MTH302: INTEGERS, POLYNOMIALS AND MATRICES
LECTURE 2

VARADHARAJ R. SRINIVASAN

Keywords: Matrix rings, polynomial rings, power series rings, ring of Gaussian integers, ring of integers modulo n.

1. MATRIX RINGS.

Let R be a ring. For any matrix $A = (a_{ij}) \in M_n(R)$ and $r \in R$, we denote the matrix $(r \cdot a_{ij})$ by rA. Let $r \in R$. The matrix $A = (a_{st}) \in M_n(R)$ such that $a_{ij} = r$ for a fixed i, j and $a_{st} = 0$ when $s \neq i$ or $t \neq j$ will be denoted by rE_{ij}. When R has 1, the matrix $1E_{ij}$ will be simply denoted by E_{ij}. Note that

$$aE_{ij} \cdot bE_{st} = \begin{cases} (a \cdot b)E_{it} & \text{if } j = s \\ 0 & \text{otherwise.} \end{cases}$$

Notation for the identity matrix: If R is a ring with 1 then the identity matrix of $M_n(R)$ will be denoted by I_n.

Remark 1.1. Given a ring R, every element of $A = (a_{ij}) \in M_n(R)$ can be uniquely written as

$$A = \sum_{i=1,j=1}^{n} a_{ij} E_{ij}.$$

Transpose of a matrix: Given a matrix $A = (a_{ij}) \in M_n(R)$, the transpose of A, sometimes denoted by A^T, is the matrix (a_{ji}).

Adjoint of a matrix: Let $A = (a_{ij}) \in M_n(R)$. The $ij-$th cofactor of A, denoted by c_{ij}, is the product of $(-1)^{i+j}$ and the determinant of the submatrix of A obtained by deleting the $i-$th row and $j-$th column. The transpose of the cofactor matrix (c_{ij}) is called the *adjoint* of A, denoted by $Adj(A)$.

Proposition 1.2. *If R is a commutative ring with 1 then $A \in M_n(R)$ is a unit if and only if $det(A)$ is a unit in R.*

Proof. Let $A \in M_n(R)$ be a unit. Then there is a matrix $B \in M_n(R)$ such that $A \cdot B = I_n = B \cdot A$. Applying determinant, we obtain $det(A) \cdot det(B) = 1 = det(B) \cdot det(A)$. Thus $det(A) \in R$ is a unit. Conversely, we know that $A \cdot Adj(A) = Adj(A) \cdot A = det(A)I_n$ (why?). Since $det(A)$ is a unit in R, we have an element $det(A)^{-1} \in R$ such that $det(A) \cdot det(A)^{-1} = det(A)^{-1} \cdot det(A) = 1$. Thus

$$A \cdot (det(A)^{-1} Adj(A)) = (det(A)^{-1} Adj(A)) \cdot A = I_n. \quad (why?)$$

Hence A is a unit in $M_n(R)$. (Where did we use that R is commutative?) □

2. Polynomial and Power Series Rings

Let $\mathbb{W} := \{0, 1, 2, \cdots\}$ and R be a ring. Let $R^{\mathbb{W}}$ be the set of all functions from $\mathbb{W}$ to R. Define addition and multiplication on $R^{\mathbb{W}}$ as follows:

Addition: $(f+g)(n) = f(n) + g(n)$ for all $n \in \mathbb{W}$
Multiplication: $(f \cdot g)(n) = \sum_{i=0}^{n} f(i) \cdot g(n-i)$ for all $n \in \mathbb{W}$.

Under these operation $R^{\mathbb{W}}$ forms a ring. If $f \in R^{\mathbb{W}}$ then f defines a sequence of images $f(0), f(1), \cdots$ in R. Conversely, if $a_0, a_1, \cdots$ is a sequence in R then f defined by $f(n) := a_n$ defines a function from $\mathbb{W}$ to R. In this sense, f is often denoted by its image and written as a formal expression in a variable X as

$$a_0 + a_1 X + a_2 X^2 + \cdots$$

Henceforth, we identify $R^{\mathbb{W}}$ with $R[[X]] := \{a_0 + a_1 X + \cdots \mid a_n \in R\}$; $f \mapsto f(0) + f(1)X + \cdots$ and call $R[[X]]$, the formal power series ring in one variable X over R. The elements of $R[[X]]$ are called formal power series. Under this identification, we have

$$\begin{aligned}
&\sum_{n=1} a_n X^n + \sum_{n=1} b_n X^n := \sum_{n=1} (a_n + b_n) X^n \\
&\left(\sum_{n=1} a_n X^n\right) \cdot \left(\sum_{n=1} b_n X^n\right) := \sum_{n=1} c_n X^n, \quad \text{where} \\
&c_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + \cdots + a_{n-1} \cdot b_1 + a_n \cdot b_0.
\end{aligned}$$

Note that two power series $f = a_0 + a_1 X + \cdots$ and $g = b_0 + b_1 X + \cdots$ are equal in $R[[X]]$ if and only if $f(n) = a_n = b_n = g(n)$ for all $n \in \mathbb{W}$.

