On the Construction of Finite Projective Planes from Homology Semibiplanes

G. Eric Mooorhouse*

From a projective plane Π with involutory homology τ one constructs an incidence system Π/τ having as points and blocks the $\langle\tau\rangle$-orbits of length 2 on the points and lines of Π, and with incidence inherited from Π. Such incidence systems satisfy certain properties which, when taken as axioms, define the class of homology semibiplanes. We describe how one determines, in principle, whether a given homology semibiplane Σ is realizable as Π/τ for some Π and τ, and moreover how many nonequivalent pairs (Π,τ) yield Σ. In case Π' is Desarguesian of prime order we show that Π' is characterized by its homology semibiplane, i.e. $\Pi/\tau \cong \Pi'/\tau'$ implies $\Pi \cong \Pi'$.

1. Introduction

A **semibiplane** (see Hughes [5] or [6]) is an incidence system $\Sigma = (\mathcal{P},\mathcal{L})$ consisting of a set $\mathcal{P}$ of **points**, and a set $\mathcal{L}$ consisting of certain subsets of $\mathcal{P}$ called **blocks**, such that

(i) any two distinct points of Σ lie in either 0 or 2 common blocks of Σ;

(ii) any two distinct blocks of Σ meet in either 0 or 2 points of Σ;

(iii) Σ is connected (in the graph-theoretic sense); and

(iv) every block of Σ contains at least 3 points.

For a semibiplane Σ, it is easily shown that there exist integers v, k such that $|\mathcal{P}| = |\mathcal{L}| = v$, each block contains exactly k points, and each point lies on exactly k blocks.

Two blocks of Σ are **parallel** if they are either equal or disjoint. Each block is parallel to exactly t blocks, where $t = v - \frac{1}{2}k(k-1)$. If parallelism is an equivalence relation on the blocks, then the dual relation on the points (i.e. $P \sim Q$ for points P, Q if either $P = Q$ or no block contains both P and Q) is also an equivalence relation. A semibiplane with these two equivalence relations is called **divisible** and satisfies the property:

$$|P^{\sim}| = |L^{||}| = t = v - \tfrac{1}{2}k(k-1) \qquad \text{for all } P \in \mathcal{P},\ L \in \mathcal{L}$$

where $P^{\sim}$ is the equivalence class of P under $\sim$, and $L^{||}$ is the parallel class of L.

* Supported by NSERC of Canada under a postdoctoral fellowship.

For basic terminology concerning projective planes, the reader may refer to [1]. If Π is a projective plane of order n admitting an involutory homology τ (so that n is odd), we construct a semibiplane $\Sigma = (\mathcal{P}, \mathcal{L})$ as follows: $\mathcal{P}$ (resp., $\mathcal{L}$) is the set of $\langle\tau\rangle$-orbits of length 2 on the points (resp., lines) of Π. Incidence in Σ is inherited from Π, viz. $\{P, P^\tau\}$ is incident with the block $\{L, L^\tau\}$ if and only if $P \in L \cup L^\tau$, where $P \neq P^\tau$ are points and $L \neq L^\tau$ are lines of Π. It follows that Σ is a divisible semibiplane with parameters $v = \frac{1}{2}(n^2-1)$, $k = n$, $t = \frac{1}{2}(n-1)$, and we write $\Sigma = \Pi/\tau$.

This motivates the following definition: a **homology semibiplane** is a divisible semibiplane in which the parameters satisfy $t = \frac{1}{2}(k-1)$ (i.e. k is odd and $v = \frac{1}{2}(k^2-1)$). We call k the **order** of Σ. Given such a homology semibiplane Σ, it is natural to ask: is $\Sigma \cong \Pi/\tau$ for some projective plane Π with an involutory homology τ? If so, is Π unique up to isomorphism? Better yet, how many nonequivalent pairs (Π, τ) give rise to Σ? (We say that (Π_1, τ_1) is **equivalent** to (Π_2, τ_2) if there exists an isomorphism $\psi : \Pi_1 \to \Pi_2$ such that $\psi \circ \tau_1 = \tau_2 \circ \psi$; clearly in this case $\Pi_1/\tau_1 \cong \Pi_2/\tau_2$.)

