11. Show that the rings $M_{nm}(R)$ and $M_n(M_m(R))$ are isomorphic (*Hint:* Use "block" addition and multiplication of matrices.)

12. Show that if R is a field, $A \in M_n(R)$ is a zero divisor in this ring if and only if A is not invertible. Does this hold for arbitrary commutative R? Explain.

2.4 QUATERNIONS

In 1843, W. R. Hamilton constructed the first example of a division ring in which the commutative law of multiplication does not hold. This was an extension of the field of complex numbers, whose elements were quadruples of real numbers $(\alpha, \beta, \gamma, \delta)$ for which the usual addition and a multiplication were defined so that $1 = (1, 0, 0, 0)$ is the unit and $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$, and $k = (0, 0, 0, 1)$ satisfy $i^2 = j^2 = k^2 = -1 = ijk$.[3] Hamilton called his quadruples quaternions. Previously he had defined complex numbers as pairs of real numbers (α, β) with the product $(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma - \beta\delta, \alpha\delta + \beta\gamma)$. Hamilton's discovery of quaternions led to a good deal of experimentation with other such "hypercomplex" number systems and eventually to a structure theory whose goal was to classify such systems. A good deal of important algebra thus evolved from the discovery of quaternions.

We shall not follow Hamilton's way of introducing quaternions. Instead we shall define this system as a certain subring of the ring $M_2(\mathbb{C})$ of 2×2 matrices with complex number entries. This will have the advantage of reducing the calculations to a single simple verification.

We consider the subset $\mathbb{H}$ of the ring $M_2(\mathbb{C})$ of complex 2×2 matrices that have the form

$$x = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{pmatrix}, \quad \alpha_i \text{ real.} \tag{14}$$

We claim that $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$. Since $\overline{a_1 - a_2} = \bar{a}_1 - \bar{a}_2$ for complex numbers it is clear that $\mathbb{H}$ is closed under subtraction; hence $\mathbb{H}$ is a subgroup of the additive group of $M_2(\mathbb{C})$. We obtain the unit matrix by taking $a = 1$, $b = 0$ in (14). Hence $1 \in \mathbb{H}$. Since

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - \bar{a}\bar{d} & -\bar{b}d + \bar{a}\bar{c} \end{pmatrix}$$

[3] It seems to have taken Hamilton ten years to arrive at this multiplication table. In fact, he had spent a good deal of effort trying to construct a field of triples of real numbers (which is not possible) before he realized that it was necessary to go to quadruples and to drop the commutativity of multiplication. Perhaps this bit of history may serve as an encouragement to the student who sometimes finds himself on the wrong track in attacking a problem. (See Carl A. Boyer, *A History of Mathematics*, New York, Wiley, 1968, p. 625.)

and $\overline{a_1 a_2} = \bar{a}_1\bar{a}_2$, the right-hand side has the form

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

where $u = ac - b\bar{d}$, $v = ad + b\bar{c}$. Hence $\mathbb{H}$ is closed under multiplication and so $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$.

We shall now show that $\mathbb{H}$ is a division ring. We note first that

$$\Delta \equiv \det\begin{pmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{pmatrix} = {\alpha_0}^2 + {\alpha_1}^2 + {\alpha_2}^2 + {\alpha_3}^2.$$

Since the α_i are real numbers this is real, and is 0 only if every $\alpha_i = 0$, that is, if the matrix is 0. Hence every non-zero element of $\mathbb{H}$ has an inverse in $M_2(\mathbb{C})$. Moreover, we have, by the definition of the adjoint given in section 2.3, that

$$\operatorname{adj}\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}.$$

Since $\bar{\bar{a}} = a$ this is obtained from the x in (14) by replacing a by $\bar{a}$ and b by $-b$, and so it is contained in $\mathbb{H}$. Thus if the matrix x is $\neq 0$ then its inverse is

$$\begin{pmatrix} \bar{a}\Delta^{-1} & -b\Delta^{-1} \\ \bar{b}\Delta^{-1} & a\Delta^{-1} \end{pmatrix}$$

and this is contained in $\mathbb{H}$. Hence $\mathbb{H}$ is a division ring.

The ring $\mathbb{H}$ contains in its center the field $\mathbb{R}$ of real numbers identified with the set of diagonal matrices $\operatorname{diag}\{\alpha, \alpha\}$, $\alpha \in \mathbb{R}$. $\mathbb{H}$ also contains the matrices

$$i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

We verify that

$$x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \tag{15}$$

and if $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$, $\beta_i \in \mathbb{R}$, then

$$\begin{pmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{pmatrix} = \begin{pmatrix} \beta_0 + \beta_1\sqrt{-1} & \beta_2 + \beta_3\sqrt{-1} \\ -\beta_2 + \beta_3\sqrt{-1} & \beta_0 - \beta_1\sqrt{-1} \end{pmatrix}$$

so $\alpha_i = \beta_i$, $0 \le i \le 3$. Thus any x in $\mathbb{H}$ can be written in one and only one way in the form (15). The product of two elements in $\mathbb{H}$

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k)$$

is determined by the product and sum in $\mathbb{R}$, the distributive laws and the multiplication table

$$i^2 = j^2 = k^2 = -1 \qquad (16)$$
$$ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Incidentally, because these show that $\mathbb{H}$ is not commutative we have constructed a division ring that is not a field. The ring $\mathbb{H}$ is called the *division ring of real quaternions.*

