PART I

ALGEBRAIC BACKGROUND

We are to be concerned with geometry in planes in which the coordinates of points and the equations of lines can be expressed in terms of elements either of a 'field' or of an algebraic system which satisfies all but one of the axioms which characterize a field. Familiar examples of fields are the algebraic systems whose elements are the rational numbers or the real numbers or the complex numbers; we are more particularly interested in fields with only finite numbers of elements. The 'Galois field' GF (p) of prime order p (named after E. Galois, 1811–32) has for its elements the numbers $0, 1, \ldots, p-1$ and the rules of composition are those of ordinary arithmetic, except that sums and products are 'reduced modulo p'; that is, every number is replaced by the remainder on dividing it by p.

In all these fields multiplication is commutative, and, in fact, the commutative law for multiplication is often included among the axioms for a field. But in the natural evolution of coordinate systems from *geometric* axioms, systems based on commutative fields appear as special cases of systems based on non-commutative (or 'skew') fields. We shall therefore designate as a 'field' a system which is not necessarily commutative in multiplication.

The first strictly non-commutative field to be devised was the system of 'quaternions', invented in 1843 by Sir William Rowan Hamilton to represent the operation of compounding rotations in ordinary Euclidean space. Quaternion numbers are written as $ai + bj + ck + d$ and are compounded in accordance with the axioms for a field. a, b, c, d are real numbers, and i, j, k are 'units' which are independent under addition, and under multiplication satisfy the conditions:

$$ij = k, \quad jk = i, \quad ki = j,$$
$$ji = -k, \quad kj = -i, \quad ik = -j,$$
$$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1.$$

There is a finite system, having only nine elements, which bears a strong resemblance to Hamilton's quaternions. But for the simplification consequent on using such a small system we pay the price of losing one of the distributive laws. The system is therefore not a field.

A finite commutative field† of order 9 exists also, but its definition is a little more complicated than that of the fields of prime order. This field and the 'miniquaternion system' are constructed in the first chapter. In succeeding chapters we discuss how any field may be used to coordinatize a 'projective plane', and also how, from the miniquaternion system, three quite different projective planes are obtained by using various methods of coordinatization.

† J. M. Wedderburn proved in 1905 that every finite field is commutative. For a complete account of this theorem see, for example, I. N. Herstein, 1964, p. 318.

CHAPTER 1

TWO ALGEBRAIC SYSTEMS WITH NINE ELEMENTS

1.1 Near-fields of order 9

The class of finite fields is included in a larger class of algebraic systems called 'finite near-fields', which we consider here because it includes also the miniquaternion system. In fact the miniquaternion system is the smallest near-field which is not a field (H. Zassenhaus, 1936).

DEFINITION 1.1.1 A *finite near-field* is a system $(\mathscr{S}, +, \circ)$, where $+, \circ$ are binary operations on the set $\mathscr{S}$ and

(1) $\mathscr{S}$ is finite,

(2) $+$ is a commutative group operation on $\mathscr{S}$, with identity 0,

(3) $\circ$ is a group operation on $\mathscr{S} - \{0\}$, with identity 1,

(4) $\circ$ is right-distributive over $+$, that is,

$$(\xi+\eta)\circ\zeta = (\xi\circ\zeta)+(\eta\circ\zeta) \quad \text{for all} \quad \xi,\eta,\zeta\in\mathscr{S},\dagger$$

(5) $\xi\circ 0 = 0$ for all $\xi\in\mathscr{S}$.

For convenience we make the usual convention that $\circ$ is to take precedence over $+$, so that the right-distributive law may be written more simply

$$(\xi+\eta)\circ\zeta = \xi\circ\zeta+\eta\circ\zeta.$$

If both distributive laws hold in a finite near-field then the system is a finite (commutative) field. We are to construct two near-fields of order 9: one a field, the other the miniquaternion system. In fact these are the only near-fields of order 9 (Zassenhaus, 1936).

