Introduction to Algebraic Geometry and Commutative Algebra

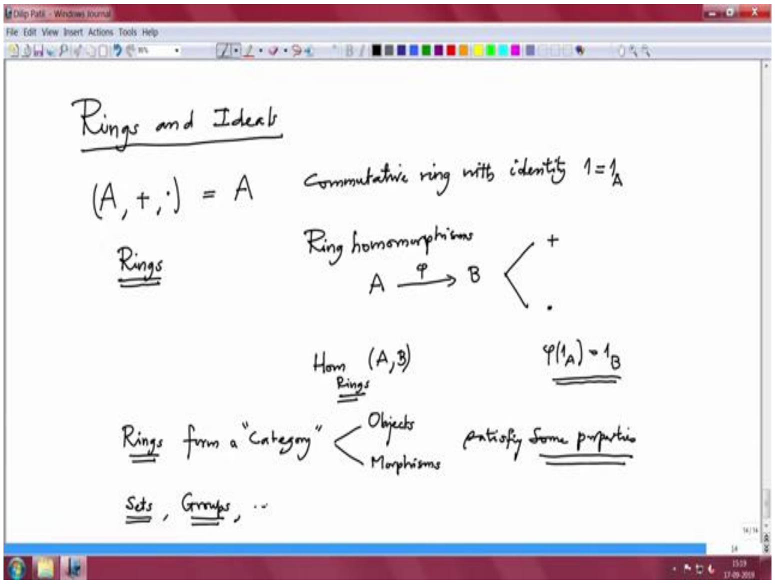
Dr. Dilip P. Patil.
Department of Mathematics, IISER Pune.
Indian Institute of Science, Bengaluru.

Lecture 03

Rings and Ideals

Welcome to the second lecture on Introduction to Algebraic Geometry and Commutative Algebra. In the last lecture you have seen definition of Affine algebraic, k algebraic set.

(Refer Slide Time: 00:47)



Rings and Ideals

$(A,+,\cdot) = A$ Commutative ring with identity $1 = 1_A$

Rings

Ring homomorphisms

$A \xrightarrow{\varphi} B \left< \begin{matrix} + \\ \cdot \end{matrix} \right.$

$\mathrm{Hom}_{\text{Rings}}(A,B)$ $\varphi(1_A) = 1_B$

Rings form a "Category" $<$ Objects, Morphisms satisfy some properties

Sets, Groups, ..

So, I will not recall much because after few algebraic preliminaries we have to again recall something. So, I will directly start with some topics which we will need more often later, which I will recollect now, some of the basic stuff, so this is Rings and Ideals.

I will also be brief in this section because I assume that many of you are acquainted with these basic topics, but for the sake of completeness, I will recall them briefly. So, as usual ring that we recall last time it has two operations plus and dot. So, with respect to plus Abelian group, with respect to multiplication it is a monoid and so on. So, I will abbreviate just these by A.

And we saw in the last lecture and as I said always we will assume always commutative, that mean these multiplication operation is commutative, commutative ring with identity and the identity is denoted by 1 or 1 which is 1 A, this will only, we will use only these notation when there is a chance of confusion and there are many rings under consideration are involved.

And then collection of all rings that is, I will keep denoting like this, rings, rings with double, underline and of course, we have ring homomorphism between the two rings, how do you compare two rings, is a ring homomorphism, ring homomorphism between the two rings A and B, just a map phi such that it should respect addition.

So, I will write abbreviately and maybe talk more because I we are assuming this but for the sake of completeness we are recalling, it respect plus, it respects multiplication and also 1 goes to 1. So phi of 1A is 1B this is also very important condition to assume, I just want to say one caution that some books they usually consider rings without identity and ring homomorphism may not map identity to identity, but we are not going to go in that generality because our main aim is to study rings which arise from algebraic geometry.

