Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

ALGEBRA I

1. Lecture 34: Definition of a ring

Today, we are going to study rings. The most prototypical example of a ring is just the ring of integers, $\mathbb{Z}$. So, we have already thought of integers as a group, but we can think of integers as a ring if we not only look at addition, but we also look at multiplication. We could take $\mathbb{Z}_n$. A more interesting example of a ring is the ring of Gaussian integers which is denoted $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$. Other interesting examples, the polynomial ring $K[x]$ over a field K. A very different kind of example is you look at the ring $M_n(K)$ of $n \times n$ matrices with entries in K, and matrix addition and matrix multiplication.

An example is the set of all continuous functions on the real numbers. Now, the sum of two continuous functions is continuous and the product of two continuous functions is continuous. In the same way,$C_\infty(\mathbb{R})$ which are infinitely differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ since the sum of infinitely differentiable functions is infinitely differentiable and a product of infinitely differentiable functions is infinitely differentiable.

A ring $(R, +, \cdot)$ is a set R with two binary operations $+$ and $\cdot$, which is an abelian group under $+$ and is closed under the associative operation $\cdot$. We also have the property of distributivity

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

In this course, we will be mostly considering unital rings, but I just wanted to be aware that this last axiom of unitality is optional.

Let G be a group and fix a field K. Define $K[G]$ to be the K-vector space with basis 1_g for all $g \in G$. Multiplication is defined by setting $1_g 1_h = 1_{gh}$ and then extending bilinearly.

Rings come in different flavors. So, there are um we have already seen unital and non-unital rings and as I said we will be mostly look at unital rings um that are commutative and non-commutative rings. So, a commutative ring is a ring where multiplication is commutative. So, ab is equal to ba for all a, b in R. So, most of the examples we looked at earlier Z , Z mod N Z, um K x that is the ring of polynomials , continuous functions on the real numbers, infinitely differentiable functions on the real numbers , Gaussian integers these are all commutative ok. But M n R or over any field K n by n matrices over K when n greater than 2 and K G , the group algebra where G is not an abelian group. These are non-commutative rings ok and these these are somehow um sometimes two very different words, there are people who work only in commutative rings and then, there are people whose main interest lie in phenomena which occur with non-commutative rings. Another interesting type of ring is what is called an integral domain. So, um this name perhaps comes from the fact that it looks lot like the integers. In an integral domain , if two elements multiply to 0, then one of them must be 0 , then a equal 0 or b equal 0. In other words, if you take two non-zero elements, their product will always be non-zero ok. So, here we have a catalog of examples which of these are integral domains. So, integers are integral domains if you multiply two non-zero integers, you always get a non-zero integer. But here is an example of a non-integral domain, Z mod 6Z is not an integral domain why? Because 3 is not equal to 0 and Z mod 6 2 is not equal to 0, but 3 into 2 is equal to 6 which is congruent to 0 in Z mod 6Z. So, 3 and 2 are non-zero elements whose product is 0 in Z mod 6Z ok. A continuous functions um is this an integral domain? So, um I will well if you are familiar with calculus, then um you can see that continuous functions in R and C infinity functions in R are not integral domains. We can find functions with disjoint supports and when you multiply them, you get the 0 function. However, you can show that a Gaussian integers form an integral domain matrices so, M 2 K and of course, M n K for any K n greater than or equal to is not an integral domain. I will give you a simple example um. You have the matrix 1, 0, 0, 0 , 0, 0, 0, 1 if you multiply them, you get 0, 0, 0, 0. So, M 2 K is not an integral domain. Well, I will leave you with one more question, what about the group algebra , is this always an integral domain ?