FINITE CUBES AND FINITE AFFINE SPACES

P.B. KIRKPATRICK
School of Mathematics and Statistics
University of Sydney, N.S.W. 2006
Australia.

Abstract

We begin by considering certain analogues, in finite 3-dimensional affine spaces, of the ordinary cube. From the properties of these structures (as geometric lattices having point sets which are threefold Cartesian products) we derive the notion of an (abstract) *finite cube*. By studying the additional properties (including the properties of certain groups associated with the cube) of members of a suitably restricted class of embedded finite cubes, we arrive at the notion of a *perfect* finite cube. Our main theorem asserts that every perfect finite cube can be embedded in a finite 3-dimensional affine space.

1 Introduction

Among the best known and most studied combinatorial designs are the finite projective and affine spaces, in particular those constructible from finite fields (which includes all the finite projective and affine spaces of dimension greater than two). Further designs can be obtained from these spaces using various constructions: for example, the points and lines of any finite 3-dimensional projective or affine space are the points and blocks of a balanced incomplete block design, as are the points and planes of any 4-dimensional projective or affine space.

Various types of subsets of the point sets of such finite spaces have been studied in the literature, including especially those (such as conics in the plane and quadric surfaces in 3-dimensional space) defined by polynomial equations in the coordinate variables. The latter may be regarded as finite analogues of the algebraic curves, surfaces etc. of classical geometry. Some of them yield further important block designs.

The study of *arbitrary* finite sets of vectors led in the 1930's to the concept of a matroid (see for example Welsh [3], p. 6 for a brief history of matroid theory), and to the related concept of a *geometric lattice* (cf. [3], p. 51). Every finite subset of the point set of a projective or affine space inherits from the enveloping space a geometric lattice structure. An important problem is the determination of sufficient conditions for an abstract geometric lattice to be embeddable (in a projective or affine space).

A *solid* in ordinary 3-dimensional Euclidean space may be thought of as a subset of the point set. The most famous solids, apart from the solid sphere, are of course the Platonic solids, of which the *cube* is probably the most familiar. We seek suitable *finite* analogues of the ordinary cube.

Now a point of Euclidean space belongs to the unit cube if and only if all of its coordinates belong to the closed interval [0, 1]. The embedded 'finite cubes' of §2 are obtained by replacing the classical coordinate field $\mathbf{R}$ by an arbitrary *finite* field F, and replacing the interval [0, 1] by an (almost) *arbitrary* subset S of F. The structure of such a 'cube' includes its structure as a geometric lattice. It also includes the structure of the point set $\mathbf{S}^3$ as a Cartesian product. These two structures are intertwined.

In §§2.5–2.8 we show how the internal structure of an embedded 'finite cube' gives rise to a certain algebraic structure, including a group the elements of which are some of the 'planes' of the 'cube'. Unfortunately, this algebraic structure is often completely trivial. However, in the case of the 'dense cubes' discussed in §§2.9–2.12, the algebraic structure contains alot of information about both the cube and its enveloping space.

Our notion of an (abstract) *finite cube*, introduced in §3, is based on some of the properties common to all embedded 'cubes'. The *rigid* finite cubes introduced in §4 have some of the additional properties common to all those embedded cubes which are 'dense' in their enveloping spaces. The group associated with a rigid cube is a *Frobenius group*. (For an account of the basic properties of Frobenius groups, see for example Huppert [1], pp. 495–508.) By imposing a certain condition (cf. axiom **B** in §5.1) on this group and its relationship to the cube, we obtain the notion of a *balanced* rigid cube. Imposing a further condition, namely that the complements of the Frobenius group be abelian, we arrive in §6 at the notion of a *perfect* finite cube.

It can be checked that every embedded finite cube which is 'dense' in its enveloping space is a perfect finite cube. Our main theorem (cf. §6.16) asserts that every perfect finite cube can be embedded in a finite 3-dimensional affine space.

2 Cubes in Finite Affine Spaces

2.1 The affine space AG$(3, F)$

Suppose that F is a finite field. Then the affine geometry AG$(3,F)$ of dimension 3 over F is a finite analogue of ordinary 3-dimensional Euclidean space. The *points* are ordered triples (x, y, z) of elements of F, the *planes* are given by linear equations $\alpha x + \beta y + \gamma z + \delta = 0$ with coefficients in F (and $\alpha = \beta = \gamma = 0$ not allowed), and two distinct planes which have a common point intersect in a *line*.

2.2 The group M

Consider the set Γ of all planes $z = ax + by + c$ with $a \neq 0$. With any plane λ in Γ we may associate a map $\lambda_* : \Delta_\circ \longrightarrow \Delta_\circ$ given by

$$\lambda_*(x, y, z) = (ax + by + c, y, ax + by + c),$$

where $\Delta_\circ$ is the plane $z = x$, considered as a set of points. If μ, with equation $z = \alpha x + \beta y + \gamma$, also belongs to Γ then the composite map $\lambda_* \mu_*$ given by

$$\lambda_*\mu_*(x, y, x) = (a\alpha x + (a\beta + b)y + a\gamma + c, y, a\alpha x + (a\beta + b)y + a\gamma + c)$$

corresponds to the plane $z = a\alpha x + (a\beta + b)y + a\gamma + c$, which we denote by $\lambda\mu$.

The set Γ, together with the binary operation on Γ which sends (λ, μ) to $\lambda\mu$, is a group. The group Γ is isomorphic to the subgroup M of GL$(3, F)$ consisting of all the matrices of the form

$$M(a, b, c) = \begin{pmatrix} a & b & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $a, b, c \in F$ and $a \neq 0$. It is also isomorphic to the group consisting of all those affine transformations of AG$(2, F)$ which fix every line parallel to the x axis.

2.3 The cube C(S)

Suppose that S is a subset of the finite field F, with $|\mathrm{S}| \geq 2$. Then $\mathrm{S}^3 = \mathrm{S} \times \mathrm{S} \times \mathrm{S}$ is a subset of the point set F^3 of AG$(3, F)$. The geometric structure of AG$(3, F)$ induces a certain geometric structure on S^3. A *point* in this structure is an element of S^3; a *line* is the intersection with S^3 of a line of AG$(3, F)$ which contains at least two points of S^3; and a *plane* is the intersection with S^3 of a plane of AG$(3, F)$ which contains three non-collinear points of S^3.

This induced geometric structure on S^3 is a (very special) example of a geometric lattice. The set S^3 also has its structure as a Cartesian product. We denote the set S^3, endowed with these two structures, by C(S). Our definition in §3.2 of an abstract *finite cube* will be based on some of the properties of C(S).

2.4 Remark

We proceed to show how the geometric structure of C(S), together with the structure of S^3 as a Cartesian product, gives rise to a certain algebraic structure (including a group which is isomorphic to some, possibly trivial, subgroup of $\mathit{\Gamma}$). This algebraic structure will be constructed in what may seem an unnecessarily indirect manner in order to show that it can be obtained without direct use of the embedding of C(S) in AG$(3, F)$. We only use the embedding to establish *properties* of the algebraic structure.

In our definition of a *rigid* finite cube in §4.1, the algebraic structure is assumed to be given. We do *not* claim that it can necessarily be obtained by the construction described in §§2.5–2.7 below. Nevertheless, this construction shows how the algebraic structure assumed in §4.1 *can* be obtained (without using the embedding of C(S) in AG$(3, F)$) in the case of a cube C(S) which is 'dense' (cf. §2.9) in AG$(3, F)$.

2.5 The planes of C(S)

We are especially interested in the planes of C(S) which belong to the set

$$\Gamma = \{\lambda | \lambda \text{ is a plane in C(S) and } \lambda = \lambda_0 \cap \mathrm{S}^3 \text{ for some } \lambda_0 \in \mathit{\Gamma}\}.$$

Associated with Γ is the subset $\Gamma_0 = \{\lambda_0 \in \mathit{\Gamma} | \lambda_0 \cap \mathrm{S}^3 \in \Gamma\}$ of $\mathit{\Gamma}$. We note that $\Delta = \Delta_0 \cap \mathrm{S}^3$ belongs to Γ, and that there is a 1–1 correspondence betweeen planes λ in Γ and planes λ_0 in Γ_0.

Since $\lambda \in \Gamma$ if and only if λ is a plane of C(S) which contains no line $x(v, w) = \{(u, v, w) | u \in \mathrm{S}\}$ and no line $z(u, v) = \{(u, v, w) | w \in \mathrm{S}\}$, Γ may be determined purely from knowledge of the internal structure of C(S).