In §2 we prescribe a general procedure for answering these questions, in principle, for a given Σ. This involves computing a certain subspace of the GF(2)-vector space whose basis is the set of incident point-block pairs of Σ. In practice, applying this method to several small semibiplanes, we have usually resorted to using a computer. However, using our procedure, in §3 we prove the following:

1.1 Theorem. *Suppose that $\Pi/\tau \cong \Pi'/\tau'$ for some pairs (Π, τ), (Π', τ') each consisting of a finite projective plane with involutory homology. If Π' is Desarguesian of prime order, then $\Pi \cong \Pi'$.*

(When Π' is Desarguesian, note that $\Pi \cong \Pi' \iff (\Pi, \tau)$ and (Π', τ') are equivalent, since the full collineation group of Π' has a single conjugacy class of involutory homologies.)

In contrast to Theorem 1.1, it is possible for a homology semibiplane to 'lift' to distinct (nonisomorphic) projective planes, as was shown by Janko and Trung [8]. If Π is a Hall plane of order 9, then $\operatorname{Aut}\Pi$ contains two conjugacy classes of involutory homologies, represented by τ_1 and τ_2, and $\Pi/\tau_1 \ncong \Pi/\tau_2$, although both Π/τ_1 and Π/τ_2 are self-dual.

It follows that the dual Π' of Π admits an involutory homology τ' such that $\Pi'/\tau' \cong \Pi/\tau_1$, and yet $\Pi' \ncong \Pi$. We wish to thank Professor Janko for alerting us to this example.

We are not aware of the existence of homology semibiplanes which do not arise from *some* projective plane. However, Janko and Trung [7] have constructed elation semibiplanes (defined analogously for $t = k/2$) which do not arise from projective planes.

2. The General Case: Construction of the Plane Π from Σ

Let $\Sigma = (\mathcal{P}, \mathcal{L})$ be a given homology semibiplane of order k. Then $\mathcal{P}$ (and likewise $\mathcal{L}$) has $k+1$ equivalence classes, each of size $t = \frac{1}{2}(k-1)$. Clearly the points of a given block $L \in \mathcal{L}$ belong to distinct point classes, and each block in $L^{||}$ meets the same k point classes. Therefore $L^{||}$ determines a point class $P^{\sim}$ such that

$$\mathcal{P} \setminus \bigcup\{M : M \in L^{||}\} = P^{\sim}.$$

This gives a bijection Γ from the set $\mathcal{L}/||$ of parallel classes of blocks, to the set $\mathcal{P}/\sim$ of point classes, namely

$$\Gamma(L^{||}) = \mathcal{P} \setminus \bigcup\{M : M \in L^{||}\}.$$

We wish to construct a projective plane Π of order k admitting an involutory homology τ such that $\Sigma \cong \Pi/\tau$. Moreover we wish to determine all possibilities for (Π, τ) to within equivalence, which yield Σ.

We first suppose that $\Sigma \cong \Pi/\tau$ and proceed to determine (Π, τ) by reversing the process described in §1. Let $F = \mathrm{GF}(2)$. Then we may suppose that Π has points and lines given by the sets of symbols

$$\{O\} \cup \{L^{||} : L \in \mathcal{L}\} \cup (\mathcal{P} \times F), \qquad \{\infty\} \cup \{P^{\sim} : P \in \mathcal{P}\} \cup (\mathcal{L} \times F),$$

respectively, each of size $1 + (k+1) + \frac{1}{2}(k^2-1) \times 2 = k^2 + k + 1$, such that

(i) τ has centre O and axis ∞; τ acts on $\mathcal{P} \times F$ and $\mathcal{L} \times F$ via $(P, i) \mapsto (P, i{+}1)$, $(L, j) \mapsto (L, j{+}1)$, and τ fixes the remaining points and lines of Π;

(ii) O is incident with each member (line) of $\{P^{\sim} : P \in \mathcal{P}\}$ and with no other line of Π;

(iii) for $L \in \mathcal{L}$, the point $L^{||}$ is incident with ∞, $\Gamma(L^{||})$, and all $(M, i) \in \mathcal{L} \times F$ such that $M \in L^{||}$, and with no other line of Π;

(iv) the point $(P, i) \in \mathcal{P} \times F$ is incident with $P^{\sim}$, with exactly one of $\{(L, 0), (L, 1)\}$ for each $L \in \mathcal{L}$ which meets P in Σ, and with no other line of Π.

