Chapter VI
Quaternions, divisibility and discreteness.

6.1 Introduction.

In this chapter we discuss further properties of quaternions and form a discrete model of quantum theory linking mathematical models to observations. We find the mappings from quaternions to objects describing the equation for the relativistic theory of the election.

The simple theory has difficulties in non cancellation of infinities, which is known as the renormalisation problem. A solution is to provide a theory which is inherently discrete at a fundamental level. We link this with the mathematical aspects we are dealing with in this chapter by discussing Wedderburn's little theorem, which states that every finite division ring is commutative. This has implications for finite quantum mechanics, which can be put in a noncommutative context, so we are stating that a noncommutative finite quantum theory is impossible if it everywhere has a division operation. A solution is that the theory does not everywhere have division and there is a level at which division is no longer possible. This is a feature of string theory, so we have derived this feature of string theory from first principles.

6.2 The quaternion division algebra.

We found in chapter I that the complex numbers obey the rules of addition, subtraction, multiplication and division given in the axioms for a mathematical field. The quaternions also obey these axioms, except that the commutative multiplicative rule is dropped. So in general if A, B and C are quaternions, then

$$AB \neq BA,$$

although the multiplicative associative rule is retained

$$(AB)C = A(BC).$$

An associative division algebra satisfies all axioms for a field except the multiplicative commutativity rule, so this is satisfied by the quaternions.

To demonstrate that the product of two quaternions with real coefficients

$$(a1 + bi + cj + dk)(p1 + qi + rj + tk) \qquad (1)$$

cannot be zero unless a = b = c = d = 0 or p = q = r = t = 0, we can equate by hypothesis the real and quaternion parts of (1) to zero, to obtain the following 4 equations in 8 unknowns.

<u>real part</u>:

$$ap - bq - cr - dt = 0 \qquad (2)$$

<u>i part</u>:

$$pb + aq + ct - dr = 0 \qquad (3)$$

<u>j part</u>:

$$pc + ar - bt + qd = 0 \qquad (4)$$

<u>k part</u>:

$$pd + at + br - cq = 0. \qquad (5)$$

The proof that these equations are inconsistent unless a quaternion in product (1) is zero, and that therefore formula (1) is not zero except under this condition is given in *Superexponential algebra* [Ad15], chapter V, section 2. We will omit here this direct proof for quaternions.

6.3 Quaternions as the highest dimensional associative division algebra.

We will later extend the number of dimensions for quaternion-like objects with a similar algebra, called octonions, but first we show that when we do this we loose associativity and therefore a matrix representation, since matrices are associative.

Definition 6.3.1. An *associative division algebra* has a multiplicative identity $1 \neq 0$ where every nonzero element has a multiplicative inverse.

We prove that *the only associative division algebras are the reals, complex numbers and quaternions*. We will represent the basis elements of these associative division algebras by hyperintricate numbers.

In category theory, a basis of a vector space is an example of a universal arrow, which shows a vector has properties independent of basis. Nevertheless, we can also prove this is so in the case where the hyperintricate basis elements are transformed to the general case studied next.

These basis elements have square ±1, and any other representation can be reduced to a linear combination of these basis elements, for which the basis element squares are also ±1. In detail, any representation of the set $\{1, i, \alpha, \phi\}$ under a change of basis which preserves squares maps each element to the set

$$\{1, \pm\sqrt{(\gamma_i^2 + \delta_i^2 + 1)}i + \gamma_i\alpha + \delta_i\phi, \pm\sqrt{(\gamma_\alpha^2 + \delta_\alpha^2 - 1)}i + \gamma_\alpha\alpha + \delta_\alpha\phi,$$
$$\pm\sqrt{(\gamma_\phi^2 + \delta_\phi^2 - 1)}i + \gamma_\phi\alpha + \delta_\phi\phi\}$$

with the coefficients $\gamma_i \neq \gamma_\alpha \neq \gamma_\phi$ etc. real. This extends to all layers.

It is not initially clear, for example, whether 1_{11}, $i_{\alpha 1}$, 1_{i1}, $i_{\phi 1}$, 1_{1i}, $i_{\alpha i}$, 1_{ii} and $i_{\phi i}$ can form a normed division algebra in which more than one square of a basis element is 1, e.g.1_{ii}.

For any hyperintricate basis element, the inverse is known. For a basis element A whose square is 1, the inverse $A^{-1} = A$. These A amount to all basis elements which have an even number (including zero) of i's in their hyperintricate representation. For any basis element, B, whose square is -1, the inverse $B^{-1} = -B$. The set of all B's is those basis elements which have an odd number of i's in their hyperintricate representation.