2.6 The maps λ_*

Let us associate with each λ in Γ a bijective map $\lambda_* : D(\lambda) \longrightarrow R(\lambda)$, where

$$D(\lambda) = \{(u, v, u) \in \Delta | (u, v, w) \in \lambda \text{ for some } w \in \mathrm{S}\},$$
$$R(\lambda) = \{(w, v, w) \in \Delta | (u, v, w) \in \lambda \text{ for some } u \in \mathrm{S}\},$$

and $\lambda_*(u, v, u) = (w, v, w) \Leftrightarrow (u, v, w) \in \lambda$. If $\lambda, \mu \in \Gamma$ and R(λ) overlaps suitably with D(μ) then there is a unique plane $\lambda \circ \mu$ in Γ such that

$$(u, v, w) \in \lambda \circ \mu \quad \text{whenever } (\lambda_* \mu_*)(u, v, u) = (w, v, w);$$

furthermore, under these conditions, the plane $(\lambda \circ \mu)_0$ in Γ_0 corresponding to $\lambda \circ \mu$ is $\lambda_0 \mu_0$, where $\lambda_0 \mu_0$ is the product of λ_0 and μ_0 in the group $\mathit{\Gamma}$.

2.7 The group G

Consider the set $\mathrm{Core}(\Gamma) = \{\lambda \in \Gamma | \lambda \circ \mu \text{ and } \mu \circ \lambda \text{ both exist for all } \mu \in \Gamma\}$. Note that $\mathrm{Core}(\Gamma) \neq \emptyset$ since $\Delta \in \mathrm{Core}(\Gamma)$. We define 'left to right' and 'right to left' products $lr(\lambda_1, \ldots, \lambda_n)$ and $rl(\lambda_1, \ldots, \lambda_n)$, for $\lambda_1, \ldots, \lambda_n \in \mathrm{Core}(\Gamma)$, as follows. If $n = 1$ then both products equal λ_1, while if $n > 1$ then $lr(\lambda_1, \ldots, \lambda_n) = lr(\lambda_1, \ldots, \lambda_{n-1}) \circ \lambda_n$ and $rl(\lambda_1, \ldots, \lambda_n) = \lambda_1 \circ rl(\lambda_2, \ldots, \lambda_n)$. Let us denote by G the subset of Γ obtained from $\mathrm{Core}(\Gamma)$ by forming all such products. Note that $G \supseteq \mathrm{Core}(\Gamma)$.

It is easily checked that $G_0 = \{\lambda_0 \in \boldsymbol{\Gamma} | \lambda_0 \cap \mathbf{S}^3 \in G\}$ is a subgroup of the group $\boldsymbol{\Gamma}$. Also, by the last remark in §2.6, $lr(\lambda_1, \ldots, \lambda_n) = rl(\lambda_1, \ldots, \lambda_n)$ whenever $\lambda_1, \ldots, \lambda_n \in \mathrm{Core}(\Gamma)$. We can therefore extend $\circ$ as follows. If $\lambda \in G$ and $\mu \in \Gamma$, choose $\lambda_1, \ldots, \lambda_n \in \mathrm{Core}(\Gamma)$ such that $lr(\lambda_1, \ldots, \lambda_n) = \lambda$, and let

$$\lambda \circ \mu = rl(\lambda_1, \ldots, \lambda_n, \mu) \text{ and } \mu \circ \lambda = lr(\mu, \lambda_1, \ldots, \lambda_n).$$

Then, by the remark in §2.6 again, $\lambda \circ \mu$ and $\mu \circ \lambda$ are well defined, G is a group (isomorphic to G_0) with respect to the restriction of $\circ$ to $G \times G$, and $(\lambda \circ \mu) \circ \nu = \lambda \circ (\mu \circ \nu)$ whenever $\lambda, \mu, \nu \in \Gamma$ and at least two of λ, μ, ν belong to G.

We may regard $\circ$ as a map from $\Omega = (G \times \Gamma) \cup (\Gamma \times G)$ to Γ.

2.8 The triple $(\Gamma, G, \circ)$

The triple $(\Gamma, G, \circ)$ is the 'algebraic structure' promised in §2.4. If $|\mathbf{S}| = 2$ and $|F|$ is odd then $|\Gamma| = 10$, $G = \{\Delta\}$ is the trivial group and $\circ$ is given by $\lambda \circ \Delta = \lambda = \Delta \circ \lambda$ for all $\lambda \in \Gamma$. At the other extreme, if $|\mathbf{S}| = |F|$ then $\mathrm{C}(\mathbf{S}) = \mathrm{AG}(3, F)$, $G = \Gamma = \boldsymbol{\Gamma}$ and $\circ$ is the group operation in $\boldsymbol{\Gamma}$, as defined in §2.2.

In any case, G is always isomorphic to the subgroup G_0 of $\boldsymbol{\Gamma}$, and $\circ$ corresponds to the map obtained when the group operation of $\boldsymbol{\Gamma}$, considered as a map from $\boldsymbol{\Gamma} \times \boldsymbol{\Gamma}$ to $\boldsymbol{\Gamma}$, is restricted to $\Omega_0 = (G_0 \times \Gamma_0) \cup (\Gamma_0 \times G_0)$. Note that $G_0 \subseteq \Gamma_0 \subseteq \boldsymbol{\Gamma}$; and that, whereas G_0 is always a subgroup of $\boldsymbol{\Gamma}$, Γ_0 need not be a subgroup of $\boldsymbol{\Gamma}$. However, Γ_0 *is* closed under multiplication (on the left or right) by elements of G_0.

2.9 Dense cubes in $\mathrm{AG}(3, F)$

We know that $G \cong G_0 \leq \boldsymbol{\Gamma}$ and (cf. §2.2) that $\boldsymbol{\Gamma} \cong \mathbf{M}$. Let $f = |F|$. Then, provided $f > 2$, $\mathbf{M}$ is a Frobenius group of order $(f-1)f^2$ with kernel $\mathbf{K}$ and complement $\mathbf{H}$, where

$$\mathbf{K} = \{M(a, b, c) \in \mathbf{M} | a = 1\} \text{ and } \mathbf{H} = \{M(a, b, c) \in \mathbf{M} | b = c = 0\}.$$

Moreover $|\mathbf{H}| = f - 1$ and $|\mathbf{K}| = f^2$.

By imposing suitable conditions on the size of G (in relation to the size of $\mathbf{M}$) we can ensure that G is also a Frobenius group. The conditions we shall choose are designed in fact to ensure as well that it is possible to reconstruct the embedding of $\mathrm{C}(\mathbf{S})$ in its enveloping space $\mathrm{AG}(3, F)$ from a knowledge of just the triple $(\Gamma, G, \circ)$, the structure of $\mathrm{C}(\mathbf{S})$ as a geometric lattice and the structure of the point set $\mathbf{S}^3$ as a Cartesian product. That such a reconstruction is possible, when $\mathrm{C}(\mathbf{S})$ is 'dense' in $\mathrm{AG}(3, F)$, is a consequence of our main theorem (cf. §6.16).

We remark that the axiom $\mathbf{B}$ to be introduced in §5.1 derives its usefulness from the truth of the simple lemma stated and proved in §5.2. The hypotheses $v \leq 5u$ and $uv \neq 18$ of that lemma correspond to the requirements $|G| \geq \frac{1}{5}f^3$ and $|G| \neq 162$ in the definition below. (Note that $18 = 2 \times 9$ and $162 = 2 \times 9^2$.) The further requirements $f > 3$, $|G| \neq 16, 25$ are suggested by the lemma to be proved in §2.10.

In view of these considerations, we shall say that $\mathrm{C}(\mathbf{S})$ is *dense* in $\mathrm{AG}(3, F)$ if

$$|G| \geq \tfrac{1}{5} f^3, f > 3 \text{ and } |G| \neq 16, 25, 162.$$

Note that $\mathrm{AG}(3, F)$ is dense in itself whenever $|F| > 3$. Our aim for the rest of this section is to obtain a reasonably detailed description of the algebraic structure $(\Gamma, G, \circ)$, and its relation to $\mathrm{C}(\mathbf{S})$, for the case where $\mathrm{C}(\mathbf{S})$ is dense in $\mathrm{AG}(3, F)$. This description will be the basis of our definition in §6.1 of an (abstract) 'perfect finite cube'.

2.10 Lemma

If $X \leq \mathbf{M}, |X| \geq \frac{1}{5} f^3$, $f > 3$ and $|X| \neq 16, 25$ then X properly contains the Frobenius kernel $\mathbf{K}$ of $\mathbf{M}$.