THEOREM 1.1.1 *If* $(\mathscr{S}, +, \circ)$ *is a finite near-field then* $0\circ\xi = 0$ *for all* $\xi\in\mathscr{S}$.

† Some authors—for example, H. Zassenhaus—replace the right-distributive law by the left-distributive law.

First

$$(0+0)\circ\xi = 0\circ\xi + 0\circ\xi \quad \text{(right-distributivity)}.$$

But $\qquad 0+0=0 \qquad$ (0 is identity for $+$),

and so $\qquad 0\circ\xi = 0\circ\xi + 0\circ\xi.$

Therefore

$$\begin{aligned} -(0\circ\xi)+0\circ\xi &= -(0\circ\xi)+(0\circ\xi+0\circ\xi) \\ &= [-(0\circ\xi)+0\circ\xi]+0\circ\xi \text{ (associativity of } +) \\ &= 0+0\circ\xi \\ &= 0\circ\xi. \end{aligned}$$

EXERCISE 1.1.1 Show that in any finite near-field:
(i) $\xi\circ\eta = 0 \Rightarrow$ either $\xi = 0$ or $\eta = 0$,
(ii) $1 \neq 0$ and $-1 \neq 0$.

In any near-field $(\mathscr{S}, +, \circ)$ of order 9, the subset $\mathscr{D} = \{0, 1, -1\}$ of $\mathscr{S}$ plays a special role. For consider the additive subgroup of $\mathscr{S}$ generated by 1. This necessarily contains 0 and -1; $-1 \neq 1$ since $-1 = 1$ would imply $1+1 = 0$, that is, the subgroup has order two, which is impossible since the group $(\mathscr{S}, +)$ has order nine, so that by Lagrange's Theorem any non-trivial subgroup of it has order three or nine. If the subgroup is of order nine then $\mathscr{S}$ itself is generated by 1, that is, the elements of $\mathscr{S}$ are

$$0,\ 1,\ 1+1,\ \ldots,\ 1+1+1+1+1+1+1+1,$$

and $\qquad 1+1+1+1+1+1+1+1+1 = 0;$

but

$$(1+1+1)\circ(1+1+1) = 1+1+1+1+1+1+1+1+1 = 0,$$

by repeated application of the right-distributive law, so

$$1+1+1 = 0,$$

giving a contradiction. Therefore the additive subgroup generated by 1 has order three: it must be $\mathscr{D} = \{0, 1, -1\}$, and we must have $1+1+1 = 0$.

$(\mathscr{D}, +, \circ)$ is the Galois field GF(3), which we shall usually denote simply by $\mathscr{D}$.

THEOREM 1.1.2 *In any near-field $(\mathscr{S}, +, \circ)$ of order 9, the subset $\mathscr{D} = \{0, 1, -1\}$ is such that $(\mathscr{D}, +, \circ)$ is the Galois field of order 3.*

EXERCISE 1.1.2 Write out addition and multiplication tables for $\mathscr{D}$.

EXERCISE 1.1.3 Show that in any near-field of order 9

(i) $\xi + \xi + \xi = 0$ for all ξ

(ii) $(-1) \circ \xi = -\xi = \xi \circ (-1)$ for all ξ

(iii) $(-\xi) \circ \eta = -(\xi \circ \eta) = \xi \circ (-\eta)$ for all ξ, η

(iv) $(-\xi) \circ (-\eta) = \xi \circ \eta$ for all ξ, η.

