Matrix Rings

One of the rings studied last week was $R = \mathbb{Z} + \mathbb{Z} \cdot \sqrt{5}$. The idea behind this construction can be replicated with any commutative ring R in place of $\mathbb{Z}$ and any element r of R in place of 5 as follows.

We take S to be the collection of pairs (a, b) of elements of R and define addition and multiplication as follows:

$$(a, b) + (a', b') = (a + a', b + b') \text{ and } (a, b) \cdot (a', b') = (a \cdot a' + b \cdot b' \cdot r, a \cdot b' + a' \cdot b)$$

As a specific example, we can consider the Gaussian integers $\mathbb{Z}[i]$ which is the ring consisting of complex numbers of the form $a + b \cdot i$ where a and b are integers; recall that $i^2 = -1$.

Instead of writing the formulas above it is easier to write:

- addition is component-wise
- $(1, 0)$ is the multiplicative identity and $(0, 1)^2 = r$.

Exercise: Show that the formula for multiplication follows from the above two rules and the distributive and associative laws.

A different example is to consider the case where the element $r = 0$. In this case we can think of the elements as $a + b \cdot \epsilon$ where $\epsilon = (0, 1)$. Then $\epsilon^2 = 0$. As you can imagine this plays an important role in the algebraic approach to calculus!

So far, we have only constructed commutative rings. However, we have another example of "quaternions". Given two elements r and s of the ring R, we can create a new ring out of 4-tuples (a_0, a_1, a_2, a_3) of elements of R. Addition of two such 4-tuples is component-wise as above. For multiplication we have the rules:

$$(0, 1, 0, 0)^2 = r; (0, 0, 1, 0)^2 = s; (0, 1, 0, 0) \cdot (0, 0, 1, 0) = (0, 0, 0, 1) = -(0, 0, 1, 0) \cdot (0, 1, 0, 0)$$

The last rule makes multiplication non-commutative.

Exercise: Using the associative law show that $(0, 0, 0, 1)^2 = -r \cdot s$.

Quaternions were first discovered classically by Hamilton in the special case when $R = \mathbb{R}$ is the ring of real numbers and $r = s = -1$ while tring to find a way to parametrize 3-dimensional rotations in a way similar to the use of unit complex numbers to parametrise 2-dimensional rotations. Hamilton's quaternions can also be understood as follows.

Consider the ring $\mathbb{H}$ ('H' for Hamilton) consisting of pairs $(a, \vec{v})$ where a is a real number and $\vec{v}$ is a vector in 3-dimensional space. Addition is carried out component-wise and multiplication is defined as follows:

$$(a, \vec{v}) \cdot (b, \vec{w}) = (ab - \vec{v} \cdot \vec{w}, \vec{v} \times \vec{w})$$

Here $\vec{v} \cdot \vec{w}$ denotes the usual "dot-product" of the vectors and $\vec{v} \times \vec{w}$ denotes the "cross-product" of the vectors.

Exercise: Check that $\mathbb{H}$ is a ring under these operations.

Exercise: Check that the two ways of constructing $\mathbb{H}$ result in the same ring via a natural correspondence.

The above rings appear to be constructed as follows. We take the ring S to consist of n-tuples of elements of R and define the operations via the rules:

- addition is defined component-wise.
- for the tuples $e_i = (0, \ldots, 1, \ldots, 0)$ (where 1 is in the i-th place) we define mutliplications $e_i \cdot e_j$ as linear combinations (using elements $c_{i,j,k}$ in R):

$$e_i \cdot e_j = \sum_{k=1}^{n} c_{i,j,k} e_k$$

Do all such definitions give a ring? No.

Exercise: (Starred) Check that the associative law for multiplication requires some identities to hold in R for the elements $c_{i,j,k}$.

Rather than check such identities each time, it is easier to see these examples as special cases of "matrices" as we shall do below. In that case, the associative law needs to be checked just once!

Matrices over a ring

Given positive integers p and q, a $p \times q$ matrix A over R consists of pq elements of R placed in a grid with p rows and q columns. The element of R in the i-th row and j-th column is denoted by $A_{i,j}$. We will study $p \times q$ matrices over R for various values of p and q and various rings R.

We define addition of matrices component-wise; so we can only add matrices when they are of the *same* $p \times q$-type over the *same* ring R.

We can multiply a $p \times q$ matrix A by a $q \times r$ matrix B on the *right* to obtain a $p \times r$ matrix C where:

$$C_{i,j} = \sum_{k=1}^{q} A_{i,k} \cdot B_{k,j}$$

where all the entries are in R and, the multiplication and addition on the right-hand-side are in R.