In particular $(P, 0)$ lies on (L, i) if and only if $(P, 1)$ lies on $(L, i{+}1)$. Let $\mathcal{F} \subset \mathcal{P} \times \mathcal{L}$ be the set of **flags** (i.e. incident point-block pairs) of Σ. Then incidence in Π is completely determined by the function $\alpha : \mathcal{F} \to F$ such that $(P, 0)$ meets $(L, \alpha(P, L))$, and we may write $(\Pi, \tau) = \Sigma^{\alpha}$. It remains to determine necessary conditions (and these will also be sufficient) such that Π is a projective plane.

Suppose that P, Q, L, M form a **digon** in Σ (i.e. $P \neq Q$ are points, $L \neq M$ are blocks with $L \cap M = \{P, Q\}$). By considering Figure 1 for all possible values $i, j, \ell, m \in F$, we see that $\alpha(P, L) + \alpha(P, M) + \alpha(Q, L) + \alpha(Q, M) = 1$.

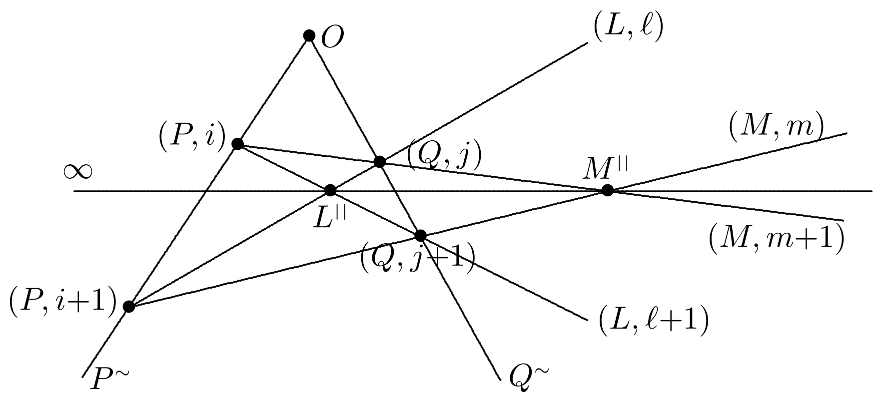

FIGURE 1. Lifting a digon of Σ to Π

Now let V be the vector space of all functions $\mathcal{F} \to F$, so that $\dim_F V = |\mathcal{F}| = \frac{1}{2}k(k^2 - 1)$. The standard basis for V is given by $\{\chi_{P,L} : (P, L) \in \mathcal{F}\}$ where

$$\chi_{P,L}(Q, M) = \begin{cases} 1 & \text{if } (Q, M) = (P, L), \\ 0 & \text{otherwise.} \end{cases}$$

Equip V with the nondegenerate symmetric bilinear form

$$(\beta, \gamma) = \sum_{(P,L) \in \mathcal{F}} \beta(P, L)\gamma(P, L), \qquad \text{for } \beta, \gamma \in V.$$

We have shown that

(1) $(\alpha,\delta) = 1$ for all $\delta \in \mathcal{D}$, where $\mathcal{D} = \big\{\chi_{P,L} + \chi_{P,M} + \chi_{Q,L} + \chi_{Q,M} :$ P, Q, L, M form a digon in $\Sigma\big\}$.

Writing $U^\perp = \{\beta \in V : (\beta,\gamma) = 0 \text{ for all } \gamma \in U\}$ for any subset $U \subseteq V$, (1) is clearly equivalent to

(1′) $\alpha \in \mathcal{C}^\perp \setminus \delta_0^\perp$, where $\mathcal{C} = \langle \delta + \delta' : \delta, \delta' \in \mathcal{D}\rangle$ and δ_0 is any given element of $\mathcal{D}$.