THEOREM 1.1.3 *Suppose $(\mathscr{S}, +, \circ)$ is a near-field of order 9 and $\sigma \in \mathscr{S}$, but $\sigma \notin \mathscr{D}$. Then each element of $\mathscr{S}$ may be written uniquely in the form $a + b \circ \sigma$, with $a, b \in \mathscr{D}$.*

Assume $$a + b \circ \sigma = a' + b' \circ \sigma \quad (a, b, a', b' \in \mathscr{D}).$$

Then $$\begin{aligned} a - a' &= b' \circ \sigma - (b \circ \sigma) \\ &= b' \circ \sigma + (-b) \circ \sigma = [b' + (-b)] \circ \sigma \\ &= (b' - b) \circ \sigma. \end{aligned}$$

If $b' \neq b$, then $\sigma = (b'-b)^{-1} \circ (a - a') \in \mathscr{D}$; but $\sigma \notin \mathscr{D}$, so $b' = b$, which implies that $a' = a$. It follows that there are nine distinct elements $a + b \circ \sigma$ in $\mathscr{S}$ corresponding to the nine pairs a, b. But $\mathscr{S}$ has only nine elements, so the theorem is proved.

This theorem implies that, once an element σ not in $\mathscr{D}$ has been chosen, there is a natural 1–1 correspondence between elements of $\mathscr{S}$ and ordered pairs (a, b) of elements of $\mathscr{D}$:

$$a + b \circ \sigma \leftrightarrow (a, b).$$

If we identify corresponding elements, that is, write

$$(a, b) = a + b \circ \sigma,$$

then since

$$(a_1 + b_1 \circ \sigma) + (a_2 + b_2 \circ \sigma) = (a_1 + a_2) + (b_1 + b_2) \circ \sigma$$

we have $$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2).$$

This means that the addition operation in $\mathscr{S}$ is uniquely determined by the addition operation of the Galois field $\mathscr{D}$, and thus:

THEOREM 1.1.4 *The additive groups of all near-fields of order 9 have the same abstract group structure (that is, they are isomorphic).*

1.2 The Galois field $\mathscr{F}$ of order 9

We now construct, using $\mathscr{D}$, a near-field $\mathscr{F}$ of order 9 which, in addition to satisfying the conditions of Definition 1.1.1, is left-distributive, and therefore a field.

The nine elements of $\mathscr{F}$ are the ordered pairs (a, b), $a, b \in \mathscr{D}$. Addition in $\mathscr{F}$ is defined by the rule

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

and multiplication by

$$(a_1, b_1) \times (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1),$$

where $a_1 a_2, b_1 b_2$, etc., denote products in $\mathscr{D}$. (Compare with addition and multiplication of ordinary complex numbers when they are written as ordered pairs of real numbers.)

It is easily seen that $+$ is a commutative group operation on $\mathscr{F}$: the commutativity and associativity follow from the same properties of $+$ in $\mathscr{D}$; the identity is $0 = (0, 0)$ and the inverse $-(a, b)$ of (a, b) is $(-a, -b)$.

By the symmetry of the formula for $(a_1, b_1) \times (a_2, b_2)$ and the commutativity of the operations in $\mathscr{D}$, the operation $\times$ is commutative. That $\times$ is a group operation on $\mathscr{F} - \{0\}$ is again straightforward. (The proof is the same as for the complex numbers.) The identity is $1 = (1, 0)$ and the inverse $(a, b)^{-1}$ of $(a, b) \neq (0, 0)$ is $(a/(a^2 + b^2), \; -b/(a^2 + b^2))$. (If $a, b \in \mathscr{D}$ then $a^2 + b^2 = 0 \Leftrightarrow a = b = 0$.)

Finally, $\times$ is associative:

$$\begin{aligned}
(a_1, b_1) &\times [(a_2, b_2) \times (a_3, b_3)] \\
&= (a_1, b_1) \times (a_2 a_3 - b_2 b_3, a_2 b_3 + b_2 a_3) \\
&= (a_1 a_2 a_3 - a_1 b_2 b_3 - b_1 a_2 b_3 - b_1 b_2 a_3, \\
&\qquad a_1 a_2 b_3 + a_1 b_2 a_3 + b_1 a_2 a_3 - b_1 b_2 b_3) \\
&= (a_1 a_2 - b_1 b_2, a_1 b_2 + b_1 a_2) \times (a_3, b_3).
\end{aligned}$$

Thus $\times$ is a group operation on $\mathscr{F} - \{0\}$.