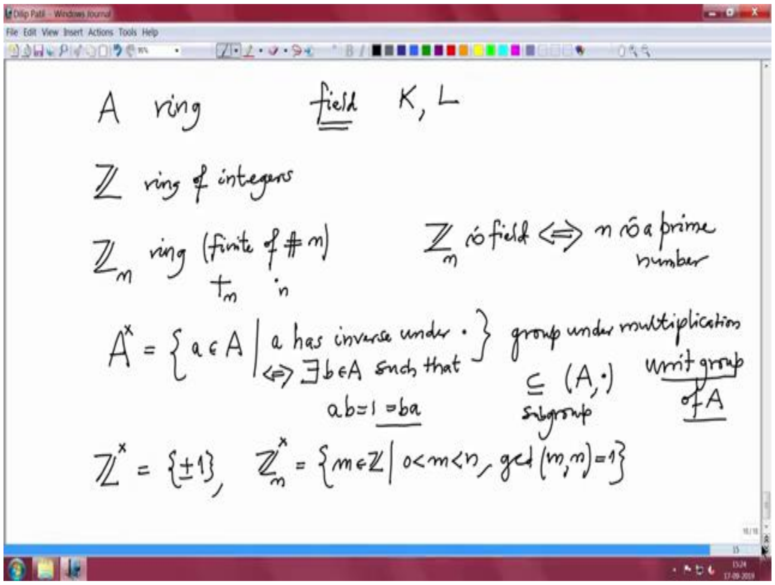
And those are mainly polynomial rings and rings which are constructed from the polynomial rings. So, ring homomorphism defined then, this set of all rings homomorphism from A to B denoted by Hom, Hom is for homomorphism rings AB, this is the set of all ring homomorphism from the ring A to the ring B and I will just note here that rings with this ring homomorphism form a categories.

So, this precisely in the due course I will make it more and more clear. So, this right now just it is the objects whenever you have category, there are objects and their morphism and this had some properties, this to satisfy some obvious property, this properties I will, I will recall in the due course, but in this case they are obvious.

So objects are rings morphisms are rings homomorphism and so, what are obvious properties we need they are satisfied in this case, so do not worry about it. So, before that there is a category of sets, the category of objects are sets and morphisms are maps between the sets. Similarly, there will be groups and so on.

So, category means two things, the data given is there objects and there morphism and this should satisfy some properties and the properties are for example, composition, identity map and so on. So, more and more when I need it I will keep recalling it so, that this definition will become more and more precise right now, you only deal with examples.

(Refer Slide Time: 06:54)


Dilip Patil - Windows Journal
File Edit View Insert Actions Tools Help

A ring $\qquad$ <u>field</u> K, L

$\mathbb{Z}$ ring of integers

$\mathbb{Z}_n$ ring (finite of # n) $\qquad$ $\mathbb{Z}_n$ is field $\Longleftrightarrow$ n is a prime number

$+_n \quad \cdot_n$

$A^\times = \{a \in A \mid a$ has inverse under $\cdot \Longleftrightarrow \exists\, b \in A$ such that $ab = 1 = ba\}$ group under multiplication $\subseteq (A, \cdot)$ subgroup $\qquad$ unit group of A

$\mathbb{Z}^\times = \{\pm 1\}, \quad \mathbb{Z}_n^\times = \{m \in \mathbb{Z} \mid 0 < m < n, \gcd(m, n) = 1\}$

So, now, how do we know so the ring A, so this is ring, if you have seen when you studied linear algebra, usually the base was a field. So, field and what is the main advantage in the field? That it is a ring of course, but every nonzero element is inverse, which is not true in the case of ring because a typical example of a ring is Z, this is ring of integers and polynomial rings. So, fields are usually denoted by K, L etcetera, rings are denoted by A, B, C, R etcetera. So, this is a first example of ring also another typical example we will keep using it Z modulo n so this is also ring.

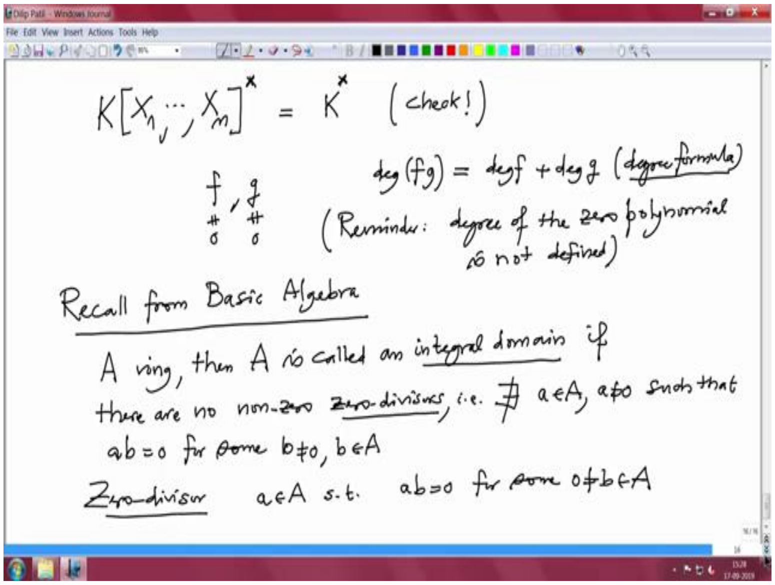
This is a finite ring and finite of cardinality equal to n, this is ring in general commutative, the operations are addition modulo n and multiplication modulo n. So, you add usually and divide by an intake the remainder that is the definition of addition modulo n and similarly, multiplication modulo n.

