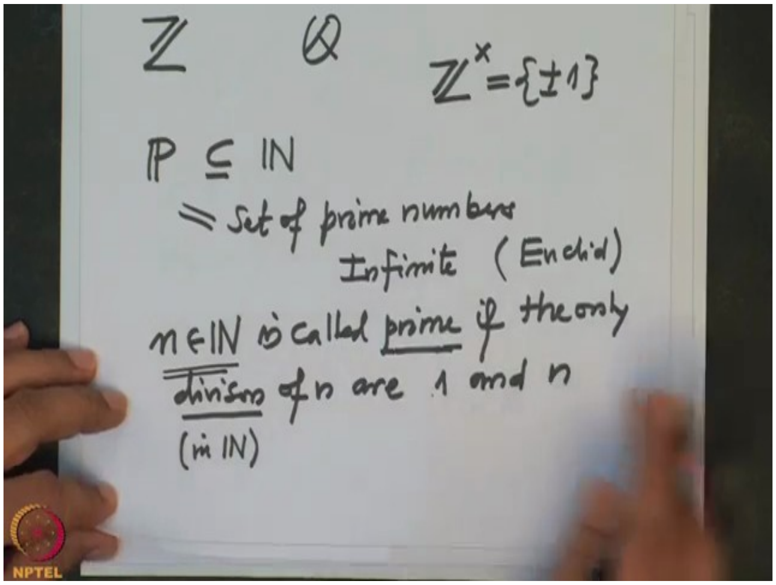
$K[X]$, K field, $K^{\times} = K \setminus \{0\}$.

$F \in K[X]$ F is prime if the only divisors of F in $K[X]$ are of the form aF, $a \in K^{\times}$

So for example, if I want to say, let us take our concrete example of this, this is my ring now, K[X]. K is a field. This is what our main interest in this course. And K is an arbitrary field, may not be finite, may not be $\mathbb{Q}$, may not be $\mathbb{R}$, maybe $\mathbb{C}$ or arbitrary field. Then when do I say a polynomial F is a prime polynomial? When do I say F is prime? If, now I should also define like that, about what are the divisors but now I have to say divisors here.

If the only divisors of F in K[X] are of the form a times F, where a varies in a non-zero element in the field. So that is K^x . Remember K^x because K is a field. K^x is what? K^x is all non-zero elements. That is, and why does it come from? Why does it not appear in this definition of $\mathbb{Z}$?

(Refer Slide Time: 26:55)



$\mathbb{Z}$ $\mathbb{Q}$ $\mathbb{Z}^{\times}=\{\pm 1\}$

$\mathbb{P} \subseteq \mathbb{N}$

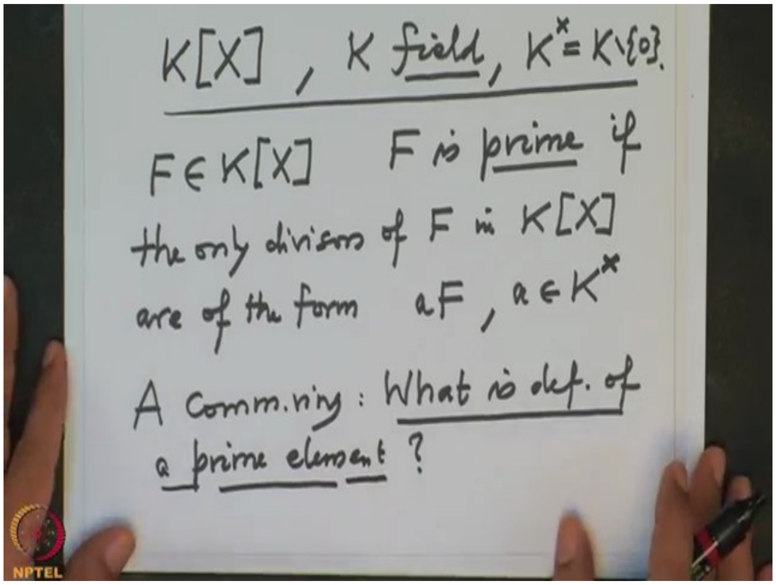
= Set of prime numbers

Infinite (Euclid)

$n \in \mathbb{N}$ is called prime if the only divisors of n are 1 and n (in $\mathbb{N}$)

It does not appear here because we have banned it. Because you see what is $\mathbb{Z}^x$; $\mathbb{Z}^x=\{\pm 1\}$. And we made it shortcut here by taking elements only in $\mathbb{N}$. So that -1 got canceled here. -1 was rejected because of this assumption. So it is only 1 and n.

(Refer Slide Time: 27:20)



$K[X]$, K field, $K^{\times} = K \setminus \{0\}$.

$F \in K[X]$ F is prime if the only divisors of F in $K[X]$ are of the form aF , $a \in K^{\times}$

A comm. ring : What is def. of a prime element ?

So more generally, this is, in this case this is exactly are the prime elements. This is also not very satisfactory. I will show as we progress. This K may not be field always. So we should really have a definition in, when arbitrary A is arbitrary commutative ring, then what is the definition of, so what is the definition of a prime element? I am just raising this question here so that next time you will be better prepared. You please think about it. What should be the right definition of a prime element in general in a ring? Okay, so we will continue after the break.