Proof. We begin by observing that X is conjugate in $\mathbf{M}$ to a subgroup $W = UV$ with $U \leq \mathbf{H}, V \leq \mathbf{K}$ and $|W| = |X| \geq \frac{1}{5} f^3$. Since $U < \mathbf{H}$ and $V < \mathbf{K}$ would imply $|W| = |U|.|V| \leq \frac{1}{6}(f-1)f^2 < \frac{1}{5} f^3$, either $U = \mathbf{H}$ or $V = \mathbf{K}$. Actually we must have $V = \mathbf{K}$. For suppose that $U = \mathbf{H}$. Then $|H|$ divides $|V| - 1$, since W is a Frobenius group with complement $\mathbf{H}$ and kernel V. Moreover $|V|$ divides f^2, $|\mathbf{H}| = f - 1$ and f is a prime power. It follows that either $|V| = f$ or $|V| = f^2$. But $|V| = f$ is not possible, since $|W| \geq \frac{1}{5} f^3$ and $f > 3$. Therefore $|V| = f^2$ and $V = \mathbf{K}$.

Since $W = UV$ it follows that $W \supseteq \mathbf{K}$. However X is conjugate to W and $\mathbf{K} \lhd \mathbf{M}$. We conclude that $X \supseteq \mathbf{K}$. Moreover $|X| \neq \mathbf{K}$ since $|X| \geq \frac{1}{5} f^3$, $f > 3$ and $|X| \neq 16, 25$.

2.11 The group G_0 when the cube is dense

Assuming that $\mathrm{C}(\mathbf{S})$ is dense in $\mathrm{AG}(3, F)$, let $X =$ the image of G_0 under the isomorphism from $\varGamma$ to $\mathbf{M}$ which sends the plane $z = ax + by + c$ to $M(a, b, c)$. Then X satisfies the hypotheses of the above lemma and so $X \supset \mathbf{K}$. It follows that, for some fixed $\varrho \in F \backslash \{0, 1\}$,

$$X = \{M(a, b, c) \in \mathbf{M} | a = \varrho^r \text{ for some integer } r\}.$$

Naturally, G_0 consists of the corresponding set of planes in $\mathrm{AG}(3, F)$.

2.12 The triple $(\Gamma, G, \circ)$ of a dense cube

From the above description of G_0 we deduce (assuming still that $\mathrm{C}(\mathbf{S})$ is dense in $\mathrm{AG}(3, F)$) that G is a Frobenius group, that the Frobenius complements in G are abelian (indeed cyclic) and that if K is the kernel of G then $|G| \geq \frac{1}{5}|K|^{3/2}$. We also deduce the following rather complicated but easily checked property (cf. $\mathbf{R}8$ in §4.1):

If $(\lambda, \mu), (\lambda, \nu) \in \varOmega$, $(u, v, u) \in \mu$, $(w, v, w) \in \nu$, $\mu \cap \Delta \not\supseteq \{(s, v, s) | s \in \mathbf{S}\}$ and $\mu \circ \alpha = \nu \circ \lambda$ then $(u, v, w) \in \lambda$.

Another easily checked consequence of our description of G_0 is that, if l is any line of $\mathrm{C}(\mathbf{S})$ contained in the plane Δ then there is at least one plane in $G \backslash \{\Delta\}$ which contains l.

Finally we remark that, since $G_0 \subseteq \Gamma_0 \subseteq \varGamma$ and $G_0 \trianglelefteq \varGamma$, if $\lambda \in \Gamma$ and $\alpha \in G$ then there is a unique plane $\lambda(\alpha)$ in G such that $\lambda \circ \alpha = \lambda(\alpha) \circ \lambda$.

3 Abstract Finite Cubes

3.1 The points, lines and planes of C

We assume from now on that S denotes a fixed set. As usual, S^3 denotes the Cartesian product $S \times S \times S$. The structure of S^3 as a Cartesian product will be very important. We assume that certain subsets of S^3 have been designated as *lines* and that certain other subsets of S^3 have been designated as *planes*. By a *point* we mean an element of S^3.

The triple consisting of S^3, the set of all lines and the set of all planes will be denoted by C throughout.

3.2 Definition

We shall call the triple C, defined as in §3.1, a *finite cube* if it satisfies the nine conditions listed below.

C1 S is a finite set and $|S| \geq 2$.

C2 Given any two points p and q, there is a unique line $p \vee q$ which contains both p and q.

C3 Given any three non-collinear points p,q and r, there is a unique plane $p \vee q \vee r$ which contains all of p, q, r.

C4 If a plane contains two points p and q then it also contains the line $p \vee q$.

C5 Every line contains at least two points and every plane contains at least one set of three non-collinear points.

C6 If λ is a plane then each of the sets $\lambda' = \{(u, v, w) \in S^3 | (w, v, u) \in \lambda\}$ and $\lambda'' = \{(u, v, w) \in S^3 | (v, u, w) \in \lambda\}$ is a plane.

C7 If λ is a plane and $(a, b, c) \in \lambda$ and $\{(u, v, w) | u \in S\} \subseteq \lambda$ for some $v, w \in S$ then $\{(u, b, c) | u \in S\} \subseteq \lambda$.

C8 If $a \in S$ then $\{(a, v, w) | v, w \in S\}$ is a plane.

C9 $\Delta = \{(u, v, w) \in S^3 | u = w\}$ is a plane.

It is easily checked that C(S), as defined in §2.3, is always a finite cube. In particular, taking $\mathrm{S} = F$, $\mathrm{AG}(3, F)$ itself is a finite cube.

From now on we assume that C is a finite cube.

3.3 The lattice of flats of C

The finite cube C gives rise to a geometric lattice of rank 4, with flats: the empty set, the points, lines and planes of C, and the set S^3 itself. Thus, for example, if l is a line and p is a point not on l then by C3–5 there is a unique plane $l \vee p$ which contains both l and p.

We shall sometimes find it convenient to denote the intersection $\alpha \cap \beta$ of two flats α and β by $\alpha \wedge \beta$.

3.4 The x-planes and x-lines

By C6,8 if $a, b, c \in S$ then each of the sets

$$\begin{aligned} x(a) &= \{(u, v, w) \in S^3 | u = a\}, \\ y(b) &= \{(u, v, w) \in S^3 | v = b\} \text{ and} \\ z(c) &= \{(u, v, w) \in S^3 | w = c\} \end{aligned}$$

is a plane. We call these planes *x-planes*, *y-planes* and *z-planes* respectively. By C1–4 each of the sets $y(b) \cap z(c)$, $z(c) \cap x(a)$, $x(a) \cap y(b)$ is a line. We call these lines *x-lines*, *y-lines* and *z-lines* respectively.

By C6,7 every plane which contains an x-line, a y-line or a z-line is a union of x-lines, y-lines or z-lines (respectively); that is, if λ is such a plane and $p \in \lambda$ then λ contains the unique x-line, y-line or z-line (respectively) which passes through p.

3.5 The line d

The set $\Delta'' = \{(u, v, w) \in S^3 | v = w\}$ is a plane, by C6,9. It follows that the 'diagonal' of S^3, that is

$$d = \Delta \cap \Delta'' = \{(u, v, w) \in S^3 | u = v = w\},$$

is a line.

3.6 Ordinary planes, ordinary lines and the sets Kax, Hax

We call a line l an *ordinary line* if it is neither an x-line nor a z-line; and we call a plane λ an *ordinary plane* if it contains no x-lines and no z-lines, i.e. if every line contained in λ is an ordinary line. We write:

$$\begin{aligned} \Gamma &= \text{the set of all ordinary planes, and} \\ L &= \text{the set of all ordinary lines.} \end{aligned}$$

Note that $\Delta \in \Gamma$. The points and lines contained in Δ are also of special interest, and we will see later (cf. §§4.7–4.9) that those lines contained in Δ of the form $y(b) \cap \Delta$ play a different rôle from the rest. As we shall frequently be thinking of the lines contained in Δ as 'axes' for the pencils of planes containing them, let us use the following notation:

$$\begin{aligned} L(\Delta) &= \{l \in L | l \subset \Delta\}, \\ Kax &= \{k \in L(\Delta) | k = y(b) \text{ for some } b \in S\}, \text{ and} \\ Hax &= \{h \in L(\Delta) | h \notin Kax\}. \end{aligned}$$

Note that if $p = (a, b, a) \in \Delta$, then exactly one of the lines of $L(\Delta)$ passing through p belongs to Kax, namely the line $y(b) \cap \Delta$; the rest, including the line $x(a) \cap \Delta$, belong to Hax. Note also that $d \in Hax$.

3.7 Proposition

Every point of C lies on at least two ordinary lines, and if $|S| > 2$ then every line of C is contained in at least two ordinary planes.

Proof. If $p = (a, b, c) \in S^3$ then, since $|S| \geq 2$, there is a point $q = (u, v, w) \in S^3$ with $u \neq a, v \neq b, w \neq c$. The y-line through p, and the line $p \vee q$, both belong to L. It is not difficult to see that if $|S| > 2$ then every line is contained in at least four planes, of which (by C6,7) at most two are non-ordinary.

