MTH302: INTEGERS, POLYNOMIALS AND MATRICES
LECTURE 1

VARADHARAJ R. SRINIVASAN

1. Introduction

The course MTH302, *Integers, Polynomials and Matrices* is a fancy (rather comical!) name for a first course on Rings and Module run elsewhere. The course content is extremely important to understanding all of the mathematics you may encounter henceforth. We shall closely follow the book by C. Musili, *Rings and Modules* throughout this semester. The lecture notes will be updated frequently.

2. Basic Definitions and Examples

Semigroup: Let R be nonempty set. A *binary operation* $+$ on R is a map from $R \times R$ to R; $(r, s) \mapsto r + s$. We call $(R, +)$, a semigroup if $(r + s) + t = r + (s + t)$ for all $r, s, t \in R$. If S is a nonempty subset of a semigroup R then S is called a *subsemigroup* if $+$ restricts to a binary operation on S.

Group: A semigroup $(R, +)$ is called a *group* if

G1. there is an element $0_R \in R$, or simply $0 \in R$, (called the *additive identity* element) such that $r + 0 = r = 0 + r$ for all $r \in R$ and

G2. there is an element $s \in R$ for each element $r \in R$ such that $r + s = 0 = s + r$.

Abelian Group: A group $(R, +)$ is be called an *abelian group* if $r + s = s + r$ for all $r, s \in R$.

Subgroup: A nonempty subset S of group R is called a *subgroup* of $(R, +)$ if $+$ restricts to a binary operation on S, $0 \in S$ and for every $r \in S$, the inverses $-r \in S$.

Rings: Let R be a nonempty set with two binary operations $+$ and $\cdot$ such that

R1. $(R, +)$ is an abelian group

R2. $(R, .)$ is a semigroup

and for all $r, s, t \in R$,

R3. $(r + s) \cdot t = r \cdot t + s \cdot t$ and

R4. $r \cdot (s + t) = r \cdot s + r \cdot t$.

Then $(R, +, \cdot)$ is a called a *r*ing. Furthermore, if $r \cdot s = s \cdot r$ for all $r, s \in R$ then $(R, +, \cdot)$ is called a *c*ommutative ring. If $(R, +, \cdot)$ is a ring and there is an element $e \in R$ such that $a \cdot e = e \cdot a = a$ for all $a \in R$ then e is called an (the) *identity* (or *unity*) of the ring R corresponding to $\cdot$ operation (should not be confused with 0, which is the identity with respect to $+$). We write "Let $(R, +, \cdot)$ be a ring with identity", to mean that R has an identity e corresponding to the $\cdot$ operation.

If $(R, +, \cdot)$ is a ring with identity e. Then e is an unique such element: If $t \in R$ is also an identity then $e = e \cdot t = t \cdot e = t$. We use the notation 1 or 1_R to denote the identity element of $(R, +, \cdot)$.

Examples.

1. $(\mathbb{Z}, +, .)$, the set of integers with usual addition and multiplication (1 is the identity).
2. $(\mathbb{Q}, +, .)$, the set of rational numbers with usual addition and multiplication (1 is the identity).
3. $(\mathbb{R}, +, .)$, the set of real numbers with usual addition and multiplication (1 is the identity).
4. $(\mathbb{C}, +, .)$, the set of complex numbers with usual addition and multiplication (1 is the identity).
5. Let $F = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. The set of all $n \times n$ matrices over F, denoted by $M_n(F)$, is a ring with identity under the matrix addition and multiplication: Let

$$(r_{ij}) := \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix}, \text{ where } r_{11}, r_{12}, \cdots, r_{nn} \in F.$$

Matrix addition: $(r_{ij}) + (s_{ij}) = (r_{ij} + s_{ij})$. When $n = 2$, we have

$$\begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} + \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} = \begin{pmatrix} r_{11} + s_{11} & r_{12} + s_{12} \\ r_{21} + s_{21} & r_{22} + s_{22} \end{pmatrix}$$

The identity with respect to $+$ is the zero matrix; the matrix whose entries are 0.