So, these rings are not fields in general but you would have studied in your first course on algebra, the Z mod n is a field, if and only if n is a prime number. So, we will have lots of examples of a field but the real obstacle, why algebra or arbitrary ring becomes more difficult than the linear algebra, that is algebra over field. That is because the units may be too few.

So, for a general ring A I will denote A cross, these are all the elements in A such that A has inverse under multiplications. That means what? So, this means that is if and only there exist B in A, such that AB equal to 1 and also BA equal to 1. We do not have to say this because we are assuming the ring is commutative. So, this is obviously a group under multiplication, in fact it is a subgroup of the monoid A dot, this is a sub group and this group is, this can be too small.

So, for example, in case of Z this is just two elements plus minus 1 and in case of Z modulo n it is just all those integers m in Z such that 0 less than m, less than n, and gcd of m and n is 1, o prime integers in between 0 and m. So, this is called a unit group of the rings, this group is called unit group of A, the smaller the group it is we will have difficulties in studying the equations so, this is about the ring.

(Refer Slide Time: 11:21)


Dilip Patil - Windows Journal
File Edit View Insert Actions Tools Help

$K[X_1, \ldots, X_m]^{\times} = K^{\times}$ (check!)

$\underset{\neq 0}{f}, \underset{\neq 0}{g}$ $\deg(fg) = \deg f + \deg g$ (degree formula)

(Reminder: degree of the zero polynomial is not defined)

Recall from Basic Algebra

A ring, then A is called an integral domain if there are no non-zero zero-divisors, i.e. $\nexists$ $a \in A$, $a \neq 0$ such that $ab = 0$ for some $b \neq 0$, $b \in A$

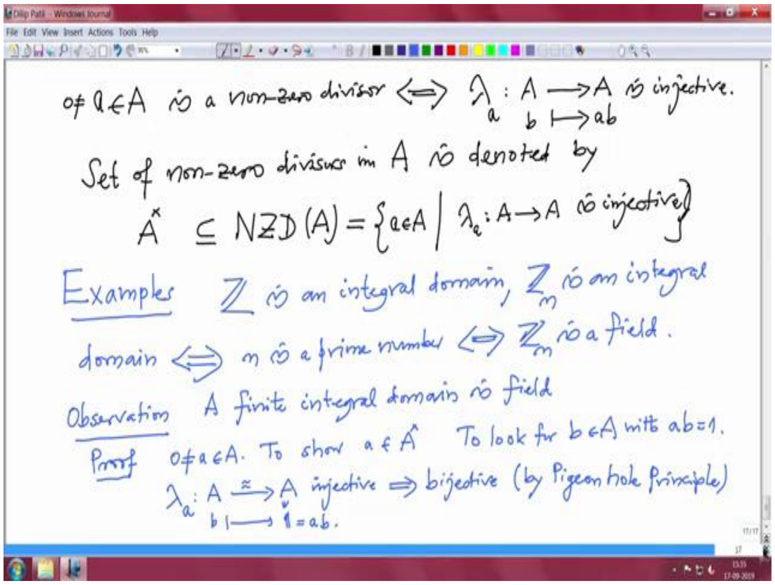
Zero-divisor $a \in A$ s.t. $ab = 0$ for some $0 \neq b \in A$

Now, another last lecture we have mainly considered this rings, polynomial rings K X 1 to Xn, polynomial ring in n variables, in this case the units are precisely the constants nonzero constants. So, the unit group does not change, this I will leave it for you to check, this is very important fact we will use it again and again. So, there are not too many units. So, these will follow from the fact that if I have two polynomials f and g degree of f time g equal to degree f plus degree g. These are if they are nonzero polynomials both are non zero then this, remember I just want to remind you, reminder degree of the zero polynomial is not defined.