Let $R_0^{\mathbb{W}} := \{f \in R^{\mathbb{W}} \mid f(n) = 0 \text{ for all but finitely many } n\}$. Then $R_0^{\mathbb{W}}$ can be easily seen to be a subring of $R^{\mathbb{W}}$. The restriction of the identification $f \mapsto f(0) + f(1)X + \cdots$ to the ring $R_0^{\mathbb{W}}$ has its image as the set

$$R[X] := \{a_0 + a_1 X + \cdots \mid a_n \in R, a_n = 0 \text{ for all but finitely many } n.\}$$

The ring $R[X]$ will be called the *ring of polynomials* in one variable X over R. The elements of $R[X]$ are called polynomials.

If $f = a_0 + a_1 X + \cdots$ is a polynomial such that $a_m = 0$ for all $m > n$ and $a_n \neq 0$ then we shall write $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$. In this case, n is called the *degree* of f and a_n is called the *leading coefficient* of f.

Proposition 2.1. *Let R be an integral domain with 1.*

(1) A polynomial $f = a_0 + a_1 X + \cdots + a_n X^n$ of degree n is a unit in $R[X]$ if and only if a_0 is a unit in R and $n = 0$.
(2) A power series $f = a_0 + a_1 X + \cdots$ is a unit in $R[[X]]$ if and only if a_0 is a unit in R.

Proof. Let $f = a_0 + a_1X + \cdots + a_nX^n$, a polynomial of degree n, be a unit in $R[X]$ and $g = b_0 + b_1X + \cdots + b_mX^m \in R[X]$, a polynomial of degree m, be the inverse of f. Then we have

$$f \cdot g = a_0 \cdot b_0 + (a_1 \cdot b_0 + a_0 \cdot b_1)X + \cdots + a_n \cdot b_m X^{n+m} = 1 + 0X + \cdots + 0X^{n+m}$$
$$g \cdot f = b_0 \cdot a_0 + (b_1 \cdot a_0 + b_0 \cdot a_1)X + \cdots + b_m \cdot a_n X^{n+m} = 1 + 0X + \cdots + 0X^{n+m}$$

Then, $a_0 \cdot b_0 = 1 = b_0 \cdot a_0$. If $n \geq 1$ then since $a_n \cdot b_m = 0$, $a_n \neq 0$ and $b_m \neq 0$, we obtain that R is not an integral domain. Thus $n = 1$. Converse is obvious!

If $g = b_0 + b_1X + \cdots$ is an inverse of a power series $f = a_0 + a_1X + \cdots$ then it is obvious that $a_0 \cdot b_0 = b_0 \cdot a_0 = 1$. Now let $f = a_0 + a_1X + \cdots$ be a power series and a_0 be a unit. One can easily find a power series $g = b_0 + b_1X + \cdots \in R[[X]]$, whose coefficients are determined in a recursive fashion using the relations $f \cdot g = g \cdot f = 1 + 0X + \cdots$ and the fact that $a_0b_0 = b_0a_0 = 1$. □

3. Integers modulo n

Let $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ be the collection of all equivalence classes $\overline{m}$ of integers under the equivalence relation

$$a \sim_n b \quad \text{if } a - b \text{ is divisible by } n.$$

Then $\mathbb{Z}_n$ forms a commutative ring under the following operations[1]

Addition: $\overline{i} + \overline{j} = \overline{i + j}$,
Multiplication: $\overline{i} \cdot \overline{j} = \overline{ij}$.

For $n \geq 2$, $\mathbb{Z}_n$ is a commutative ring with identity $\overline{1}$. It can be easily seen that $\mathbb{Z}_n = \{\overline{0}\}$ if and only if $n = 1$. Therefore, in the foregoing, we shall assume $n \geq 2$.

Proposition 3.1. *$\overline{x} \in \mathbb{Z}_n$ is a unit if and only if $\overline{x}$ is not a zero-divisor if and only if x is coprime to n*

Proof. If $\overline{x}$ is a unit then it is clear that $\overline{x}$ is not a zero divisor (why?). Conversely, if $\overline{x}$ is not a zero divisor then $\overline{y} \mapsto \overline{xy}$ is an injective map on the finite set $\mathbb{Z}_n$. Therefore it is surjective. Thus we obtain an element $y \in \mathbb{Z}$ such that $\overline{x} \cdot \overline{y} = \overline{1}$. Similarly, the map $\overline{x} \mapsto \overline{yx}$ is also bijective and we obtain an element $z \in \mathbb{Z}$ such that $\overline{z} \cdot \overline{x} = \overline{1}$. It follows that $\overline{y} = \overline{z}$ and thus $\overline{x}$ is a unit.

If $\overline{x}$ is a unit then there is a $y \in \mathbb{Z}$ such that $xy - 1$ is divisibe by n. That is $xy + zn = 1$ for some $z \in \mathbb{Z}$. This implies that x and y are coprime. A similar argument proves the converse. □

Proposition 3.2. *$\mathbb{Z}_n$ is an integral domain if and only if n is prime if and only if $\mathbb{Z}_n$ is a field.*

Proof. From the previous proposition, it is evident that $\mathbb{Z}_n$ is an integral domain if and only if $\mathbb{Z}_n$ is a field. Observe that $n = lm$ for $2 \leq l \leq n - 1$ and $2 \leq m \leq n - 1$ if and only if $\overline{l}\overline{m} = \overline{n} = \overline{0}$. This completes the proof of the propostion. □

[1] I expect you to check that the operations are indeed well-defined and that $\mathbb{Z}_n$ forms a ring.