3.8 The reconstruction of C from S and Γ

If $|S| > 2$ then the ordinary lines of C are just the intersections of pairs of planes in Γ which have more than one common point, and the x-lines and z-lines are determined by S^3 alone. Using C6—8 we see that the non-ordinary planes are determined once all the lines are known.

If $|S| = 2$ we do not even need to know Γ to determine the lines, and so C is still determined once S and Γ are known.

3.9 The maps λ_* associated with C

With each plane λ in Γ we may (cf. §2.6) associate a map $\lambda_* : D(\lambda) \longrightarrow R(\lambda)$, where

$$D(\lambda) = \{(u,v,u) \in \Delta | (u,v,w) \in \lambda \text{ for some } w \in \mathbf{S}\},$$
$$R(\lambda) = \{(w,v,w) \in \Delta | (u,v,w) \in \lambda \text{ for some } u \in \mathbf{S}\},$$

and $\lambda_*(u,v,u) = (w,v,w) \Leftrightarrow (u,v,w) \in \lambda$. The assumption that λ contains no x-line and no z-line guarantees that λ_* is well defined and bijective.

4 Rigid Cubes

4.1 Definition

We say the finite cube C is *rigid* if there exists a subset G of Γ and a map

$$\circ : \Omega = (\Gamma \times G) \cup (G \times \Gamma) \longrightarrow \Gamma$$

satisfying the eight conditions listed below. Here Γ denotes as usual the set of all ordinary planes (cf. §3.6); and we write $\lambda \circ \mu$ instead of $\circ(\lambda, \mu)$ when the latter is defined, i.e. $(\lambda, \mu) \in \Omega$.

R1 $\Delta \in G$, and $\alpha' \in G$ whenever $\alpha \in G$.

R2 If $l \in L(\Delta)$ then there are at least two planes in G which contain l.

R3 The restriction of $\circ$ to the subset $G \times G$ of Ω is a group operation on G.

R4 If $\lambda \in \Gamma \backslash G$ and $\alpha, \beta \in G$ then $\lambda \circ \alpha = \lambda \circ \beta \Rightarrow \alpha = \beta$, $\alpha \circ \lambda = \beta \circ \lambda \Rightarrow \alpha = \beta$, $\lambda \circ (\alpha \circ \beta) = (\lambda \circ \alpha) \circ \beta$, $(\alpha \circ \beta) \circ \lambda = \alpha \circ (\beta \circ \lambda)$ and $(\alpha \circ \lambda) \circ \beta = \alpha \circ (\lambda \circ \beta)$.

R5 If $\lambda \in \Gamma \backslash G$ and $\alpha \in G$ then there is a unique element $\lambda(\alpha)$ of G such that $\lambda \circ \alpha = \lambda(\alpha) \circ \lambda$.

R6 If $(\lambda, \mu) \in \Omega$ and $\lambda_* \mu_*(u,v,u) = (w,v,w)$ then $(u,v,w) \in \lambda \circ \mu$.

R7 If $\lambda \in \Gamma \backslash G, \alpha \in G$ and $\lambda_* \alpha_* \lambda_*{}^{-1}(u,v,u) = (w,v,w)$ then $(u,v,w) \in \lambda(\alpha)$.

R8 If $(\lambda, \mu), (\lambda, \nu) \in \Omega, (u,v,u) \in \mu, (w,v,w) \in \nu$, $\mu \cap \Delta \not\supseteq y(v) \cap \Delta$ and $\lambda \circ \mu = \nu \circ \lambda$ then $(u,v,w) \in \lambda$.

It can be checked that if C(S) is dense in AG$(3, F)$ then it is rigid according to this definition. Also AG$(3, F)$ itself is a rigid cube whenever $|F| \geq 3$.

We assume from now on that C is a rigid cube, and we shall write $\lambda\mu$ instead of $\lambda \circ \mu$ when $(\lambda, \mu) \in \Omega$ and use standard group theoretic notation and terminology when discussing the group G guaranteed by **R3**. The identity element of G is the plane Δ (indeed $\lambda\Delta = \lambda = \Delta\lambda$ for all $\lambda \in \Gamma$). The inverse α^{-1} of any element α of G is the plane $\alpha' = \{(a,b,c) \in S^3 | (c,b,a) \in \alpha\}$.

4.2 The map $\Phi : \Gamma \longrightarrow Aut(G)$

If $\alpha \in G$ we shall mean by $\hat{\lambda}(\alpha)$ either the conjugate $\lambda\alpha\lambda^{-1}$ of α in G if $\lambda \in G$ or else, if $\lambda \in \Gamma \backslash G$, the element $\lambda(\alpha)$ of G described in **R5**. Note that in either case

$$\lambda\alpha = \hat{\lambda}(\alpha)\lambda.$$

It is easily checked, using the axioms above, that (for all $\lambda \in \Gamma$) the resulting map $\hat{\lambda} : G \longrightarrow G$ is an automorphism of the group G. Thus we have a map

$$\Phi : \Gamma \longrightarrow Aut(G) \quad \text{given by } \Phi(\lambda) = \hat{\lambda}.$$

It also follows readily from our axioms that $\Phi(\lambda\mu) = \Phi(\lambda)\Phi(\mu)$ whenever $(\lambda, \mu) \in \Omega$.

4.3 Special subsets of Γ

If $\Psi \subseteq \Gamma$, p is a point and l is a line then we may consider the following subsets of Γ:

$$\Psi^* = \Psi \backslash \{\Delta\},\ \Psi(p) = \{\lambda \in \Psi | \lambda \ni p\} \text{ and } \Psi(l) = \{\lambda \in \Psi | \lambda \supset l\}.$$

Of special interest are the sets $G(p)$ and $\Gamma(p)$, especially when $p \in \Delta$; and the sets $G(l)$ and $\Gamma(l)$, especially when $l \subset \Delta$, i.e. $l \in L(\Delta)$. It is easily checked, using **R6** in particular, that if $p \in \Delta$ then $G(p)$ is a subgroup of G and also that if $l \in L(\Delta)$ then $G(l) < G$. Also, by **R2**, $|G(l)| \geq 2$ whenever $l \in L(\Delta)$. If $p \in l$ and $l \in L(\Delta)$ then

$$1 < G(l) < G(p) < G.$$

4.4 Proposition

If $u, v, w \in S$, $p = (u, v, u)$, $q = (w, v, w)$, $\lambda \in \Gamma$ and $\alpha \in G$ then :

(i) $\hat{\lambda}(G(p)) = G(q) \Leftrightarrow (u, v, w) \in \lambda$, and
(ii) $\alpha\Gamma(p)\alpha^{-1} = \Gamma(q) \Leftrightarrow (u, v, w) \in \alpha$.

Proof. Suppose first that $(u, v, w) \in \lambda$. Let $\beta \in G^*(p)$, $\gamma \in G^*(q)$ and $\mu = \lambda^{-1} = \lambda'$. Then

$$\lambda_*\beta_*\lambda_*{}^{-1}(w, v, w) = \lambda_*\beta_*(u, v, u) = \lambda_*(u, v, u) = (w, v, w),$$

and so $\hat{\lambda}(\beta) \in G(q)$ by **R5,6,7**. Similarly $\hat{\mu}(\gamma) \in G(p)$. Thus $\hat{\lambda}(G(p)) \subseteq G(q)$ and $\hat{\mu}(G(q)) \subseteq G(p)$, whence $\hat{\lambda}(G(p)) = G(q)$. Conversely, suppose $\hat{\lambda}(G(p)) = G(q)$. Choose $\beta \in G^*(x(u) \cap \Delta)$ and let $\gamma = \hat{\lambda}(\beta)$. Then $\lambda\beta = \gamma\lambda$ and so, by **R8**, $(u, v, w) \in \lambda$.

A parallel argument establishes the condition for (u, v, w) to belong to α.

4.5 Proposition

The map $\Phi : \Gamma \longrightarrow Aut(G)$ is injective.

Proof. Suppose $\lambda, \mu \in \Gamma$ and $\Phi(\lambda) = \Phi(\mu)$. Let $(u, v, w) \in \lambda$, $p = (u, v, u)$ and $q = (w, v, w)$. Then $\hat{\lambda}(G(p)) = G(q)$ by §4.4 and therefore $\hat{\mu}(G(p)) = G(q)$. It follows, using §4.4 again, that $(u, v, w) \in \mu$. We have shown that $\lambda \subseteq \mu$. Similarly $\mu \subseteq \lambda$.

4.6 Proposition

If $h \in Hax$ then $\Gamma(h) = \{\lambda \in \Gamma | \lambda G(h) = G(h)\lambda\}$.