So, sometime this is also called a degree formula and this is more generally also true now let me recall, I am just recalling these few facts on the basic algebra one has learned, recall from basic algebra, when do you call and A ring and you call A is called an integral domain, if there are no non zero divisors. So, what is a zero divisor? That is there does not exist any A in a nonzero such that A times B 0 for some non zero B.

So, such an element A if there exists such a B, B non zero and A B zero then A is called a zero divisors and if there is no such they will call it a…So zero divisor by definition, zero divisor means an element A in a such that A times B is zero for some non zero B and we call it as zero divisor. So the zero dividers are the most troublesome because you cannot cancel them.

(Refer Slide Time: 15:14)


Dilip Patil - Windows Journal
File Edit View Insert Actions Tools Help

$0 \neq a \in A$ is a non-zero divisor $\Longleftrightarrow$ $\lambda_a : A \longrightarrow A$, $b \longmapsto ab$ is injective.

Set of non-zero divisors in A is denoted by

$$A^{\times} \subseteq NZD(A) = \{a \in A \mid \lambda_a : A \to A \text{ is injective}\}$$

Examples $\mathbb{Z}$ is an integral domain, $\mathbb{Z}_m$ is an integral domain $\Longleftrightarrow$ m is a prime number $\Longleftrightarrow$ $\mathbb{Z}_m$ is a field.

Observation A finite integral domain is field

Proof $0 \neq a \in A$. To show $a \in A^{\times}$ To look for $b \in A$ with $ab = 1$.

$\lambda_a : A \xrightarrow{\approx} A$ injective $\Rightarrow$ bijective (by Pigeon hole Principle)

$b \longmapsto 1 = ab$.

So, equivalently so, element A is a nonzero divisor if and only if non zero A, if and only if the multiplication by A, this is a map from A to A, this map is just simply any B going to A times B. A is injective, this is equivalent definition. So that is an integral domain.

The set of non zero divisors, this is a very important set as you will see in coming lectures, in the ring A is denoted by NZD of A this is a set of all non zero divisors in A, in the notation this is same thing as all the A in A such that lambda A to A is injective.

Once A is injective A cannot be zero. So, that is a set of non zero divisors we well denote. Now, the next thing for example, in the examples, some examples, Z is an integral domain, there are no zero divisors in Z, that is obvious because in multiplication of two nonzero integers is again non zero is one. Also, when is Z mod n is an integral domain, if and only if n is a prime number if and only if Z modulo n is a field.

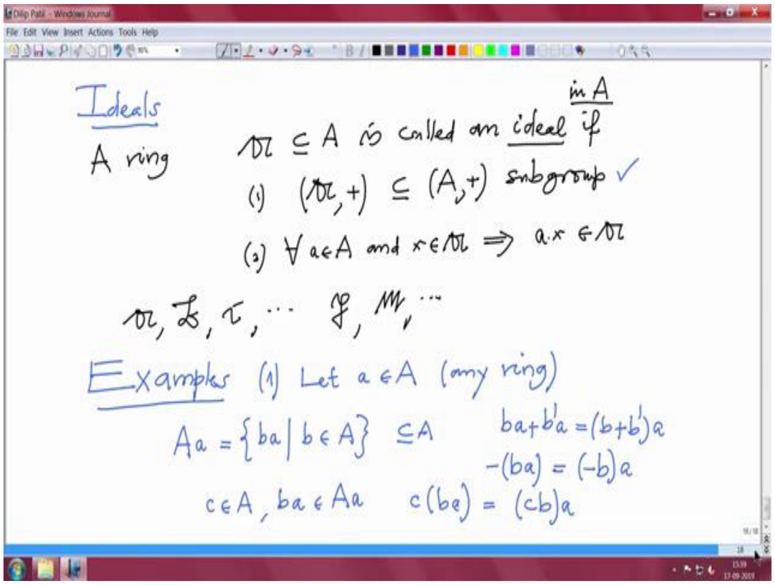
That is also clear from this middle work. But we can also nicely observed that this observation is very useful sometimes, a finite integral domain is a field so proof, of course field is always an integral domain, field everybody is a unit. Therefore, units are nonzero divisors. So, I forgot to mention here the non zero divisors, set of non zero divisors contains these unit group because any unit is a nonzero divisor, that even can see easily from here.

