The Quaternions

We have not yet given an example of a noncommutative division ring. The *quaternions* of Hamilton are the standard example of a strictly skew field; let us describe them.

HISTORICAL NOTE

Sir William Rowan Hamilton (1805–1865) discovered quaternions in 1843 while he was searching for a way to multiply number triplets (vectors in $\mathbb{R}^3$). Six years earlier he had developed the complex numbers abstractly as pairs (a, b) of real numbers with addition $(a, b) + (a' + b') = (a + a', b + b')$ and multiplication $(a, b)(a'b') = (aa' - bb', ab' + a'b)$; he was then looking for an analogous multiplication for 3-vectors that was distributive and such that the length of the product vector was the product of the lengths of the factors. After many unsuccessful attempts to multiply vectors of the form $a + bi + cj$ (where 1, i, j are mutually perpendicular), he realized while walking along the Royal Canal in Dublin on October 16, 1843, that he needed a new "imaginary symbol" k to be perpendicular to the other three elements. He could not "resist the impulse ... to cut with a knife on a stone of Brougham Bridge" the fundamental defining formulas for multiplying these quaternions.

The quaternions were the first known example of a strictly skew field. Though many others were subsequently discovered, it was eventually noted that none were finite. In 1909 Joseph Henry Maclagan Wedderburn (1882–1948), then a preceptor at Princeton University, gave the first proof of Theorem 32.10.

Let the set $\mathbb{H}$, for Hamilton, be $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Now $\langle \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}, +\rangle$ is a group under addition by components, the direct product of $\mathbb{R}$ under addition with itself four times. This gives the operation of addition on $\mathbb{H}$. Let us rename certain elements of $\mathbb{H}$. We shall let

$$\begin{aligned} 1 &= (1, 0, 0, 0), \quad i = (0, 1, 0, 0), \\ j &= (0, 0, 1, 0), \quad \text{and} \quad k = (0, 0, 0, 1). \end{aligned}$$

We furthermore agree to let

$$\begin{aligned} a_1 &= (a_1, 0, 0, 0), \quad a_2 i = (0, a_2, 0, 0), \\ a_3 j &= (0, 0, a_3, 0) \quad \text{and} \quad a_4 k = (0, 0, 0, a_4). \end{aligned}$$

In view of our definition of addition, we then have

$$(a_1, a_2, a_3, a_4) = a_1 + a_2 i + a_3 j + a_4 k.$$

Thus

$$\begin{aligned} &(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) \\ &\quad = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k. \end{aligned}$$

We now give Hamilton's fundamental formulas for multiplication in $\mathbb{H}$, We start by defining

$$\begin{aligned} 1a = a1 = a \quad &\text{for} \quad a \in \mathbb{H}, \\ i^2 = j^2 = k^2 &= -1, \end{aligned}$$

and

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad \text{and} \quad ik = -j.$$

Note the similarity with the so-called cross product of vectors. These formulas are easy to remember if we think of the sequence

$$i, j, k, i, j, k.$$

The product from left to right of two adjacent elements is the next one to the right. The product from right to left of two adjacent elements is the negative of the next one to the left. We then define a product to be what it must be to make the distributive laws hold, namely,

$$\begin{aligned}
&(a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 i + b_3 j + b_4 k) \\
&\quad = (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) i \\
&\qquad + (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) j \\
&\qquad + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) k.
\end{aligned}$$

Exercise 19 shows that the quaternions are isomorphic to a subring of $M_2(\mathbb{C})$, so multiplication is associative. Since $ij = k$ and $ji = -k$, we see that multiplication is not commutative, so $\mathbb{H}$ is definitely not a field. Turning to the existence of multiplicative inverses, let $a = a_1 + a_2 i + a_3 j + a_4 k$, with not all $a_i = 0$. Computation shows that

$$(a_1 + a_2 i + a_3 j + a_4 k)(a_1 - a_2 i - a_3 j - a_4 k) = a_1{}^2 + a_2{}^2 + a_3{}^2 + a_4{}^2.$$

If we let

$$|a|^2 = a_1{}^2 + a_2{}^2 + a_3{}^2 + a_4{}^2 \qquad \text{and} \qquad \bar{a} = a_1 - a_2 i - a_3 j - a_4 k,$$

we see that

$$\frac{\bar{a}}{|a|^2} = \frac{a_1}{|a|^2} - \left(\frac{a_2}{|a|^2}\right) i - \left(\frac{a_3}{|a|^2}\right) j - \left(\frac{a_4}{|a|^2}\right) k$$

is a multiplicative inverse for a. We have demonstrated the following theorem.

32.9 Theorem The quaternions $\mathbb{H}$ form a strictly skew field under addition and multiplication. ♦

Note that $G = \{\pm 1, \pm i, \pm j, \pm k\}$ is a group of order 8 under quaternion multiplication. This group is generated by i and j, where

$$i^4 = 1, \qquad j^2 = i^2 \qquad \text{and} \qquad ji = i^3 j.$$

The group G is not cyclic. Recall that Corollary 28.7 states that if F is a field and H is a finite subgroup of the multiplicative group F^*, then H is cyclic. This example shows that Corollary 28.7 cannot be generalized to skew fields.

There are no finite strictly skew fields. This is the content of a famous theorem of Wedderburn, which we state without proof.