Proof. If $\lambda \in \Gamma(h)$ then $\hat{\lambda}(G(p)) = G(p)$ for all $p \in h$ by §4.4, and so $\hat{\lambda}(G(h)) = G(h)$. Conversely, if $\lambda \in \Gamma$ and $\hat{\lambda}(G(h)) = G(h)$, choose $\alpha \in G^*(h)$ and let $\beta = \hat{\lambda}(\alpha)$; then $\beta \in G(h)$ and $\lambda\alpha = \beta\lambda$, and so (by **R**8) $\lambda \supset h$ which means that $\lambda \in \Gamma(h)$.

4.7 Proposition

The group G is a Frobenius group, and if $h \in Hax$ then $G(h)$ is a Frobenius complement in G.

Proof. Since $h \in L(\Delta)$, $1 < G(h) < G$. Moreover using **R**8 we see that $N_G(G(h)) = G(h)$; and that if $\alpha \in G$ then $\alpha G(h)\alpha^{-1} \cap G(h) \neq 1$ implies that $\alpha G(h)\alpha^{-1} = G(h)$. So $G(h)$ is a Frobenius complement in G.

4.8 The Frobenius kernel K and the planes $\tau(h, h')$

We denote the Frobenius kernel of G by K. By §4.7, if $h \in Hax$ then $K \cap G(h) = 1$ and $KG(h) = G$. Also, by the standard results on Frobenius groups (cf. Huppert [1], pp. 495–508), K is a nilpotent characteristic subgroup of G and K acts faithfully, via conjugation, as a sharply transitive permutation group on the set of all Frobenius complements of G. If $h, h' \in Hax$ then there is a unique element $\tau(h, h')$ of K such that

$$\hat{\tau}(h, h')(G(h)) = G(h').$$

Note that if $\tau = \tau(h, h')$ then, by §4.6, $\tau\Gamma(h)\tau^{-1} = \Gamma(h')$.

4.9 Proposition

If $k \in Kax$ then $G(k)$ is a subgroup of K.

Proof. Now $k = y(a) \cap \Delta$ for some $a \in S$. Let $h = x(a) \cap \Delta$. We show first that $G(k)$ is $\Gamma(h)$-invariant. Let $\lambda \in \Gamma^*(h)$ and $\sigma \in G(k)$, and choose $(u, v, w) \in \lambda \backslash \Delta$. Then $(u, a, w) \in \lambda$ since λ contains the y-line h. Also $w \neq a$ since λ is an ordinary plane; and so $(a, a, a) \vee (w, a, w) = k$. Moreover $\lambda_* \sigma_* \lambda_*{}^{-1}(a, a, a) = (a, a, a)$ and

$$\lambda_* \sigma_* \lambda_*{}^{-1}(w, a, w) = \lambda_* \sigma_*(u, a, u) = \lambda_*(u, a, u) = (w, a, w).$$

It follows by **R**5,6,7 that $\hat{\lambda}(\sigma) \in G(k)$. So $G(k)$ is $\Gamma(h)$-invariant. Now $G(h)$ is a complement in G and K is the kernel. Also $G(h) \cap G(k) = 1$ and $G(k)$ is $G(h)$-invariant. Thus $G(k) \leq K$.

5 Balanced Rigid Cubes

5.1 Definition

We say that the rigid cube C is *balanced* if it satisfies the extra condition:

B If $p \in d$ then $|G(p) \cap K| \leq 5|G(d)|$ and $|G(p) \cap K|.|G(d)| \neq 18$.

Here K denotes as usual the kernel of G (cf. §4.8) and d denotes the 'diagonal' of C (cf. §3.5). It can be checked that C(**S**) is balanced whenever C(**S**) is dense in AG$(3, F)$. Moreover AG$(3, F)$ itself is a balanced rigid cube whenever $|F| \geq 3$.

From now on we assume that C is a balanced rigid cube.

5.2 Lemma

If u, v, v' are integers, $u \geq 2$, $v \geq v' \geq 2$, $u|v-1$, $u|v'-1$, $v'|v$ and $v \leq 5u$ but $uv \neq 18$, then $v' = v$.

Proof. There exist positive integers s and t such that $v' = su+1$ and $v = v't = (su+1)t$. Now $u|t-1$ since $u|v-v' = (su+1)(t-1)$, and therefore $t = wu+1$ for some non-negative integer w. Assume that $t \neq 1$. Then $w \geq 1$ and so $s+w \geq 2$. However $(sw)u + (s+w) < 5$ since $5u \geq v = [(sw)u + (s+w)]u + 1$. It follows that $u = 2$ and $s = w = 1$, and therefore $uv = u(su+1)(wu+1) = 18$, contradicting $uv \neq 18$.

5.3 Proposition

If $k \in Kax$ and $p = k \wedge d$ then :

(i) $G(k)G(d) = G(p)$,
(ii) $G(k)$ is $\Gamma(d)$-invariant, and
(iii) $G(k)$ has no $G(d)$-invariant subgroups other than $\{\Delta\}$ and $G(k)$.

Proof. Let $k = y(a) \cap \Delta$ and $h = x(a) \cap \Delta$. Now $G(p)$ is a Frobenius group, since $G(h) < G(p) < G$ and $G(h)$ is a Frobenius complement in G; and $G(k) \leq G(p) \cap K$ by §4.9. Moreover (by the proof in §4.9) $G(k)$ is $G(h)$-invariant. Applying the Lemma (with $u = |G(h)| = |G(d)|, v = |G(p) \cap K|$ and $v' = |G(k)|$) and axiom **B**, we deduce that $G(k) = G(p) \cap K$.

It follows that $G(p) = G(k)G(d)$. But $G(p)$ is clearly $\Gamma(d)$-invariant (by **R**5–7), and so its kernel $G(k)$ is also $\Gamma(d)$-invariant. Applying the Lemma and axiom **B** again, with $v = |G(k)| = |G(p) \cap K|$, we establish (iii).

5.4 Proposition

If $k \in Kax$ then $G(k) = \Gamma(k)$.

Proof. Suppose $\lambda \in \Gamma^*(k)$, and choose $(u, v, w) \in \lambda \backslash \Delta$. Let $p = k \wedge d$, $h = p \vee (u, v, u)$ and $h' = p \vee (w, v, w)$. Then $h, h' \in Hax$, and $\hat{\lambda}(G(h)) = G(h')$ by §4.4. Now $G(p)$ is a Frobenius group, with kernel $G(k)$; and $G(h)$ and $G(h')$ are both complements in $G(p)$. So $\tau(h, h') \in G(k)$. However $(u, v, w) \in \tau(h, h')$ by **R**8. Therefore $\lambda = k \vee (u, v, w) = \tau(h, h') \in G(k)$.

5.5 Proposition

If $k \in Kax$ then $G(k)$ is an elementary abelian group.

Proof. Consider the derived group $J = [G(k), G(k)]$ of $G(k)$. Observe that $J \neq G(k)$ since $G(k)$, being a Frobenius kernel, is nilpotent; and that J is $G(d)$-invariant, since it is a characteristic subgroup of $G(k)$ and $G(k)$ is $G(d)$-invariant. It follows by §5.3 that $J = 1$. Now let p be any prime divisor of $|G(k)|$. Then $P = \{\sigma \in G(k) | \sigma^p = \Delta\}$ is a subgroup of $G(k)$, since $G(k)$ is abelian. We deduce, using §5.3 again, that $P = G(k)$.

5.6 Proposition

If $k, k' \in Kax$ then $G(k')G(k)$ is an abelian group.

Proof. We may suppose $k \neq k'$. Let $k = y(a) \cap \Delta$, $k' = y(b) \cap \Delta$, choose $u \in S\backslash\{b\}$, let $\sigma = k \vee (u, b, b)$ and let $p = (b, b, b)$. Then $\sigma \in G^*(k)$ by §5.4. If $\rho \in G(k')$ then

$$\sigma_*\rho_*\sigma_*{}^{-1}(b, b, b) = \sigma_*\rho_*(u, b, u) = \sigma_*(u, b, u) = (b, b, b)$$

and therefore, by **R6**, $\sigma\rho\sigma^{-1} \in G(p)$. We have shown that $\hat{\sigma}(G(k')) \subseteq G(p) \cap K = G(k')$ for some $\sigma \in G^*(k)$. Now let $J = G(k) \cap N_G(G(k'))$. Then $J \neq 1$ and J is a $G(d)$-invariant subgroup of $G(k)$; and so, by §5.3, $J = G(k)$, i.e. $G(k) \subseteq N_G(G(k'))$. Similarly $G(k') \subseteq N_G(G(k))$. Since $G(k)$ and $G(k')$ are both abelian groups, it follows that $G(k')G(k)$ is an abelian group.

5.7 Proposition

If $k, k', k'' \in Kax$ and k, k', k'' are distinct, then $G(k'') \subset G(k')G(k)$.