So, proof of this, so, suppose A is finite integral domain, we want to show that every nonzero A, to show it belongs to a unit. That is what we want to show because A field if and only if the unit group is the maximum one that is in case of field unit group is just removing zero all the units that is all the unit group. So, to show this I have to produce, so A B, so I have to produce so to look for B in A with A B equal to one, because we are commutative case always. So how do you look for B.?

So, look at this multiplication map by A it is a map from A to A and because A is an integral domain, every nonzero element is a non zero divisor. Therefore, the lambda map is injective but then it is a finite set, the map is from finite set to finite set and then use Pigeon Hole principle to conclude this map is bijective. Therefore, bijective write it by Pigeon Hole principle.

So, that means, this bijective means, one is here that should come from somebody. So, A has to go to one, but where do we go B? B goes to by definition A times B. So, we got one equal to A B and therefore, it is invertible. So, we have proved that finite integral domains are field. How do you know test somebody is a field or not?

(Refer Slide Time: 21:36)


Dilip Patil - Windows Journal
File Edit View Insert Actions Tools Help

Ideals

A ring $\quad \mathfrak{a} \subseteq A$ is called an ideal $\underline{\text{in } A}$ if

(1) $(\mathfrak{a}, +) \subseteq (A, +)$ subgroup ✓

(2) $\forall\, a \in A$ and $x \in \mathfrak{a} \Rightarrow a \cdot x \in \mathfrak{a}$

$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots \mathfrak{p}, \mathfrak{m}, \cdots$

Examples (1) Let $a \in A$ (any ring)

$Aa = \{ ba \mid b \in A \} \subseteq A \qquad ba + b'a = (b+b')a$

$-(ba) = (-b)a$

$c \in A,\ ba \in Aa \qquad c(ba) = (cb)a$

For that I will introduce what are called ideals. Last time also briefly we have dealt with some ideals in some, in connection with the affine algebraic K sets. So, let us recall what are ideal. So, ideal in a ring so, start with A is a ring and a subset A, this is a gothic of A is called an ideal.

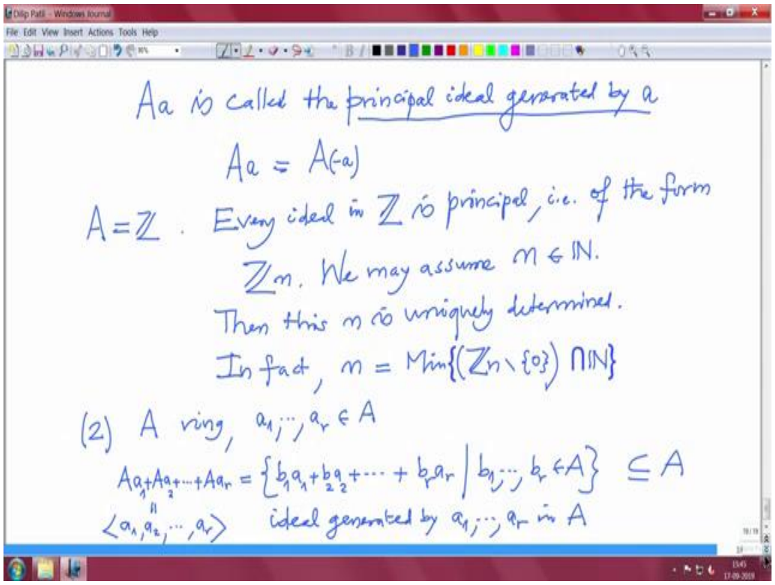
If two conditions, number one A with respect to the plus either subgroup of A plus, subgroup and second for every A in A and x in A x in the gothic A times x this is a multiplication ring, this falls inside gothic and such a thing is called an ideal in the ring A. Ideal to be precise you could write in A and usually I will denote in this course ideals by the gothic letters like A, B, C etcetera P, M etcetera, initially it is difficult to draw, but certainly they are not as difficult as our Indian alphabets.