32.10 Theorem **(Wedderburn's Theorem)** Every finite division ring is a field.

Proof See Artin, Nesbitt, and Thrall [24] for a proof of Wedderburn's theorem. ◆

EXERCISES 32

Computations

In Exercises 1 through 3, let $G = \{e, a, b\}$ be a cyclic group of order 3 with identity element e. Write the element in the group algebra $\mathbb{Z}_5 G$ in the form

$$re + sa + tb \qquad \text{for} \qquad r, s, t \in \mathbb{Z}_5.$$

1. $(2e + 3a + 0b) + (4e + 2a + 3b)$ **2.** $(2e + 3a + 0b)(4e + 2a + 3b)$ **3.** $(3e + 3a + 3b)^4$

In Exercises 4 through 7, write the element of $\mathbb{H}$ in the form $a_1 + a_2 i + a_3 j + a_4 k$ for $a_i \in \mathbb{R}$.

4. $(i + 3j)(4 + 2j - k)$ **5.** $i^2 j^3 kji^5$

6. $(i + j)^{-1}$ **7.** $[(1 + 3i)(4j + 3k)]^{-1}$

8. Referring to the dihedral group $D_3 = \{\iota, \rho, \rho^2, \mu, \mu\rho, \mu\rho^2\}$ as defined in Section 4, compute the product

$$(0\iota + 1\rho + 0(\rho^2) + 0\mu + 1(\mu\rho) + 1(\mu\rho^2))(1\iota + 1\rho + 0(\rho^2) + 1\mu + 0(\mu\rho) + 1(\mu\rho^2))$$

in the group ring $\mathbb{Z}_2 D_3$.

9. Find the center of the group $\langle \mathbb{H}^*, \cdot \rangle$, where $\mathbb{H}^*$ is the set of nonzero quaternions.

Concepts

10. Find two subsets of $\mathbb{H}$ different from $\mathbb{C}$ and from each other, each of which is a field isomorphic to $\mathbb{C}$ under the induced addition and multiplication from $\mathbb{H}$.

11. Determine whether each of the following is true or false.

a. $M_n(F)$ has no divisors of 0 for any n and any field F.
b. Every nonzero element of $M_2(\mathbb{Z}_2)$ is a unit.
c. End(A) is always a ring with unity $\neq 0$ for every abelian group A.
d. End(A) is never a ring with unity $\neq 0$ for any abelian group A.
e. The subset Iso(A) of End(A), consisting of the isomorphisms of A onto A, forms a subring of End(A) for every abelian group A.
f. $R\langle \mathbb{Z}, + \rangle$ is isomorphic to $\langle Z, +, \cdot \rangle$ for every commutative ring R with unity.
g. The group ring RG of an abelian group G is a commutative ring for any commutative ring R with unity.
h. The quaternions are a field.
i. $\langle \mathbb{H}^*, \cdot \rangle$ is a group where $\mathbb{H}^*$ is the set of nonzero quaternions.
j. No subring of $\mathbb{H}$ is a field.

12. Show each of the following by giving an example.

a. A polynomial of degree n with coefficients in a strictly skew field may have more than n zeros in the skew field.
b. A finite multiplicative subgroup of a strictly skew field need not be cyclic.

Theory

13. Let ϕ be the element of End($\langle \mathbb{Z} \times \mathbb{Z}, + \rangle$) given in Example 32.2. That example showed that ϕ is a right divisor of 0. Show that ϕ is also a left divisor of 0.

14. Show that $M_2(F)$ has at least six units for every field F. Exhibit these units. [Hint: F has at least two elements, 0 and 1.]

15. Show that End ($\langle \mathbb{Z}, + \rangle$) is naturally isomorphic to $\langle \mathbb{Z}, +, \cdot \rangle$ and that End($\langle \mathbb{Z}_n, + \rangle$) is naturally isomorphic to $\langle \mathbb{Z}_n, +, \cdot \rangle$.

16. Show that End($\langle \mathbb{Z}_2 \times \mathbb{Z}_2, + \rangle$) is not isomorphic to $\langle \mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot \rangle$.

17. Referring to Example 32.3, show that $YX - XY = 1$.

18. If $G = \{e\}$, the group of one element, show that RG is isomorphic to R for any ring R.

19. There exists a matrix $K \in M_2(\mathbb{C})$ such that $\phi : \mathbb{H} \to M_2(\mathbb{C})$ defined by

$$\phi(a + bi + cj + dk) = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + c\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} + dK,$$

for all $a, b, c, d \in \mathbb{R}$, gives an isomorphism of $\mathbb{H}$ with $\phi[\mathbb{H}]$.

a. Find the matrix K.

b. What 8 equations should you check to see that ϕ really is a homomorphism?

c. What other thing should you check to show that ϕ gives an isomorphism of $\mathbb{H}$ with $\phi[\mathbb{H}]$?

20. Let R be a ring with unity, let $a \in R$, and let $\lambda_a : R \to R$ be given by

$$\lambda_a(x) = ax$$

for $x \in R$.

a. Show that λ_a is an endomorphism of $\langle R, +\rangle$.

b. Show that $R' = \{\lambda_a \mid a \in R\}$ is a subring of $\text{End}(\langle R, +\rangle)$.

c. Prove the analogue of Cayley's theorem for R by showing that R' of (b) is isomorphic to R.