Proof. Let $k = y(a) \cap \Delta$, $k' = y(b) \cap \Delta$, $k'' = y(c) \cap \Delta$, $\rho = k \vee (a, c, b)$, $\sigma = k' \vee (b, c, a)$ and $p = (b, c, b)$. Then $\rho \in G^*(k)$, $\sigma \in G^*(k')$ and $\rho_*\sigma_*(b, c, b) = \rho_*(a, c, a) = (b, c, b)$, so that $\rho\sigma \in G(p) \cap K = G(k'')$. Moreover $\rho\sigma \neq \Delta$ since $G(k) \cap G(k') = 1$. Let $J = G(k'') \cap G(k')G(k)$. Then $J \neq 1$ and therefore, since J is $G(d)$-invariant, $J = G(k'')$ by §5.3.

5.8 Proposition

If $k, k' \in Kax$ and $k \neq k'$ then $K = G(k')G(k)$.

Proof. Let $\sigma \in K$ and choose $(u, v, w), (u', v', w') \in \sigma$ with $v \neq v'$. Let $p = (u, v, u)$, $q = (w, v, w)$, $p' = (u', v', u')$, $q' = (w', v', w')$, $h_1 = p \vee p'$, $h_2 = p' \vee q$, $h_3 = q \vee q'$, $k_1 = y(v) \cap \Delta$ and $k_2 = y(v') \cap \Delta$. Then $h_1, h_2, h_3 \in Hax$, $\hat{\sigma}(G(h_1)) = G(h_3)$, $G(p') = G(k_2)G(h_1) = G(k_2)G(h_2)$ and $G(q) = G(k_1)G(h_2) = G(k_1)G(h_3)$. It follows that $\sigma = \tau(h_1, h_3)$, that $\tau(h_1, h_2) \in G(k_2)$ and that $\tau(h_2, h_3) \in G(k_1)$; and therefore $\sigma = \tau(h_2, h_3)\tau(h_1, h_2) \in G(k_1)G(k_2)$. Using §5.6 and §5.7 we conclude that $\sigma \in G(k')G(k)$.

Remark. We have now completely determined the structure (as a group) of the Frobenius kernel K of G. It is an elementary abelian group. Moreover, for all $k \in Kax$, $G(k)$ is a subgroup of K and $|G(k)|^2 = |K|$.

5.9 Proposition

$\Gamma = K\Gamma(d)$.

Proof. Let $\lambda \in \Gamma$, choose $(u, v, w) \in \lambda$ and let $p = (u, v, u)$. Also choose $b \in S\backslash\{v\}$ and let $\rho = (y(b) \cap \Delta) \vee (w, v, u)$. Then $\rho \in K$ by §4.9 and §5.4; and $\mu = \rho\lambda \in \Gamma(p)$, since $\rho_*\lambda_*(u, v, u) = (u, v, u)$. Now choose $(u', v', w') \in \mu\backslash y(v)$, let $p' = (u', v', u')$ and let $\sigma = (y(v') \cap \Delta) \vee (w', v', u')$. Then $\sigma \in K$ and $\nu = \sigma\mu \in \Gamma(p) \cap \Gamma(p') = \Gamma(h)$, where $h = p \vee p' \in Hax$. Let $\tau = \tau(h, d)$. Then $\tau\Gamma(h) = \Gamma(d)\tau$ (cf. §4.8). It follows that $\tau\nu = \omega\tau$ for some $\omega \in \Gamma(d)$, and so $\lambda = \rho^{-1}\sigma^{-1}\nu = \rho^{-1}\sigma^{-1}\tau^{-1}\omega\tau \in K\Gamma(d)K$. We conclude that $\Gamma = K\Gamma(d)K$.

Since $\Gamma(d)$ acts on G via the map Φ of §4.2, and K is a characteristic subgroup of G, $\Gamma(d)K = K\Gamma(d)$. Thus $\Gamma = K\Gamma(d)K = KK\Gamma(d) = K\Gamma(d)$.

5.10 Proposition

If $k \in Kax$ and $\rho, \rho' \in G^*(k)$ then $\rho' = \hat{\lambda}(\rho)$ for some $\lambda \in \Gamma(d)$.

Proof. Let $k = y(a) \cap \Delta$, $h = x(a) \cap \Delta$ and $p = (a, a, a)$. Then $\tau = \tau(h, d) \in G^*(k)$. It suffices to show that if $\sigma \in G^*(k)$ then $\hat{\lambda}(\sigma) = \tau$ for some $\lambda \in \Gamma(d)$.

Let $\sigma \in G^*(k)$ and $(u, v, w) \in \sigma \backslash \Delta$. Then $u \neq w$ and $v \neq a$. Let $h_1 = (u, v, u) \vee p$ and $h_2 = (w, v, w) \vee p$. Then $h_1, h_2 \in Hax$ and (by §4.4) $\hat{\sigma}(G(h_1)) = G(h_2)$; and $\hat{\tau}(G(h)) = G(d)$, as $\tau = y(a) \vee (a, v, v)$. Consider the plane $\mu = p \vee (u, v, a) \vee (w, v, v)$. It can be checked that $\mu \in \Gamma$ and that $\hat{\mu}(G(h_1)) = G(h)$ and $\hat{\mu}(G(h_2)) = G(d)$. Now σ is the unique element of K which maps $G(h_1)$ to $G(h_2)$, and τ is the unique element of K which maps $G(h)$ to $G(d)$ (via conjugation). Also $\hat{\mu} \in Aut(G)$ and $\hat{\mu}(K) = K$. So $\hat{\mu}(\sigma) = \tau$ and therefore, by §5.9, $\hat{\lambda}(\sigma) = \tau$ for some $\lambda \in \Gamma(d)$.

6 Perfect Finite Cubes

6.1 Definition

We shall call the balanced rigid cube C a *perfect finite cube* if it satisfies the extra condition

P If $\lambda \in \Gamma(d)$ and $\alpha \in G(d)$ then $\lambda\alpha = \alpha\lambda$.

It has already been remarked (cf. §5.1) that if C(**S**) is dense in AG$(3, F)$ then it is a balanced rigid cube, and it is easily checked (cf. §2.11) that C(**S**) also satisfies our new condition. So every dense cube is perfect. Moreover, AG$(3, F)$ itself is a perfect finite cube whenever $|F| \geq 3$.

Throughout this final section we assume that C is a perfect finite cube. Note that, since every abelian Frobenius complement is cyclic (cf. [1], p. 499), axiom **P** implies that $G(d)$ is a cyclic group. It also implies that if $\lambda \in \Gamma(d)$ then $\hat{\lambda}(\alpha) = \alpha$ for all $\alpha \in \Gamma(d)$.

6.2 The choice of k, k' and k''

Let us arbitrarily *choose* three distinct elements k, k', k'' of Kax. We regard k, k', and k'' as fixed henceforth. Now $k = y(t) \cap \Delta$ and $k' = y(t') \cap \Delta$ for some $t, t' \in S$. We also regard t and t' as fixed from now on, and write:

$$h = x(t) \cap \Delta, \quad h' = x(t') \cap \Delta, \quad \rho_0 = \tau(d, h) \text{ and } \sigma_0 = \tau(d, h').$$

For any $s \in S$, let $h(s) = x(s) \cap \Delta$ and $k(s) = y(s) \cap \Delta$. Note that $h = h(t)$, $h' = h(t')$, $k = k(t)$ and $k' = k(t')$.

6.3 Proposition

The map $\varphi : \Gamma(d) \longrightarrow Aut(G(k))$ given by $\varphi(\lambda) =$ the restriction of $\hat{\lambda}$ to $G(k)$ is injective.

Proof. We begin by noting that there is a unique map $\vartheta : G(k') \longrightarrow G(k)$ such that

(i) $\quad \vartheta(\sigma) = \rho \Leftrightarrow \sigma\rho \in G(k'')$.

Moreover ϑ is an isomorphism. Furthermore, since each of $G(k)$, $G(k')$ and $G(k'')$ is $\Gamma(d)$-invariant,

(ii) $\quad \vartheta(\hat{\lambda}(\sigma)) = \hat{\lambda}(\vartheta(\sigma))$ for all $\lambda \in \Gamma(d)$ and $\sigma \in G(k')$.

Suppose now that $\lambda, \mu \in \Gamma(d)$ and that $\hat{\lambda}(\sigma) = \hat{\mu}(\sigma)$ for all $\sigma \in G(k')$. Then

$$\hat{\lambda}(\sigma'\vartheta(\sigma)\alpha) = \hat{\lambda}(\sigma')\vartheta(\hat{\lambda}(\sigma))\hat{\lambda}(\alpha) = \hat{\mu}(\sigma'\vartheta(\sigma)\alpha)$$

for all $\sigma, \sigma' \in G(k')$ and $\alpha \in G(d)$, by (ii) and axiom **P**. Since $G = KG(d) = G(k')G(k)G(d)$ it follows that $\Phi(\lambda) = \Phi(\mu)$, whence (by §4.5) $\lambda = \mu$.