So, and from the given ideals I will construct more ideals. Now, first how to give examples of ideals? So, some examples we should see, always every concept should be followed by some examples. So, let us take very well known simple what we have worked with the ring A equal to Z, ring of integers or let me first take arbitrary ring. So, let us take a arbitrary and let us take an element.

So let A fix an element A in the ring A, A is an ring. Now, what do you do? You take all A multiples of this small a so, that means I am taking at all b times a, where b is varying in the ring A, for the obvious notation for this set I will denote A times small a. Simply because this b is varying. So, they are all capital A multiples of this so, this is obviously a subset, obviously, if I take two such elements ba and another one b prime a and add them, it is again of these form, this is b plus b prime a. See, you have used the distributive law here.

So, therefore, this is closed under addition and also it closed under inverses because, additive inverse because minus of b times a equal to minus b times a. So, this is obviously a subgroup and the second. So, these we have checked this and second condition is also obvious because if I take any other c in A and any element ba in this multiples of a then, what c times ba? This is nothing but, I will now put a bracket like this c times b times a and this again have that form. So, you see, we have all the things which are stated in the definitions are used. So these becomes an ideal so, there are lots of ideals in a ring.

(Refer Slide Time: 26:20)


Dilip Patil - Windows Journal
File Edit View Insert Actions Tools Help

Aa is called the principal ideal generated by a

$$Aa = A(-a)$$

$A = \mathbb{Z}$. Every ideal in $\mathbb{Z}$ is principal, i.e. of the form $\mathbb{Z}m$. We may assume $m \in \mathbb{N}$.

Then this m is uniquely determined.

In fact, $m = \text{Min}\{(\mathbb{Z}n \setminus \{0\}) \cap \mathbb{N}\}$

(2) A ring, $a_1, \cdots, a_r \in A$

$$Aa_1 + Aa_2 + \cdots + Aa_r = \{b_1a_1 + b_2a_2 + \cdots + b_ra_r \mid b_1, \cdots, b_r \in A\} \subseteq A$$

$$\overset{\shortparallel}{\langle a_1, a_2, \cdots, a_r \rangle}$$ ideal generated by $a_1, \cdots, a_r$ in A

When does it become, this ideal A is usually called the principal ideal generated by a. This a is not uniquely determined by this ideal because you see a and a minus a will also generate the same ideal. So, A times A and A times minus A, these two ideals are same. So, now you specialize A equal to Z, then all in fact, we can prove stronger than this then every ideal in Z is principal, that is of the form Z times sum n and we may assume that n is actually a natural number.

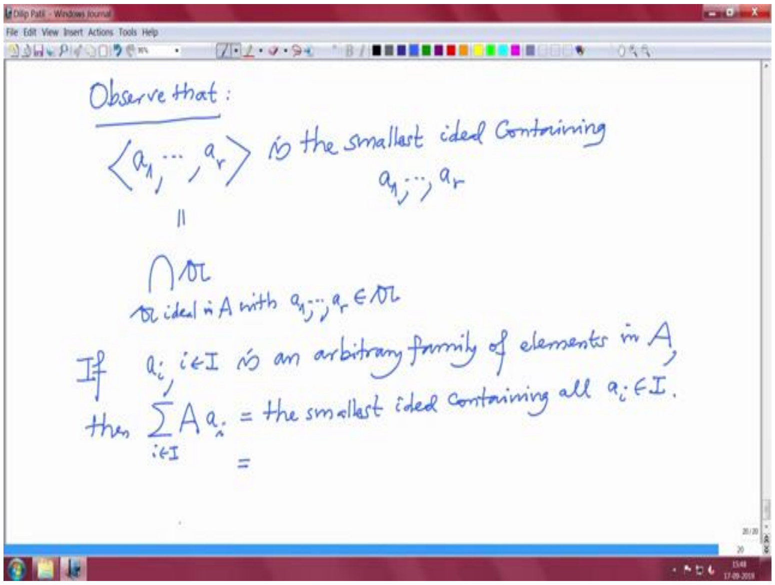
If it is negative, then you replaced by minus n and then you still get the same ideal and what is I advantage of this? Then this n is uniquely determined. In fact, n is the smallest and is the min among all multiples minus 0. So, that is and we can imitate this process for two elements, and three elements and finitely many elements or even arbitrary family of elements.

