TWO NONCOMMUTATIVE RINGS

The Ring of Quaternions. This ring was invented by the Irish mathematician William Hamilton in the 1840s. It is often denoted by $\mathbb{H}$. The elements of $\mathbb{H}$ are called *"quaternions."*. As a set, $\mathbb{H}$ consists of expressions of the form $a + bi + cj + dk$, where a, b, c, and d are arbitrary real numbers. Consider two elements α and β in $\mathbb{H}$. Thus, we can write

$$\alpha \ = \ a + bi + cj + dk \ , \qquad \beta \ = \ a' + b'i + c'j + d'k \ \ ,$$

where $a,\ b,\ c,\ d,\ a',\ b',\ c',\ d'$ are real numbers. We define addition and multiplication by the following formulas:

$$\alpha \ + \ \beta \ = \ (a+a') \ + \ (b+b')i \ + \ (c+c')j \ + \ (d+d')k \quad .$$

and

$$\alpha \cdot \beta \ = \ A \ + \ Bi \ + \ Cj \ + \ Dk \ \ ,$$

where A, B, C, and D are the real numbers given by

$$A \ = \ aa' - bb' - cc' - dd' \ , \qquad B \ = \ ab' + ba' + cd' - dc' \ ,$$

$$C \ = \ ac' - bd' + ca' + db' \ , \qquad D \ = \ ad' + bc' - cb' + da' \quad .$$

The structure of the underlying additive group of $\mathbb{H}$. the additive group of $\mathbb{H}$ is isomorphic to the additive group of $\mathbb{R}^4$. Note that $\mathbb{R}^4$ consists of all 4-tuples (a, b, c, d), where a, b, c, and d are real numbers. Addition is component-wise. The group $\mathbb{R}^4$ is the direct product $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. The isomorphism is the function $a + bi + cj + dk \mapsto (a, b, c, d)$.

Multiplication in $\mathbb{H}$. It is not necessary to remember the above definition of multiplication. It is derived by using the distributive law many times, giving sixteen terms altogether. One can identify the ring of real numbers $\mathbb{R}$ with the following subring of $\mathbb{H}$:

$$\mathbb{R} \ = \ \{ \ a + 0i + 0j + 0k \mid a \in \mathbb{R} \ \}$$

One has an isomorphism from $\mathbb{R}$ to that subring defined by $a \mapsto a + 0i + 0j + 0k$. Thus, we can think of $\mathbb{R}$ as a subring of $\mathbb{H}$. The additive identity $0_{\mathbb{H}}$ of $\mathbb{H}$ is $0 + 0i + 0j + 0k$, which is now identified with the real number 0. The multiplicative identity $1_{\mathbb{H}}$ is $1 + 0i + 0j + 0k$, which is now identified with the real number 1. The definition of multiplication in $\mathbb{H}$ is based on the following ingredients.

1. Elements of $\mathbb{R}$ are in the center of $\mathbb{H}$.
2. $i^2 \ = \ -1, \qquad j^2 \ = \ -1, \qquad k^2 \ = \ -1 \ .$
3. $ij \ = \ k, \qquad jk \ = \ i, \qquad ki = j \qquad ji \ = \ -k, \qquad kj \ = \ -i, \qquad ik = -j \ \ .$

The group of units of $\mathbb{H}$. Notice the following special case of multiplication:

$$\big(a+bi+cj+dk\big)\cdot\big(a+(-b)i+(-c)j+(-d)k\big) \;=\; (a^2+b^2+c^2+d^2)+0i+0j+0k \;\;,$$

which is an element of the subring $\mathbb{R}$ of $\mathbb{H}$. Let e denote the right side of the above equation. That is, e is the real number $a^2+b^2+c^2+d^2$. Notice that if $\alpha = a+bi+cj+dk$ and $\alpha \neq 0_{\mathbb{H}}$, then e is a positive real number, and hence is nonzero. We then obtain the equation

$$\big(a+bi+cj+dk\big)\big((a/e)+(-b/e)i+(-c/e)j+(-d/e)k\big) \;=\; 1$$

and therefore α is a unit of $\mathbb{H}$. That is, every nonzero element of $\mathbb{H}$ is a unit of $\mathbb{H}$. Therefore, $\mathbb{H}^\times = \mathbb{H} - \{0\}$.

The ring $\mathbb{H}$ is a noncommutative ring with identity such that $1_{\mathbb{H}} \neq 0_{\mathbb{H}}$ and such that $\mathbb{H}^\times = \mathbb{H} - \{0\}$. This means that $\mathbb{H}$ is a division ring, but $\mathbb{H}$ is not a field.

The ring of 2×2 matrices over $\mathbb{R}$. We denote this ring by $M_2(\mathbb{R})$. Its elements are 2×2 matrices with real entries. Addition and multiplication of matrices are defined in the usual ways, which are familiar from linear algebra. The underlying additive group of $M_2(\mathbb{R})$ is isomorphic to the additive group of $\mathbb{R}^4$. Thus, the additive groups of the rings $\mathbb{H}$ and $M_2(\mathbb{R})$ are isomorphic. As for multiplication, an alternative way to define that operation is as follows. We use the following notation:

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \;\;.$$

For any real numbers a, b, c, d, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \;=\; aE_{11} + bE_{12} + cE_{21} + dE_{22} \;\;.$$

Just as for $\mathbb{H}$, one can define the product $\alpha\beta$ of two matrices $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by using the distributive law many times, obtaining sixteen terms, and then using the following definitions. For $1 \le s,\; t,\; u,\; v \le 2$, define

$$E_{st}E_{uv} \;=\; \begin{cases} E_{sv} & \text{if } t = u \\[2ex] 0_{M_2(\mathbb{R})} & \text{if } t \neq u \end{cases}$$

One can identify $\mathbb{R}$ with a subring of $M_2(\mathbb{R})$ by the map $a \mapsto aE_{11} + aE_{22}$. Note that $aE_{11} + aE_{22} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, which is often referred to as a *"scalar matrix"*. With this identification, the ring $\mathbb{R}$ is a contained in the center of $M_2(\mathbb{R})$. The additive and multiplicative identity elements of $M_2(\mathbb{R})$ are $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, respectively.

The ring $M_2(\mathbb{R})$ is a noncommutative ring with identity, but is not a division ring. The group of units of $M_2(\mathbb{R})$ is usually denoted by $GL_2(\mathbb{R})$.