Matrix multiplication: $(r_{ij}) \cdot (s_{ij}) = (\sum_{l=1}^{n} r_{il} s_{lj})$. When $n = 2$, we have

$$\begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} \cdot \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} = \begin{pmatrix} r_{11}s_{11} + r_{12}s_{21} & r_{11}s_{12} + r_{12}s_{22} \\ r_{21}s_{11} + r_{22}s_{21} & r_{21}s_{12} + r_{22}s_{22} \end{pmatrix}.$$

Identity (or unity):

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

6. Let $(R, +, \cdot)$ be a ring. Then $M_n(R)$ is a ring with the matrix addition and multiplication. If e is the identity of R then $M_n(R)$ has the identity

$$\begin{pmatrix} e & 0 & \cdots & 0 \\ 0 & e & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e \end{pmatrix}.$$

For an integer $n \in \mathbb{Z}$ and $r \in R$, an element of a ring R, define $na = a + a + \cdots + a$, a added n times, if n is positive. If $n = 0$ then define $na = 0$ and if n is negative, define $na = -a + (-a) + \cdots + (-a)$, that is $(-a)$ added n times.

Proposition 2.1. *Let $(R, +, \cdot)$ be any ring. Then*

(1) $0 \cdot a = a \cdot 0$ *for all* $a \in R$
(2) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$ *for all* $a, b \in R$.
(3) $n(a \cdot b) = (na) \cdot b = a \cdot (nb)$ *for all* $a, b \in R$ *and* $n \in \mathbb{Z}$.
(4) $(mn)a = m(na) = n(ma)$ *for all* $m, n \in \mathbb{Z}$ *and* $a \in R$.

Proof. Let $a, b \in R$. Observe that $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Thus $0 \cdot a = 0$. Likewise, one shows that $a \cdot 0 = 0$. Since $0 = (a + (-a))$, we have $0 = 0 \cdot b = (a + (-a)) \cdot b$. This shows that $a \cdot b + (-a) \cdot b = 0$, whence $-(a \cdot b) = (-a) \cdot b$. A similar agrument proves that $-(a \cdot b) = a \cdot (-b)$. Using distributive laws R3 and R4 and an induction on n, one can show that $n(a \cdot b) = (na) \cdot b = a \cdot (nb)$ and that $(mn)a = m(na) = n(ma)$ for all $m, n \in \mathbb{Z}$ and $a \in R$. ☐

Units of a ring: Let $(R, +, \cdot)$ be a ring with 1_R. An element $a \in R$ is called a *unit* if $a \cdot b = b \cdot a = 1_R$ for some $b \in R$. The set of all units of a ring R is denoted by $\mathcal{U}(R)$

Subring: Let $(R, +, \cdot)$ be a ring. A subset S of R is a *subring* of R if $(S, +)$ is a subgroup of $(R, +)$ and $(S, \cdot)$ is a subsemigroup of $(S, \cdot)$.

Center of a ring: Let $(R, +, \cdot)$ be a ring. The set $\mathcal{Z}(R) := \{x \in R \mid x \cdot r = r \cdot x \text{ for all } r \in R\}$ is called the *c*enter of the ring R. It can be easily seen that $\mathcal{Z}(R)$ is a subring of R.

Zero divisors: Let $(R, +, \cdot)$ be a ring. An element $a \in R$ is called a *left zero-divisor* if there is an element $0 \neq b \in R$ such that $a \cdot b = 0$. Similarly, one defines *right zero-divisors*.

In any ring with two elements, 0 is a zero-divisor, called the trivial zero-divisor.

Integral domain: A ring $(R, +, \cdot)$ is called an integral domain if there are no nontrivial zero divisors. In this course, an integral domain is neither required to be a commutative ring nor must have unity.

Examples:

(1) $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Q}, +, \cdot)$, which in turn is a subring of $(\mathbb{R}, +, \cdot)$.

(2) $\mathcal{U}(R)$ of $R = M_2(\mathbb{Q})$ is the set $GL_2(\mathbb{Q})$of all invertible matrices of $M_2(\mathbb{Q})$.

(3) $M_n(F)$, where $F = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is not an integral domain:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ is a left zero-divisor.

(4) Consider the ring $R := M_2(\mathbb{Q})$ with the matrix addition and multiplication. Then

$$\mathcal{Z}(R) = \left\{ \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix} \,\middle|\, a \in \mathbb{Q} \right\}.$$

The matrix of the above form are called *scalar* matrices.

Division Ring: A ring $(R, +, \cdot)$ with identity is said to be a *division ring* if $\mathcal{U}(R) = R \setminus \{0\}$. That is, $R \setminus \{0\}$ is a group under the $\cdot$ operation.

Field: A commutative division ring is called a *field*.

Examples:

(1) $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ under usual addition and multiplication forms a field.

(2) The set

$$\mathcal{Q} := \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\},$$

where $\bar{u}$ is the complex conjugate of u, is a division ring under matrix multiplication. But $\mathcal{Q}$ is not a field (why?).