The proof of right-distributivity is routine:

$$\begin{aligned}
&[(a_1, b_1) + (a_2, b_2)] \times (a_3, b_3) \\
&\quad = (a_1 + a_2, b_1 + b_2) \times (a_3, b_3) \\
&\quad = (a_1 a_3 + a_2 a_3 - b_1 b_3 - b_2 b_3, a_1 b_3 + a_2 b_3 + a_3 b_1 + a_3 b_2) \\
&\quad = (a_1 a_3 - b_1 b_3, a_1 b_3 + a_3 b_1) + (a_2 a_3 - b_2 b_3, a_2 b_3 + a_3 b_2) \\
&\quad = (a_1, b_1) \times (a_3, b_3) + (a_2, b_2) \times (a_3, b_3).
\end{aligned}$$

Thus $\mathscr{F}$ is a near-field of order 9. But $\times$ is commutative. So $\mathscr{F}$ is also left-distributive; that is, $\mathscr{F}$ is a commutative field.

For simplicity we shall henceforth denote $\times$ by the usual . or juxtaposition.

If we write $a = (a, 0)$ and $\epsilon = (0, 1)$ then we may easily verify that $(a, b) = a + b\epsilon$ and $\epsilon^2 = -1$.

Let us examine the multiplicative group of $\mathscr{F}$. This group is in fact cyclic. It is not generated by ϵ since $\epsilon^2 = -1$, $\epsilon^4 = 1$. But $(1-\epsilon)^2 = 1 + \epsilon + \epsilon^2 = \epsilon$, so that $(1-\epsilon)^4 = \epsilon^2 = -1$, and, therefore, $(1-\epsilon)^8 = 1$ and no smaller power of $1-\epsilon$ is equal to 1.

Denote $1-\epsilon$ by ω. The powers of ω are:

$$\begin{aligned}
\omega &= 1 - \epsilon, & \omega^5 &= -1 + \epsilon, \\
\omega^2 &= \epsilon, & \omega^6 &= -\epsilon, \\
\omega^3 &= 1 + \epsilon, & \omega^7 &= -1 - \epsilon, \\
\omega^4 &= -1, & \omega^8 &= 1.
\end{aligned}$$

Considering the non-zero elements of $\mathscr{F}$ as powers of ω simplifies multiplication, but makes addition a little more complicated. Addition may be performed without referring back to ϵ by using the relation

$$\omega^2 = -\omega + 1.$$

For example, $\omega^3 = -\omega^2 + \omega = -(-\omega + 1) + \omega = -\omega - 1$, so that $\omega^3 + 1 = -\omega$; but

$$\omega^4 = (\omega^2)^2 = (1-\omega)^2 = 1 + \omega + \omega^2 = 1 + \omega + 1 - \omega = -1,$$

and therefore $\omega^3 + 1 = -\omega = (-1).\omega = \omega^4.\omega = \omega^5$.

EXERCISE 1.2.1 From $\omega^2 = -\omega + 1$ deduce the relation $\omega^2 + 1 = \omega^3$.

If $\omega^r = a+b\epsilon$, then $(\omega^r)^3 = a^3+3a^2b\epsilon+3ab^2\epsilon^2+b^3\epsilon^3$. But

$$x \in \mathscr{D} \Rightarrow x^3 = x \quad \text{and} \quad 3x = 0.$$

Also $\epsilon^2 = -1$, so that $\omega^r = a+b\epsilon \Rightarrow w^{3r} = a-b\epsilon$.