EXERCISES

1. Define $\bar{x} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$ for $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$. Show that $\overline{x+y} = \bar{x} + \bar{y}$, $\overline{xy} = \bar{y}\bar{x}$, and that $\bar{x} = x$ if $x \in \mathbb{R}$.
2. Show that $x\bar{x} = N(x)$ where $N(x) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$. Define $T(x) = 2\alpha_0$. Show that x satisfies the quadratic equation $x^2 - T(x)x + N(x) = 0$.
3. Prove that $N(xy) = N(x)N(y)$.
4. Show that the set $\mathbb{H}_0$ of quaternions $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, whose "coordinates" α_i are rational, form a division subring of $\mathbb{H}$.
5. Verify that the set I of quaternions x in which all the coordinates α_i are either integers or all are halves of odd integers is a subring of $\mathbb{H}$. Is this a division subring? Show that $T(x)$ and $N(x) \in \mathbb{Z}$ for any $x \in I$. Determine the group of units of I.
6. Show that the subring of $M_2(\mathbb{C})$ generated by $\mathbb{C}$ and $\mathbb{H}$ is $M_2(\mathbb{C})$.
7. Let m and n be non-zero integers and let R be the subset of $M_2(\mathbb{C})$ consisting of the matrices of the form
$$\begin{pmatrix} a + b\sqrt{m} & c + d\sqrt{m} \\ n(c - d\sqrt{m}) & a - b\sqrt{m} \end{pmatrix}$$
where $a, b, c, d \in \mathbb{Q}$. Show that R is a subring of $M_2(\mathbb{C})$ and that R is a division ring if and only if the only rational numbers x, y, z, t satifying the equation $x^2 - my^2 - nz^2 + mnt^2 = 0$ are $x = y = z = t = 0$. Give a choice of m, n that R is a division ring and a choice of m, n that R is not a division ring.
8. Determine the center of $\mathbb{H}$. Determine the subring $C(i)$ commuting with i.
9. Let S be a division subring of $\mathbb{H}$ which is stabilized by every map $x \to dxd^{-1}$, $d \neq 0$ in $\mathbb{H}$. Show that either $S = \mathbb{H}$ or S is contained in the center.
10. (Cartan-Brauer-Hua.) Let D be a division ring, C its center and let S be a division subring of D which is stabilized by every map $x \to dxd^{-1}$, $d \neq 0$ in D. Show that either $S = D$ or $S \subset C$.

2.5 IDEALS, QUOTIENT RINGS

We define a congruence $\equiv$ in a ring to be a relation in R which is a congruence for the additive group $(R, +, 0)$ and the multiplicative monoid $(R, \cdot, 1)$. Hence $\equiv$ is an equivalence relation such that $a \equiv a'$ and $b \equiv b'$ imply $a + b \equiv a' + b'$ and $ab \equiv a'b'$. Let $\bar{a}$ denote the congruence class of $a \in R$ and let $\bar{R}$ be the quotient set. As we have seen in section 1.5, we have binary compositions $+$ and $\cdot$ in $\bar{R}$ defined by $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a}\bar{b} = \overline{ab}$. These define the group $(\bar{R}, +, \bar{0})$ and the monoid $(\bar{R}, \cdot, \bar{1})$. We also have

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b+c}) = \overline{a(b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}.$$

Similarly, $(\bar{b} + \bar{c})\bar{a} = \bar{b}\bar{a} + \bar{c}\bar{a}$. Hence $(\bar{R}, +, \cdot, \bar{0}, \bar{1})$ is a ring which we shall call a *quotient* (or *difference*) *ring* of R.

We recall also that the congruences in $(R, +, 0)$ are obtained from the subgroups I (necessarily normal since $(R, +)$ is commutative) by defining $a \equiv b$ if $a - b \in I$. Then the congruence class $\bar{a}$ is the coset $a + I$. If this is also a congruence for the multiplicative monoid, then for any $a \in R$ and any $b \in I$ we have $a \equiv a$ and $b \equiv 0$, and so $ab \equiv a0 = 0$ and $ba \equiv 0$. In other words, if $a \in R$ and $b \in I$ then ab and $ba \in I$. Conversely, suppose I is a subgroup of the additive group satisfying this condition. Then if $a \equiv a'$ and $b \equiv b' \pmod{I}$, $a - a' \in I$ so $ab - a'b = (a - a')b \in I$. Also $a'b - a'b' = a'(b - b') \in I$. Hence $ab - a'b' = (ab - a'b) + (a'b - a'b') \in I$. Hence $ab \equiv a'b' \pmod{I}$. We now give the following

DEFINITION 2.2 *If R is a ring, an ideal I of R is a subgroup of the additive group such that for any $a \in R$ and any $b \in I$, ab and $ba \in I$.*

Our results show that congruences in a ring R are obtained from ideals I of R by defining $a \equiv a'$ if $a - a' \in I$. The corresponding quotient ring $\bar{R}$ will be denoted as R/I and will be called the *quotient ring of R with respect to the ideal I*. The elements of R/I are the cosets $a + I$ and the addition and multiplication in R/I are defined by

$$(a + I) + (b + I) = (a + b) + I \qquad (17)$$
$$(a + I)(b + I) = ab + I.$$

Also I is the 0 and $1 + I$ the unit of R/I.

It is interesting to look at the "algebra" of ideals of a ring R. We note first that the intersection of any set of ideals in R is an ideal. This is immediate from the definition. If S is a subset of R then the intersection (S) of all ideals of R containing S (non-vacuous, since R is such an ideal) is an ideal containing S