Hereinafter we arbitrarily fix a choice of $\delta_0 \in \mathcal{D}$. A routine check shows that the above steps are reversible, and we have the following.

2.1 Proposition. *Given a homology semibiplane* Σ*, the set of pairs* (Π,τ) *consisting of a projective plane* Π *and involutory homology* τ *such that* $\Sigma \cong \Pi/\tau$*, is given (up to equivalence) by the set of all* Σ^α *(defined as above) such that* $\alpha \in \mathcal{C}^\perp \setminus \delta_0^\perp$*. In particular such a pair* (Π,τ) *exists if and only if* $\delta_0 \notin \mathcal{C}$*.*

Note that distinct functionals $\alpha \in \mathcal{C}^\perp \setminus \delta_0^\perp$ may yield isomorphic Σ^α's. Indeed, if $(\alpha,\delta) = 1$ for all $\delta \in \mathcal{D}$ and $\alpha' = \alpha + \sum\big\{\chi_{P,L} : P \in L\big\}$ for a given $L \in \mathcal{L}$, then we easily compute $(\alpha',\delta) = 1$ for all $\delta \in \mathcal{D}$. Since (1) and (1′) are equivalent, this means that both $\alpha, \alpha' \in \mathcal{C}^\perp \setminus \delta_0^\perp$. However $\Sigma^\alpha = (\Pi,\tau)$ is equivalent to $\Sigma^{\alpha'} = (\Pi',\tau')$. To see this, note that the symbols for points and lines of Π in the above construction may also be used for Π', although Π, Π' have different incidences as determined by α, α' respectively. Now the map ψ which interchanges $(L,0) \leftrightarrow (L,1)$ and fixes all other point and line symbols, determines an isomorphism $\psi : \Pi \to \Pi'$ such that $\psi \circ \tau = \tau' \circ \psi$, as required.

For any $\sigma \in \operatorname{Aut}\Sigma$ and $\beta \in V$, define $\beta^\sigma \in V$ by $\beta^\sigma(P,L) = \beta(P^{\sigma^{-1}}, L^{\sigma^{-1}})$. The resulting action of $\operatorname{Aut}\Sigma$ on V leaves $\mathcal{C}^\perp \setminus \delta_0^\perp$ invariant, as is easily checked by appealing to (1). For all $\sigma \in \operatorname{Aut}\Sigma$, we see that $\Sigma^\alpha = (\Pi,\tau)$ is equivalent to $\Sigma^{\alpha^\sigma} = (\Pi_\sigma,\tau_\sigma)$. This follows as above, again using shared symbols for points and lines of both Π, Π_σ, by observing that the map ψ_σ which acts on point symbols as $O \mapsto O$, $L^{||} \mapsto (L^{\sigma^{-1}})^{||}$, $(P,i) \mapsto (P^{\sigma^{-1}}, i)$ and likewise on line symbols, determines an isomorphism $\psi_\sigma : \Pi \to \Pi_\sigma$ such that $\psi_\sigma \circ \tau = \tau_\sigma \circ \psi_\sigma$.

For $P \in \mathcal{P}$, $L \in \mathcal{L}$ we write $\chi_P = \sum\{\chi_{P,M} : M \text{ contains } P\}$, $\chi_L = \sum\{\chi_{Q,L} : Q \in L\}$. For $\alpha, \alpha' \in V$ we say that α' is **equivalent** to α if $\alpha' = \alpha^\sigma + \sum_{P \in \mathcal{P}_0} \chi_P + \sum_{L \in \mathcal{L}_0} \chi_L$ for some $\sigma \in \mathrm{Aut}\,\Sigma$, $\mathcal{P}_0 \subseteq \mathcal{P}$, $\mathcal{L}_0 \subseteq \mathcal{L}$. We have shown the following.

2.2 Proposition. *Suppose that $\alpha, \alpha' \in V$ are equivalent. Then $\alpha' \in \mathcal{C}^\perp \setminus \delta_0^\perp$ if and only if $\alpha \in \mathcal{C}^\perp \setminus \delta_0^\perp$.*

In addition we have shown the '$\Rightarrow$' half of the following, and the converse follows with some further thought.