There are only two possibilities for basis elements, they either commute, AB = BA, or they anticommute, AB = -BA, arising from the commutation or anticommutation of their layers.

Consider finding the inverse of $aA_1 + bA_2$, $A_1 \neq A_2$, where A_1^2 and $A_2^2 = 1$. This is then

$$(aA_1 - bA_2)/(a^2 - b^2) \qquad (1)$$

when A_1 and A_2 commute and

$$(aA_1 + bA_2)/(a^2 + b^2)$$

when A_1 and A_2 anticommute. If we use the fact that 1 is always present amongst such A's, then for some values of a and b, (1) holds, which implies that there exist a's and b's for which (1) includes the possibility of dividing by zero. The statement that we can do division is used in the definition of a division algebra (although we have to specifically exclude division by zero, as for a field), therefore there exists in such division algebras only one basis element with square 1, and this must be the real basis element. We will extend these considerations later.

To find the inverse of a1 + bB_1, where $B_1^2 = -1$, then this is

$(a1 - bB_1)/(a^2 + b^2)$,

which introduces no further problems.

To find the inverse of $aB_1 + bB_2$, for $B_1^2 = -1$ and $B_2^2 = -1$, then this is the permitted

$-(aB_1 + bB_2)/(a^2 + b^2)$,

when B_1 and B_2 anticommute, which is now the only possibility, since the alternative holds if and only if (1) can hold. The above argument may be generalised for more B_r's, and it becomes necessary to stipulate that all $B_1, B_2, \ldots B_n$ mutually anticommute.

We know there are solutions for B_1, B_2, B_3 given by basis elements for the quaternions. Now assume the existence of four such basis elements, B_1, B_2, B_3, B_4, all mutually anticommuting and distinct, so that $B_rB_s = -B_sB_r$. We will use associativity of these basis elements in computing from $B_1B_2B_3B_4$ its mirror reflection in two separate ways. So

$$\begin{aligned}B_1B_2B_3B_4 &= -B_1B_2B_4B_3\\ &= B_1B_4B_2B_3\\ &= -B_4B_1B_2B_3\\ &= B_4B_1B_3B_2\\ &= -B_4B_3B_1B_2\\ &= B_4B_3B_2B_1.\end{aligned}$$

However

$$\begin{aligned}(B_1B_2)(B_3B_4) &= -(B_3B_4)(B_1B_2)\\ &= -(B_4B_3)(B_2B_1),\end{aligned}$$

a contradiction.

Thus the maximum number of dimensions for an associative division algebra is 4. ☐

6.4 Quaternions, bosons and fermions.

We relate our discussion on quaternions to Eli Cartan's *The theory of spinors* [Ca66] where he claims a bijection between spinors and the relativistic (Dirac) equation of the electron which maps to quaternions. We will find these spinors do not map to quaternions and we cannot adjoin spinors to quaternions in a matrix formalism, because the dimension of this combination is greater than 4, so by the result of the previous section, the algebra cannot be a matrix one, and is nonassociative.

Cartan introduces spinors via the observable coefficients of vectors with zero norm

$$x_1^2 + x_2^2 + x_3^2 = 0 \qquad (1)$$

satisfied by two numbers h_0, h_1 given by

$$\begin{aligned}x_1 &= h_0^2 - h_1^2\\ x_2 &= i(h_0^2 + h_1^2)\\ x_3 &= -2h_0h_1,\end{aligned}$$

with possible solutions

$$h_0 = \pm\sqrt{\frac{x_1 - ix_2}{2}}, \qquad (2)$$

$$h_1 = \pm\sqrt{\frac{-x_1 - ix_2}{2}}. \qquad (3)$$

Now choose a vector dependent only on the coordinates x_1 and x_2, say $x_1 - ix_2$. If this is rotated about the axis x_3 to a vector $e^{i\theta}(x_1 - ix_2)$, then h_0 is transformed to $e^{i\theta/2}h_0$, and likewise h_1 is transformed to $e^{i\theta/2}h_1$. Then when $\theta = 2\pi$, a complete rotation, x_3 is transformed to $-x_3$. Thus the spinors h_0 and h_1 are *locally fermionic*.