So yesterday I did a little bit but now little do it more precisely. So this equally, this is example two, A is arbitrary ring and let us take, first I will take only finitely many a1…ar arbitrary r elements in the ring A and then I want to write all a linear combinations of this a1 to ar. So, that means I am considering the collection b1 a1 plus b2 a2 plus, plus, plus, plus br ar where b1 to br are arbitrary elements in the ring A.

This is obviously a subset of A and what is the suggestive notation for the set is Aa1 plus Aa2 plus, plus, plus, plus Aar or when the ring is fix ring and there is no confusion this also we will write it as like this a1, a2…ar, sometimes we can write a also just to remember the ring. But not necessarily when the ring is fixed and when there is no chance of confusion.

So, again this is obviously an ideal, you have to check this is an ideal. So, what will you check? You will check that this one is a subgroup under addition and it is closed under arbitrary multiplication by an element in a so, that I will leave it for you, just imitate what we did in case of one element. So, this is called ideal generated by a1 to ar in the ring a.

(Refer Slide Time: 31:27)


Dilip Patil - Windows Journal
File Edit View Insert Actions Tools Help

Observe that:

$\langle a_1, \cdots, a_r \rangle$ is the smallest ideal Containing $a_1, \cdots, a_r$

$$\begin{array}{c} \langle a_1, \cdots, a_r \rangle \\ \| \\ \bigcap\limits_{\mathfrak{a} \text{ ideal in } A \text{ with } a_1, \cdots, a_r \in \mathfrak{a}} \mathfrak{a} \end{array}$$

If $a_i, i \in I$ is an arbitrary family of elements in A,

then $\sum\limits_{i \in I} A a_i$ = the smallest ideal Containing all $a_i \in I$.

=

Now, let us in other words so, observe that this is very important observation and you can use it many times, this a1 to ar is the smallest ideal containing all these elements, a1 to ar, once it contain a1 to ar obviously it will contain all the linear combination and it is a smallest means? This is ideal so, it has to be smallest. So, in other words in the notation, these mean this is equal to intersection of A and these intersection running over ideal in a with all these a1 to ar belong to a.

Obviously, there is at least one ideal which contain all the elements namely the capital A. So, this makes sense, see the problem will arise from set theory only when you have a set where there is the indexing cities empty set. So, that is the smallest ideal containing this. Now, if you have not finitely many elements but arbitrary family, so now I will write if ai y in i and I is an arbitrary family of elements in the ring A.

Then obviously now the other side is very good, then the smallest ideal containing all these elements is called the ideal generated by a1 to ai and again we will denote it by this one, then this notation while multiples of these and sum, this is by definition, this is the smallest ideal containing all ais.

That makes sense because there is at least one ideal which contain all of them namely the capital A and therefore, the smallest mix in you take the intersection, but you can also describe like earlier description. So, this is precisely the linear combination but now when you say linear combination you have to take finite linear combination.

So, let me write precisely set of all summation bj aj where j index running in j, where j is the finite subset of y, j is finite and these bj’s are element in the ring A. So, look at this finite linear combination all of them and obviously that forms an ideal the same checking and then this one. So, therefore this is called ideal generated by the family ai. So, I just to one being a little bit more, sure when do you call an ideal to be non unit ideal? A is called a non unit ideal if this A is not the whole ring, then you call it a non unit ideal. So, how do you check? Some ideal is unit ideal or non unit ideal.

(Refer Slide Time: 36:30)

So, an ideal A in the ring A is a unit ideal if A equal to the whole ring A and that is equivalent to saying equivalently sum u belongs to A for some unit u in A, because once u belong, then it has the inverse and if you multiply that inverse by u then that will be one and then therefore, one we belong here and so it will be equal. So just check this, this is obvious, but I would like you to keep checking things so that things become more and more easier.

So, another last observation, a ring A is a field if and only if A has exactly two ideals. Ones is zero, zero means, the singleton zero, this is obviously are an ideal and the unit ideal, these are the only two ideals because it is a field, once it is a field every nonzero element is a unit. So, if you have a non zero ideal it will continue unit and therefore, by observation it is a unit ideal.

Conversely, there are only two ideals, any nonzero element will generate a unit ideal because it is a non zero ideal and therefore, if A equal to A that is equivalent to saying A is a unit, all these are easy things to check. So, I will leave it for you to check this thing. And I will stop for this half and we should continue after the break. Thank you.