6.4 Proposition

Each element of Γ may be *uniquely* represented in the form $\sigma\rho\lambda$, where $\sigma \in G(k')$, $\rho \in G(k)$ and $\lambda \in \Gamma(d)$.

Proof. Suppose $\alpha, \beta \in K$, $\lambda, \mu \in \Gamma(d)$ and $\alpha\lambda = \beta\mu$. Then $\varphi(\lambda) = \varphi(\mu)$ since K is abelian and $G(k) \subset K$; and so (by §6.3) $\lambda = \mu$. It follows that $\alpha = \beta$. Now apply §5.8 and §5.9.

6.5 The field F and the maps ε, $\hat{\varepsilon}$ and e

From now on, let $u = |G(d)|$ and $v = |G(k)| = |G(k')| = |G(k'')|$. Note that $|K| = v^2$. Also, since $G(k)$ is elementary abelian (indeed K itself is elementary abelian), $v = p^r$ for some prime p and positive integer r. So there exists a finite field (unique to within isomorphism) of order v. Let us *choose* such a field $F = (F, +, \times)$.

Since the group $(F, +)$ is elementary abelian and $|(F, +)| = v = |G(k)|$, we may also *choose* an isomorphism

$$\varepsilon : G(k) \longrightarrow (F, +).$$

We will adjust the choice of ε in §6.11. Note that ε induces an isomorphism

$$\hat{\varepsilon} : Aut(G(k)) \longrightarrow Aut(F, +) \quad \text{given by } \hat{\varepsilon}(g) = \varepsilon g \varepsilon^{-1}.$$

Another map we will have occasion to use is the map $e : Aut(F, +) \longrightarrow F$ given by $e(\sigma) = \sigma(1)$. Recall also the maps $\varphi : \Gamma(d) \longrightarrow Aut(G(k))$ and $\vartheta : G(k') \longrightarrow G(k)$ introduced in §6.3. We have:

$$G(k') \xrightarrow{\vartheta} G(k) \xrightarrow{\varepsilon} (F, +)$$

and

$$\Gamma(d) \xrightarrow{\varphi} Aut(G(k)) \xrightarrow{\hat{\varepsilon}} Aut(F, +) \xrightarrow{e} F.$$

6.6 The subsets H, H', Σ and Σ' of $A = Aut(G(k))$

The group $Aut(F, +)$ has a cyclic (Singer) subgroup Σ_F consisting of the $v - 1$ maps $\sigma_a : F \longrightarrow F$ given by $\sigma_a(b) = a \times b$. Since $u | v - 1$, Σ_F has a unique subgroup of order u which we denote by H_F. Now consider the subsets

$$H = (\hat{\varepsilon})^{-1}(H_F), \quad H' = \varphi(G(d)), \quad \Sigma = (\hat{\varepsilon})^{-1}(\Sigma_F) \quad \text{and } \Sigma' = \varphi(\Gamma(d))$$

of the group $A = Aut(G(k))$. Observe that $H \leq \Sigma \leq A$, $H' \subseteq \Sigma' \subseteq A$ and $H' \leq A$; and that H and H' are both cyclic groups of order u, since $H \cong H_F$ and $H' \cong G(d)$. (Recall that φ is injective by §6.3; and that $G(d)$ is cyclic, as was remarked in §6.1.) Furthermore $\Sigma' \subseteq C_A(H')$, by axiom **P**.

6.7 Assumed result

If $\sigma \in \Sigma$ and either $r = 1$, or $r > 1$ and the order of σ does not divide $p^j - 1$, for all $j \in \{1, \ldots, r-1\}$, then $C_A(\sigma) = \Sigma$.

Proof. See Huppert [1], p. 187.

6.8 Assumed result

If $r > 1$, $p^r \neq 64$ and either $r \neq 2$ or else $p + 1$ is not a power of 2 then $p^r - 1$ has a prime divisor q such that $q \nmid p^j - 1$ for all $j \in \{1, \ldots, r-1\}$.

Proof. See Huppert and Blackburn [2], p. 508. This result is due to Zsigmondy [5].

6.9 Proposition

H and H' are conjugate in A.

Proof. Let $x = (v-1)/u$ and note that $x \in \{1, \ldots, 4\}$ by axiom **B**.

Case 1: $v \notin \{9, 25, 49, 64\}$. The assertion is trivial when $r = 1$, since then A is cyclic and therefore $H = H'$; so assume $r > 1$. Suppose $r = 2$ and $p = 2^b - 1$. Then $b \geq 4$ since $v \notin \{1, 9, 49\}$. Also $p - 1 = 2(2^{b-1} - 1)$, $p^2 - 1 = 2^{b+1}(2^{b-1} - 1)$, $|A| = (p^2 - 1)p(p-1)$ and the Sylow 2-subgroups of A have order 2^{b+2}. Since $u = (p^2 - 1)/x$ and $x \in \{1, \ldots, 4\}$, H' possesses an element of order 8. The square of this element has order 4, and is conjugate to an element σ of Σ (by the Sylow theorems). By §6.7, $C_A(\sigma) = \Sigma$ since $4 \nmid p - 1$. It follows that H and H' are conjugate in A.

Now suppose that either $r > 2$ or else $p + 1$ is not a power of 2. Then $p^r - 1$ has a prime divisor q such that $q \nmid p^j - 1$ for all $j \in \{1, \ldots, r-1\}$, by §6.8. Note that $q \neq 2$ since $r > 1$. Also, if 3 is the only possible value for q then $r = 2$ (since $3 | p^2 - 1$) and, since $p^2 - 1 = (p-1)(p+1)$ and $\gcd(p-1, p+1) = 2$, the only prime divisors of $p^2 - 1$ are 2 and 3. It follows, since $u = (p^r - 1)/x$ and $x \in \{1, \ldots, 4\}$, that H' possesses an element of order q, unless $r = 2$, $p^2 - 1 = 3 \times 2^b$, $3 \nmid p - 1$ and $x = 3$, in which case it is easily shown that $v \in \{4, 25\}$. But $v \neq 25$ by hypothesis, and if $v = 4$ and $x = 3$ then $u = 1$, which is impossible by **R2**. Therefore H' has an element of order q, and this element is conjugate to an element σ of Σ (since Σ contains a Sylow subgroup of A). Moreover $C_A(\sigma) = \Sigma$ by §6.7. So H and H' are conjugate in A.

Case 2: $v \in \{9, 25, 49, 64\}$. If $u = v - 1$ then the split extensions $G(k)H$ and $G(k)H'$ are isomorphic groups (by a well known theorem of Zassenhaus[4] on sharply 2-transitive permutation groups) and therefore H and H' are conjugate in $A = Aut(G(k))$.

If $(u, v) \in \{(6, 25), (12, 25), (16, 49), (24, 49)\}$ then the Sylow argument used above still works. Recall that $uv \neq 18$ by axiom **B**. We need therefore only consider $(u, v) \in \{(4, 9), (8, 25), (12, 49), (21, 64)\}$. Here we can use standard linear algebra, in particular the Rational Decomposition Theorem, to deal with each case separately. Suppose for example that $(u, v) = (21, 64)$. Over a field of order 2 the polynomial $x^{21} - 1$ factorizes as

$$(x+1)(x^2+x+1)(x^3+x^2+1)(x^3+x+1)(x^6+x^5+x^4+x^2+1)(x^6+x^4+x^2+x+1).$$

It follows that the minimum polynomial for a generator of H' is either $x^6+x^5+x^4+x^2+1$ or $x^6 + x^4 + x^2 + x + 1$. Now $x^6 + x^4 + x^2 + x + 1 = x^6(x^{-6} + x^{-5} + x^{-4} + x^{-2} + 1)$. So in either case H and H' are conjugate in A.

6.10 Proposition

$\Sigma = C_A(H)$ and $\Sigma' = C_A(H')$.

Proof. If $r > 1$ then $u \not| p^j - 1$ for all $j \in \{1, \ldots, r-1\}$, since $(p^r - 1)/u \in \{1, \ldots, 4\}$ and $uv \neq 18$. It follows by §6.7 that $C_A(H) = \Sigma$. Now $|\Sigma'| = |\Gamma(d)| \geq v - 1$ by §5.10 and §6.3. Also $\Sigma' \subseteq C_A(H')$ and H' is conjugate to H. So $\Sigma' = C_A(H')$.

