MATH 171: WORKSHEET R3

DAGAN KARP

ABSTRACT. We study examples of rings: polynomials, matrices and group rings.

1. POLYNOMIAL RINGS (AFTER P. GRILLET)

Intuitively, a polynomial in one indeterminate x and coefcients in a ring R is a linear combination

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

of powers of x with coefficients $a_0, \ldots, a_n \in R$.

But what is x? What is a *variable* or an *indeterminate*? Note that x acts as a place holder, and that the polynomial is determined by its coefficients!

Definition 1. *A* polynomial *with one indeterminate and coefcients in a ring* R *is an infinite sequence*

$$a = (a_0, a_1, a_2, \ldots, a_n, \ldots)$$

of elements of R *such that* $a_n = 0$ *for almost all* n*.*

Remark 2. To say that $a_n = 0$ for almost all n is to say that there are only a finite number of n such that $a_n \neq 0$. In other words, the set

$$\{n \in \mathbb{N} \cup \{0\} : a_n \neq 0\}$$

is finite. Or, equivalently, there exists some $N > 0$ such that $a_i = 0$ for all $i > N$.

We may define addition of polynomials componentwise,

$$(a_0, a_1, \ldots, a_n, \ldots) + (b_0, b_1, \ldots, b_n, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$$

In other words,

$$a + b = c$$

where $c_i = a_i + b_i$.

Multiplication is defined by

$$ab = c$$

where c is given by

$$c_n = \sum_{i+j=n} a_i b_j.$$

Proposition 3. *When* R *is a ring, polynomials with one indeterminate and coefficients in* R *form a ring, denoted* $R[x]$*. If* R *is commutative, then* $R[x]$ *is commutative.*

Definition 4. *The* indeterminate x *in* $R[x]$ *is defined by*

$$x = (0, 1, 0, 0, \dots, 0, \dots).$$

Now that x is defined, we can write polynomials in familiar form

$$(a_0, a_1, a_2, \dots, a_n, \dots) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

Definition 5. *The* degree *of a non-zero polynomial* $a(x) \in R[x]$ *is the largest* n *such that* $a_n \neq 0$. *Then* a_n *is called the* leading coefficient *of* a *and the term* $a_n x^n$ *is called the* leading term *of* a.

Proposition 6. *Let* R *be an integral domain, and let* $a(x)$ *and* $b(x)$ *be two non-zero polynomials in* $R[x]$.

(1) $\deg(ab) = \deg(a) + \deg(b)$
(2) *The units of* $R[x]$ *are the units of* R.
(3) $R[x]$ *is an integral domain.*

2. Matrix Rings

Definition 7. *For a ring* R *and* $n \in \mathbb{N}$, *let* $M_n(R)$ *denote the set of all* $n \times n$ *matrices with entries in* R. *For a matrix* A *in* $M_n R$, *we denote by* $A_{i,j}$ *the entry of* A *in row* i *and column* j.

Addition of matrices is defined by

$$A + B = C,$$

where

$$C_{i.j} = A_{i,j} + B_{i,j}.$$

Multiplication is the standard matrix multiplication:

$$(AB)_{i,j} = \sum_{k=1}^{n} A_{i,k} B_{k,j}.$$

Definition 8. *The units of* $M_n(R)$ *are called* the general linear group, *which is denoted*

$$GL_n(R) = \{A \in M_n(R) : A \text{ is invertible}\}$$

Definition 9. *Let* R *be a commutative ring with identity.*

(1) *The* special linear group, $SL_n(R)$, *is the subgroup of* $GL_n(R)$ *consisting of matrices with determinant* 1.
(2) *The* orthogonal group, $O_n(R)$, *is the subgroup of* $GL_n(R)$ *consisting of orthogonal matrices, i.e. those matrices* A *such that* $AA^t = I$, *where* A^t *is the transpose of* A, *and* I *is the identity matrix.*
(3) *The* unitary group, U_n, *is the subgroup of* $GL_n(\mathbb{C})$ *of matrices such that* $AA^* = I$, *where* A^* *is the transpose conjugate of* A.
(4) *The* symplectic group Sp_n *is the subgroup of* $GL_n(\mathbb{H})$ *such that* $AA^* = I$, *where* A^* *is the quaternionic complex conjugate of* A.

3. Group Rings

Definition 10. *Let* R *be a commutative ring with identity and let* G *be a finite group*

$$G = \{g_1, \dots g_n\}.$$

The group ring RG *of* G *with coefficients in* R *is the set of all formal sums*

$$RG = \{a_1 g_1 + \cdots a_n g_n : a_i \in R,\ g_i \in G\}.$$

If e is the identity in G and $a \in R$, we define

$$a \cdot e = a \in RG.$$

Similarly, for the identity $1 \in R$ and $g \in G$ we define

$$1 \cdot g = g \in RG.$$

Addition is defined componentwise

$$(a_1 g_1 + \cdots + a_n g_n) + (b_1 g_1 + \cdots + b_n g_n) = ((a_1 + b_1)g_1 + \cdots + (a_n + b_n)g_n).$$

Multiplication is defined by

$$(a g_i) \cdot (b g_j) = (ab)(g_i g_j),$$

with the additional requirement that the distributive law holds.

4. Exercises

4.1. **Exercise.** Prove Proposition 3.

4.2. **Exercise.** Calculate x^2 in $R[x]$, using the definition of the indeterminate x above and our knowledge of multiplication in $R[x]$. In general, what is x^n?

4.3. **Exercise.** Prove proposition 6.

4.4. **Exercise.** Let R be any ring and $n \geqslant 2$. Show that $M_n(R)$ is not commutative by considering the following example. Let $a, b \in R$ be such that $ab \neq 0$ and let

$$A = \begin{pmatrix} a & 0 & \\ 0 & 0 & \\ & & \ddots \end{pmatrix} \qquad B = \begin{pmatrix} 0 & b & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \ddots \end{pmatrix}$$

Compare AB and BA.

4.5. **Exercise.** Show that RG has zero divisors for any non-trivial group G by considering the product

$$(1 - g)(1 + g + g^2 + \cdots + g^{m-1}),$$

where $g \in G$ is an element of order m.

4.6. **Exercise.** Show that $\mathbb{R}Q$ is not the same ring as $\mathbb{H}$, where Q is the quaternion group and $\mathbb{H}$ are is the quaternion ring, i.e.

$$Q = \{\pm 1, \pm i, \pm j, \pm k \mid i^2 = j^2 = k^2 = -1, ij = k, ji = -k, \text{ etc}\}$$
$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R},\ i, j, k \in Q\}.$$