Following the practice with complex numbers we use the terminology

DEFINITION 1.2.1 $a+b\epsilon$ and $a-b\epsilon$ are *conjugate* members of $\mathscr{F}$, and we write

$$(a+b\epsilon)^* = a-b\epsilon, \quad \text{that is} \quad (\omega^r)^* = \omega^{3r}.$$

We usually write ω^{r*} for the conjugate of ω^r. Note that

$$\omega^{r*} = \omega^{3r} = (\omega^3)^r = (\omega^*)^r.$$

For future reference we give the complete table for addition, in terms of ω:

Table 1.2.1

$+$	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
1	ω^4	ω^7	ω^3	ω^5	0	ω^2	ω	ω^6
ω	ω^7	ω^5	1	ω^4	ω^6	0	ω^3	ω^2
ω^2	ω^3	1	ω^6	ω	ω^5	ω^7	0	ω^4
ω^3	ω^5	ω^4	ω	ω^7	ω^2	ω^6	1	0
ω^4	0	ω^6	ω^5	ω^2	1	ω^3	ω^7	ω
ω^5	ω^2	0	ω^7	ω^6	ω^3	ω	ω^4	1
ω^6	ω	ω^3	0	1	ω^7	ω^4	ω^2	ω^5
ω^7	ω^6	ω^2	ω^4	0	ω	1	ω^5	ω^3

1.3 The miniquaternion system $\mathscr{Q}$

Next we construct a near-field $\mathscr{Q}$ of order 9 which is not left-distributive; $\mathscr{Q}$ will be called 'the miniquaternion system'.

The elements of $\mathscr{Q}$ are the same as those of $\mathscr{F}$; that is, the nine ordered pairs (a, b) with $a, b \in \mathscr{D}$. Furthermore, addition in $\mathscr{Q}$ is the same as in $\mathscr{F}$ (cf. Theorem 1.1.4):

$$(a_1, b_1)+(a_2, b_2) = (a_1+a_2, b_1+b_2).$$

That is, if we express the elements of $\mathscr{Q}$ as powers of ω the addition table is again Table 1.2.1.

While multiplication is of course different, we can define it in terms of multiplication in $\mathscr{F}$. We divide the non-zero elements

—that is, the set of eight powers $\omega^0, \omega^1, \omega^2, \ldots, \omega^7$ of ω—into two subsets $\mathscr{E}$ and $\mathscr{O}$:

$$\mathscr{E} = \{\omega^0, \omega^2, \omega^4, \omega^6\} = \{\text{even powers of } \omega\},$$

$$\mathscr{O} = \{\omega^1, \omega^3, \omega^5, \omega^7\} = \{\text{odd powers of } \omega\}.$$

In the field $\mathscr{F}$ multiplication is given by the rules:

$$0.\xi = \xi.0 = 0 \quad \text{for all} \quad \xi, \quad \text{and} \quad \omega^r.\omega^s = \omega^{r+s}$$

(indices taken modulo 8). The new multiplication $\otimes$ is defined as follows:

$$0 \otimes \xi = 0, \quad \xi \otimes 0 = 0 \qquad \text{for all } \xi$$

$$\omega^r \otimes \omega^s = \omega^r.\omega^s = \omega^{r+s} \qquad \text{if} \quad \omega^s \in \mathscr{E}$$

$$\omega^r \otimes \omega^s = \omega^{r*}.\omega^s = \omega^{3r}.\omega^s = \omega^{3r+s} \quad \text{if} \quad \omega^s \in \mathscr{O}.$$

Thus, for example,

$$\omega^2 \otimes \omega = \omega^6.\omega = \omega^7, \quad \text{but} \quad \omega \otimes \omega^2 = \omega.\omega^2 = \omega^3.$$

So $\otimes$ is not commutative. Also $\otimes$ is not left-distributive over $+$: from Table 1.2.1

$$\omega \otimes (\omega + 1) = \omega \otimes \omega^7 = \omega^3.\omega^7$$
$$= \omega^2,$$

whereas
$$\omega \otimes \omega + \omega \otimes 1 = \omega^3.\omega + \omega.\omega^0 = \omega^4 + \omega$$
$$= \omega^6.$$

The *miniquaternion system* $\mathscr{Q}$ consists of the nine elements (a, b), and the operations $+$, $\otimes$.

EXERCISE 1.3.1 Express $(1, 1)$ and $(1, -1)$ as powers of ω and hence determine the product $(1, 1) \otimes (1, -1)$.