He considers in our notation the observable matrix basis

$$\phi_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad -i_i = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \alpha_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

so that

$$\phi_1^2 = (-i_i)^2 = \alpha_1^2 = 1_1,\ \phi_1(-i_i) = -(-i_i\phi_1),\ -i_i\alpha_1 = -\alpha_1(-i_i),\ \alpha_1\phi_1 = -\phi_1\alpha_1,$$

which he states are related to the quaternions on multiplication by -1_i

$$I_1 = -1_i\phi_1,\ I_2 = -1_i(-i_i),\ I_3 = -1_i\alpha_1. \qquad (4)$$

This is closely related to the beable basis already given by us, 1_1, α_i, i_1 and ϕ_i, which matches (4) except for minus signs whose square is 1 (it is only possible to change the basis left- or right-handedness by this means). From it Cartan is able to deduce the quaternion algebra

$$I_1^2 = I_2^2 = I_3^2 = -1,\ I_1I_2 = -I_2I_1,\ I_2I_3 = -I_3I_2,\ I_3I_1 = -I_1I_3, \qquad (5)$$

which he relates to the Dirac equation. ☐

However we must note that the transformations derived in (2) and (3) involve complex numbers, which are commutative, whereas equation (5) involves quaternions which are noncommutative. Thus there is no equation as given by Cartan of this type. ☐

There is an alternative algebra available to us, where in the intricate representation, the vector

$$a1_1 + b\alpha_i + ci_1 + d\phi_i$$

is projected not by i_1 but by 1_i. Clearly $(i_1)^2 = -1$ and $(1_i)^2 = -1$. We might wish to use this to represent both bosonic and fermionic quaternions in one object. However, as we have seen, if we adjoin the algebra for 1_1, 1_i, i_α and i_ϕ to the algebra for 1_1, i_1, α_i and ϕ_i, then we can obtain by multiplication objects like $\phi_\alpha = (i_\phi)(\alpha_i)$ with square 1, and these algebras allow zero products like $(1_1 + \phi_\alpha)(1_1 - \phi_\alpha) = (1_1)^2 - (\phi_\alpha)^2 = 0$ and singularities, that is, division by zero.

It seems when the beables are singularity free we must choose only one, but arbitrary, quaternionic algebra.

It is interesting that if, under the interpretation, the observer is measuring along (ix), then the quaternion (jy) = jx(y/x) is transformed as an observable on multiplying, say on the left, to i(jy) = ky, whereas i(kz) = -jz. Thus the coordinates in the model transform to observables in which the y and z coordinates are swapped round, and the observable coordinate z becomes negative. This transformation can be obtained from a rotation of the model coordinates to the observable coordinates, that is, it retains the handedness of the coordinate system.

In this system we can choose to embed this local quaternion structure in a global manifold which is oriented, that is say, an ix vector moving through 2π radians in a jy and kz circle returns to itself with the ix vector pointing in the same direction. When this happens, we say the observable derived from the quaternion is *globally bosonic*. We can also implement nonoriented global manifolds in which an ix vector moving through 2π radians in a jy and kz circle returns to itself with the ix vector pointing in the opposite direction. We then say the quaternion is *globally fermionic*.

Thus we are reduced to considering globally bosonic or globally fermionic quaternion structures. We will see in the chapter XI that the globally bosonic and globally fermionic idea can be extended to the octonions and n-novanions. Our escape route from contradiction is that the extended quaternion object given by the n-novanions is not representable by a matrix, and a conclusion from section 2 is that it is nonassociative. ☐

6.5 Wedderburn's little theorem.

It may be the case that the quaternion algebra is discrete, so that it has multiplication but no division. In this situation, as will be seen here from Wedderburn's little theorem, it is discrete from below and is otherwise infinite, or it can be described consistently by having an infinite upper and lower bound mapped to finite values.

A *permutation* is a bijection of a finite set to itself. A permutation which interchanges cyclically m objects of a set {1, 2, ..., m} forms an abelian group called a cycle of degree m.

This permutation is obtained from a power by specifying that a^{m-1} is the m^{th} element and the cyclic permutation consists of multiplying by a. It can be represented by

$$\begin{pmatrix} 1 & 2 & \cdots & m-1 & m \\ 2 & 3 & \cdots & m & 1 \end{pmatrix},$$

or in contracted notation by (1 2 ... m).

A noncommutative group can be generated by cycles which overlap somewhere. For example

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

The symmetric group can be described by matrices. For example $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$ can be represented by the matrix with one 1 in each row and column, and zeros elsewhere

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

in which, say, 2 → 4 is represented by a 1 in the second row and fourth column, with operations defined by matrix multiplication.

As a further example, the cyclic group of order 4 is given by the matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

All elements of the group can be obtained from the above by permuting rows or alternatively and equivalently by permuting columns.