6.11 The map j

By §6.9 and §6.10, we may assume that the isomorphism $\varepsilon : G(k) \longrightarrow (F, +)$ is chosen in such a way that

$$\hat{\varepsilon}(\varphi(\Gamma(d)) = \hat{\varepsilon}(\Sigma') = \Sigma_F.$$

Recall from §6.4 that each element of Γ may be uniquely represented in the form $\sigma\rho\lambda$, where $\sigma \in G(k')$, $\rho \in G(k)$ and $\lambda \in \Gamma(d)$. Recall also the definition of the group $\mathbf{M}$ given in §2.2. Let us consider the map $j : \Gamma \longrightarrow \mathbf{M}$ given by the rule

$$j(\sigma\rho\lambda) = M(a, 1 - a + b_0 b - c_0 c, c_0 c),$$

where $a = e\hat{\varepsilon}\varphi(\lambda)$, $b = \varepsilon(\rho)$, $c = \varepsilon\vartheta(\sigma)$, the constant b_0 is determined by the requirement that $j(\rho_0) = M(1, -1, 0)$ and the constant c_0 by the requirement that $j(\sigma_0) = M(1, -1, 1)$.

6.12 Proposition

The map $j : \Gamma \longrightarrow \mathbf{M}$ is a bijection, and $j(\mu\nu) = j(\mu)j(\nu)$ for all $(\mu, \nu) \in \Omega$.

Proof. Recall that ε, $\hat{\varepsilon}$ and ϑ are all isomorphisms, that φ is injective and that $\hat{\varepsilon}(\varphi(\Gamma(d))) = \Sigma_F$. Moreover $|\Gamma| = (v-1)v^2 = |\mathbf{M}|$. So j is clearly bijective. Suppose $\mu = \sigma_1\rho_1\lambda_1$ and $\nu = \sigma_2\rho_2\lambda_2$. Then $\mu\nu = \sigma_1\rho_1\hat{\lambda_1}(\sigma_2)\lambda_1\rho_2\lambda_2 = \sigma_1\rho_1\hat{\lambda_1}(\sigma_2)\hat{\lambda_1}(\rho_2)\lambda_1\lambda_2 = (\sigma_1\hat{\lambda_1}(\sigma_2))(\rho_1\hat{\lambda_1}(\rho_2))(\lambda_1\lambda_2)$. Straightforward calculations, using the definition of j, the property §6.3(ii) and the multiplication rule for $\mathbf{M}$, now show that $j(\mu\nu) = j(\mu)j(\nu)$.

6.13 The map i and the set $\mathbf{S}$

We observe that $j(\Gamma(d)) = \{M(a, 1-a, 0) | a \in F^*\}$, $j(\Gamma(h)) = j(\rho_0\Gamma(d))\rho_0{}^{-1}) = \{M(a, 0, 0) | a \in F^*\}$ and $j(\Gamma(h')) = j(\sigma_0\Gamma(d)\sigma_0{}^{-1}) = \{M(a, 0, 1-a) | a \in F^*\}$, where $F^* = F \backslash \{0\}$.

Now let $s \in S$ and choose $\tau \in G^*(k(s))$. Then $j(\tau) = M(1, b, c)$ for some $b, c \in S$. By §5.10, $j(G^*(k(s))) = j\{\hat{\lambda}(\tau) | \lambda \in \Gamma(d)\} = \{M(1, ab, ac) | a \in F^*\}$. Observe that $b \neq 0$, since otherwise $\tau(h, h') = \sigma_0\rho_0{}^{-1} \in G(k(s))$, which is not the case by §4.4. It follows that there is a unique element $i(s)$ of F such that

$$M(1, -1, i(s)) \in j(G^*(k(s))).$$

This condition defines an injective map $i : S \longrightarrow F$, and this map determines a subset $\mathbf{S}$ of F, given by

$$\mathbf{S} = i(S).$$

The set $\mathbf{S}$ in turn determines a finite cube $\mathrm{C}(\mathbf{S})$ in $\mathrm{AG}(3, F)$. Our aim is to show that C is isomorphic, as a geometric lattice, to the cube $\mathrm{C}(\mathbf{S})$.

6.14 The incidence condition in terms of i and j

From the definition of the map i we deduce that

$$j(G(k(s))) = \{M(1,-b,bi(s))|b \in e(H_F)\} \text{ for all } s \in S.$$

Suppose now that $s \in S\backslash\{t,t'\}$, and let $\lambda = h \vee (t',t',s)$. Then $\lambda \in \Gamma(h)$ and so $j(\lambda) = M(a,0,0)$ for some $a \in F^*$. Moreover $\hat{\lambda}(G(h')) = G(h(s))$, since λ contains the y-line through (t',t',s), by C6,7. It follows that $j(G(h(s))) = j(\hat{\lambda}(G(h'))) = \{M(a,0,0)M(b,0,1-b)M(1/a,0,0)|b \in e(H_F)\} = \{M(b,0,a-ab)|b \in e(H_F)\}$. Also $j(\tau(d,h(s)) = M(1,-1,a)$, since $j(G(h(s))) = M(1,-1,a)j(G(d))M(1,1,-a)$; and $\tau(d,h(s)) \in G(k(s))$. We conclude that $a = i(s)$ and

$$j(G(h(s))) = \{M(b,0,(1-b)i(s))|b \in e(H_F)\}.$$

Note that this is actually true for *all* $s \in S$.

Having determined $j(G(k(s)))$ and $j(G(h(s)))$ for all $s \in S$, it is now routine to check that if $(u,v,w) \in S^3$, $\lambda \in \Gamma$ and $j(\lambda) = M(a,b,c)$ then

$$(u,v,w) \in \lambda \Leftrightarrow i(w) = ai(u) + bi(v) + c$$

using the fact that if $p = (u,v,u)$ then $G(p) = G(k(v))G(h(u))$ and the fact that if $p = (u,v,u)$ and $q = (w,v,w)$ then $(u,v,w) \in \lambda \Leftrightarrow \hat{\lambda}(G(p)) = \hat{\lambda}(G(q))$ (cf. §4.4 and §5.3).

6.15 The maps $\hat{\imath}$ and $\hat{\jmath}$

Let us, to avoid confusion, now denote the set of all ordinary planes of C by $\Gamma(C)$, and the set of all ordinary planes of $\mathrm{C}(\mathbf{S})$ by $\Gamma(\mathrm{C}(\mathbf{S}))$. We define the map $\hat{\imath} : S^3 \longrightarrow \mathbf{S}^3$ by the rule

$$\hat{\imath}(u,v,w) = (i(u),i(v),i(w)) \quad \text{for all } (u,v,w) \in S^3$$

and the map $\hat{\jmath} : \Gamma(C) \longrightarrow \Gamma(\mathrm{C}(\mathbf{S}))$ by the rule

$$\hat{\jmath}(\lambda) = \{(x,y,z) \in \mathbf{S}^3|z = ax + by + c\} \Leftrightarrow j(\lambda) = M(a,b,c).$$

The calculations in §§6.12–6.14 show that $\hat{\imath}$ and $\hat{\jmath}$ are bijections, and that

$$(u,v,w) \in \lambda \Leftrightarrow \hat{\imath}(u,v,w) \in \hat{\jmath}(\lambda) \quad \text{whenever } (u,v,w) \in S^3 \text{ and } \lambda \in \Gamma(C).$$

Also, by §6.12, $|\Gamma(C)| = |\mathbf{M}| = (v-1)v^2$. We may summarize our results in the following theorem.

6.16 THEOREM

Suppose that C is a perfect finite cube with point set S^3. Then there exists a finite field F, a subset $\mathbf{S}$ of F, a bijection $\hat{\imath} : S^3 \longrightarrow \mathbf{S}^3$ (induced by a map $i : S \longrightarrow \mathbf{S}$) and a bijection $\hat{\jmath} : \Gamma(C) \longrightarrow \Gamma(\mathrm{C}(\mathbf{S}))$, such that if $(u,v,w) \in S^3$ and $\lambda \in \Gamma(C)$ then

$$(u,v,w) \in \lambda \Leftrightarrow \hat{\imath}(u,v,w) \in \hat{\jmath}(\lambda).$$

Moreover, $|\Gamma(C)| = |\Gamma(C(\mathbf{S})| = (f-1)f^2$, *where* $f = |F|$.

Proof. See the remarks in §6.15.

References

[1] B. Huppert, *Endliche Gruppen* I (Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[2] B. Huppert and N. Blackburn, *Finite Groups* II (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

[3] D.J.A. Welsh, *Matroid Theory* (Academic Press, London, New York, San Francisco, 1976).

[4] H. Zassenhaus, 'Über endliche Fastkörper', *Abh. Math. Sem. Univ. Hamburg* **11** (1936), 187-220.

[5] K. Zsigmondy, 'Zur Theorie der Potenzreste', *Monatsh. Math. Phys.* **3** (1892), 265-284.

(Received 5/12/90)