THEOREM 1.3.1 *$\mathscr{Q}$ is a near-field of order* 9.

$\mathscr{Q}$, by definition, has nine elements. The operation $+$, being the same as in $\mathscr{F}$, is a commutative group operation. The operation $\otimes$ has identity

$$1 = \omega^0 \quad (\omega^r \otimes \omega^0 = \omega^r.\omega^0 = \omega^r; \quad \omega^0 \otimes \omega^r = \omega^0.\omega^r = \omega^r).$$

Cambridge University Press
978-0-521-09064-3 - Miniquaternion Geometry: An Introduction to the Study of Projective Planes
T. G. Room and P. B. Kirkpatrick
Excerpt
More information

If $\omega^r \in \mathscr{E}$ then it has inverse ω^{-r} with respect to $\otimes$, and if $\omega^r \in \mathscr{O}$ then it has inverse ω^{-3r}. To show this, we remark first that, in $\mathscr{F}$, $\omega^{-r} = \omega^{8-r}$, so that

$$\omega^r \in \mathscr{E} \Rightarrow \omega^{-r} \in \mathscr{E} \quad \text{and} \quad \omega^{3r} \in \mathscr{E},$$

and

$$\omega^r \in \mathscr{O} \Rightarrow \omega^{-r} \in \mathscr{O} \quad \text{and} \quad \omega^{3r} \in \mathscr{O}.$$

Thus, if $\omega^r \in \mathscr{E}$, then

$$1 = \omega^{-r}.\omega^r = \omega^{-r} \otimes \omega^r,$$

$$1 = \omega^r.\omega^{-r} = \omega^r \otimes \omega^{-r},$$

while, if $\omega^r \in \mathscr{O}$, then

$$1 = \omega^{-r}.\omega^r = \omega^{-3r} \otimes \omega^r,$$

$$1 = \omega^{3r}.\omega^{-3r} = \omega^r \otimes \omega^{-3r}.$$

It remains to be proved that $\otimes$ is associative and right-distributive over $+$. If $\omega^t \in \mathscr{E}$,

$$(\omega^r + \omega^s) \otimes \omega^t = (\omega^r + \omega^s).\omega^t = \omega^r.\omega^t + \omega^s.\omega^t$$

$$= \omega^r \otimes \omega^t + \omega^s \otimes \omega^t;$$

whereas, if $\omega^t \in \mathscr{O}$,

$$(\omega^r + \omega^s) \otimes \omega^t = (\omega^r + \omega^s)^3.\omega^t = (\omega^{3r} + \omega^{3s}).\omega^t$$

$$= \omega^{3r}.\omega^t + \omega^{3s}.\omega^t$$

$$= \omega^r \otimes \omega^t + \omega^s \otimes \omega^t.$$

If $\omega^s, \omega^t \in \mathscr{E}$,

$$(\omega^r \otimes \omega^s) \otimes \omega^t = \omega^{r+s} \otimes \omega^t = \omega^{r+s+t}$$

$$= \omega^r \otimes \omega^{s+t} \quad \text{as} \quad \omega^{s+t} \in \mathscr{E}$$

$$= \omega^r \otimes (\omega^s \otimes \omega^t).$$

If $\omega^s \in \mathscr{E}$ and $\omega^t \in \mathscr{O}$,

$$(\omega^r \otimes \omega^s) \otimes \omega^t = \omega^{r+s} \otimes \omega^t = \omega^{3r+3s+t}$$

$$= \omega^r \otimes \omega^{3s+t} \quad \text{as} \quad \omega^{3s+t} \in \mathscr{O}$$

$$= \omega^r \otimes (\omega^s \otimes \omega^t).$$

We leave to the reader the proofs of associativity when

$$\omega^s \in \mathscr{O}, \quad \omega^t \in \mathscr{E} \quad \text{and when} \quad \omega^s, \omega^t \in \mathscr{O}.$$