A *ring* has two operations, + and ×, satisfying for + the axioms of an additive (abelian) group, for × the axioms of a noncommutative multiplicative group except that there may be no division, and the distributive laws connecting multiplication and addition, given in 3.5.(11).

Suppose we represent the integer parts of the rational numbers by notches along a line

```
      |____|____|____|____|____|____|____|____|____|____|____|__
  ... -1    0    1    2    3    4    5    6    7    8    9 ...
```

then any rational number may be represented uniquely by an integer plus a rational number q equal to or greater than 0 and less than 1. This is an example of the theorem given by Euclid, in book 7 of the Elements.

The algorithm may be restated as:
Theorem 6.5.1. *Every positive whole number* n *can be written uniquely in terms of a positive whole number* w *less than* n *multiplied by another natural number* $k > 0$ *with a unique remainder* $0 \leq t < w$:

$$n = kw + t. \quad (1)$$

Proof. If w divides n, then $t = 0$ and we are done. Otherwise assume (1). If n comes between kw and $(k + 1)w$, then (1) holds with $0 < t < w$. ☐

Using the theorem, we can develop an arithmetic for fixed w in which we only consider t above. This finite arithmetic is known as congruence, or clock arithmetic. The equation above is then written, in a notation due to Gauss

$$t = n \pmod{w}.$$

Theorem 6.5.2. **Lagrange's four squares theorem.** A*ny natural* (*positive whole*) *number is the sum of four squares, including possibly the zero square*.

A number of proofs of Lagrange's theorem, given in [Ad15] chapter 3, [Da82] chapter 5, [HW38] theorem 369, [La27] theorems 166-169 and [NZ60] paragraph 5.7, can be found. There is also one in Wikipedia.

Theorem 6.5.3. Wedderburn's little theorem. *Any finite division ring is commutative*.

Proof. To obtain a proof of Wedderburn's little theorem, we first will prove that every finite group can be represented by matrices (mod m). But every finite group can be represented by permutation matrices, for which the (mod m) restriction is irrelevant. Thus multiplicatively a restriction to congruence arithmetic is bogus.

For a finite ring the abelian additive part can be mapped surjectively to (mod n) for a product $n = \prod_k n_k$, and for the least common multiple denoted by l.c.m., a sum $r_k = \sum_{i=0}^{k-1} \text{l.c.m.}(n_i)$ with distinct cycles $(r_k + 1, ..., r_k + n_k)$ mapped bijectively to natural numbers n_k.

In general a division algebra is a subalgebra of the complex numbers, the quaternions or other nonassociative division algebras which may exist. Consider the associative case. It is a result of Frobenius that the quaternions are the most general associative division algebra in the non-finite case, there being no such other algebras which are not subalgebras of these.

Let the order, or number of elements, of the multiplicative part of a finite division ring be m. This is the order of the ring forgetting all additive operations. Let the order of the additive part of this ring be the n above, the order of the ring forgetting all multiplicative operations. Let the l.c.m. of m and n be L. Then the order of the finite division ring is L. This follows from the (mod L) constraint being a necessary and sufficient condition for the distributive laws

$$a(b + c) = ab + ac \quad (2)$$

and

$$(f + g)h = fh + gh \quad (3)$$

to hold for the ring.

We prove as a lemma that if the case

$$a = 0 \pmod{m},$$

$(b + c) = 0 \pmod{n}$

holds and we have

$m = pc$

$n = qc,$

where c is the highest common factor of m and n, then

$a(b + c) = 0 \pmod{pcq},$

and pcq is the l.c.m. of m and n, since any divisor of pc and qc is a divisor of pcq, this holds maximally when the divisors are m and n respectively. But since (2) and (3) hold in infinitely countable arithmetic (a way of saying this is in *characteristic zero*), and we have shown that the left hand sides hold when say $a = 0 \pmod{L}$ and $(b + c) = 0 \pmod{L}$, by the Euclidean algorithm, the remainder $\leq L$ on division by a suitable multiple of L also satisfies (2) and (3).

If not all coefficients of the basis elements i, j, k of the quaternion

$a1 + bi + cj + dk \pmod{L}$

are zero, then the inverse is

$a1 – bi – cj – dk/(a^2 + b^2 + c^2 + d^2) \pmod{L},$

and by Lagrange's four squares theorem, putting $L = (a^2 + b^2 + c^2 + d^2)$ means the inverse does not exist, since dividing by L is equivalent to dividing by zero. ☐