Exercise: Check that this multiplication is left and right distribution.

Exercise: Check that this multiplication is associative. Note that this does not require R to be commutative!

Exercise: (Starred) Why do we define matrix multiplication in *this particular way*?

To make a ring out of a collection of matrices, we should be able to add them and multiply them to obtain objects of the same type. This can only be achieved if all the matrices are of the same $p \times p$ type. For each positive integer p, the collection $M_p(R)$ of $p \times p$ matrices forms a ring.

Various rings we have studied earlier can be thought of as subrings of the ring of matrices.

Exercise: Given a commutative ring R and an element r of R show that matrices of the form:

$$\begin{pmatrix} a & b \cdot r \\ b & a \end{pmatrix}$$

are closed under addition and mutliplication; here a and b denote elements of R.

Exercise: Show that the above collection of matrices is the same as the ring S constructed earlier (via a natural correspondence).

In particular, we can think of the ring of complex numbers as the collection of matrices of the form $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ where a and b are real numbers.

Similarly, given a commutative ring R and elements r and s in R we can think of the quaternions as made up of 4×4 matrices of the form:

$$\begin{pmatrix} a & b \cdot r & c \cdot s & -d \cdot (r \cdot s) \\ b & a & -d \cdot s & c \cdot s \\ c & d \cdot r & a & -b \cdot r \\ d & c & -b & a \end{pmatrix}$$

Here a, b, c and d denote elements of R.

Exercise: Check that the above collection of matrices is closed under addition and multiplication.

Exercise: (Starred) Check that the above collection of matrices is the same as the quaternions defined earlier.

The above 4×4 matrix has a peculiar structure. In the special case of $\mathbb{H}$ we note that the matrix takes the form:

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$

We recognise that this is made up of 2×2 blocks that can be thought of as complex numbers (as above) so that the matrix becomes

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}$$

where u and v are complex numbers, and for a complex number w, the symbol $\overline{w}$ denotes its complex conjugate. The above representation of Hamilton's quaternions in terms of 2×2 matrices over complex numbers was (re-)discovered by Wolfgang Pauli and is sometimes called the Pauli representation in his honour.

Exercise: Check that 2×2 matrices of the above type with entries in the field of complex numbers is closed under addition and multiplication.

Most of the constructions of new rings from old which are "finite" in some sense are built out of the above construction. We will later look at "free" constructions. Such constructions can be clarified by a peek into category theory.

A brief introduction to category theory

The following dicussion is a useful way to understand the matrix construction from a slightly more advanced viewpoint. It is explained here *merely* to give a sense of perspective. Just as learing set theory is not essential to understanding basic mathematics (but it makes some things clearer), learning category theory is *not essential* to understanding mathematics at this level, but it *will* make some things clearer.

At the first level of mathematics, we introduce mathematical objects like numbers in arithmetic and figures in geometry. At the second level, we look at "composite" mathematical objects such as the ring of integers, the permutation group on n symbols and so on. At the third level, we study mathematical objects by studying their relations to each other. Many of the topics you study in your Mathematics majors courses will involve a type of mathematical object and transformations between objects of the same type. This is called a category of mathematical objects:

- The category of rings has objects as rings and morphisms as ring homomorphisms.
- The category of groups has objects as groups and morphisms as group homomorphisms.
- The category of topological spaces has objects as topological spaces and morphisms as continuous maps between topological spaces.
- The category of sets has objects as sets and morphisms as set maps.

In each case, the following properties hold:

- Every object X has an *identity* morphism 1_X to itself.
- Morphisms $f : X \to Y$ and $g : Y \to Z$ can be composed to give a morphism $g \circ f : X \to Z$.
- This composition is associative, so $h \circ (g \circ f) = (h \circ g) \circ f$.
- The identity morphism is an identity for composition $1_Y \circ f = f = f \circ 1_X$.

An important reason to introduce this is to bring up the notion of a *functor*. A functor F from a category $\mathcal{A}$ to a category $\mathcal{B}$ is:

- a way to assign to an object X of $\mathcal{A}$ an object $F(X)$ of $\mathcal{B}$.
- a way to assign to a morphism $f : X \to Y$ of $\mathcal{A}$ a morphism $F(f) : F(X) \to F(Y)$ of $\mathcal{B}$.

We also require the following conditions:

$$F(1_X) = 1_{F(X)} \text{ and } F(g \circ f) = F(g) \circ F(f)$$

Our study of matrices gives us the first example of an interesting functor from the category of rings to itself. For each positive integer p, the functor M_p assigns to a ring R the ring $M_p(R)$ of $p \times p$ matrices over R.