2.3 Proposition. *Suppose that $\alpha, \alpha' \in \mathcal{C}^\perp \setminus \delta_0^\perp$. Then α' is equivalent to α if and only if $\Sigma^{\alpha'}$ is equivalent to Σ^α.*

It therefore suffices to consider representatives of the distinct equivalence classes in $\mathcal{C}^\perp \setminus \delta_0^\perp$. Choose $L_0 \in \mathcal{L}$ arbitrarily, and choose P_0 in the corresponding point class (i.e. $P_0^\sim = \Gamma(L_0^{||})$). Let $\mathcal{F}_0$ be the set of flags (P, L) such that $P \sim P_0$ or $L \parallel L_0$; i.e. $\mathcal{F}_0 = \mathcal{F} \cap \big((\mathcal{P} \times L_0^{||}) \cup (P_0^\sim \times \mathcal{L})\big)$. Let $\mathcal{C}_0 = \langle \chi_{P,L} : (P,L) \in \mathcal{F}_0 \rangle$. We may 'standardize' our choice of $\alpha \in \mathcal{C}^\perp \setminus \delta_0^\perp$ as follows.

2.4 Proposition. *Every equivalence class in $\mathcal{C}^\perp \setminus \delta_0^\perp$ contains a representative in $\langle \mathcal{C}, \mathcal{C}_0 \rangle^\perp \setminus \delta_0^\perp$, i.e. a representative $\alpha \in \mathcal{C}^\perp \setminus \delta_0^\perp$ which vanishes on $\mathcal{F}_0$.*

Proof. Suppose that $\alpha \in \mathcal{C}^\perp \setminus \delta_0^\perp$ satisfies $\alpha(Q, M) = 1$ for some flag (Q, M) such that $M \parallel L_0$. Since $P_0^\sim \times L_0^{||}$ contains no flags, we have $Q \not\sim P_0$. Then $\alpha' = \alpha + \chi_Q$ satisfies $\alpha'(Q, M) = 0$ and α' agrees with α on all flags $(P, L) \in \mathcal{F}_0 \setminus \{(Q, M)\}$. By iterating this step we reduce to the case α vanishes on flags in $\mathcal{P} \times L_0^{||}$. Dually we may suppose that α vanishes on flags in $P_0^\sim \times \mathcal{L}$. $\square$

Note that 2.4 does not make full use of the standardization possible through 2.3. Indeed $\mathcal{C}^\perp \setminus \delta_0^\perp$ may contain equivalent functionals $\alpha \neq \alpha'$ both vanishing on $\mathcal{F}_0$. Nevertheless, in special cases (cf. §3) we find $\langle \mathcal{C}, \mathcal{C}_0 \rangle^\perp$ computable and sufficiently small that equivalences therein may be feasibly checked.

3. The Desarguesian Case: Proof of Theorem 1.1

Before proving Theorem 1.1 we require two preliminary results.

3.1 Lemma. *Let $q > 3$ be an odd prime power. If s, t are integers such that $0 < s, t < q-1$ then there exists $r \in \mathrm{GF}(q) \setminus \{-1, 0, 1\}$ such that*

$$r^s \neq 1 \quad \textit{and} \quad \left(\frac{r+1}{r-1}\right)^t \neq 1.$$

Proof. Let $H = \mathrm{GF}(q) \setminus \{-1, 0, 1\}$, $S = \{x^2 : x \in \mathrm{GF}(q)^\times\}$, and define $R : H \to H$ by $R(x) = (x+1)/(x-1)$.

Case (i). Suppose that $s = t = \frac{1}{2}(q-1)$, and we require that r, $R(r)$ are both nonsquares for some $r \in H$. If $q \equiv 1 \bmod 4$, then $|H \cap S| = \frac{1}{2}(q-5)$, $|H \setminus S| = \frac{1}{2}(q-1)$ and since $R : H \to H$ is bijective we may choose $r \in (H \setminus S) \cap R^{-1}(H \setminus S)$. Suppose now that $q \equiv 3 \bmod 4$, so that $|H \setminus S| = \frac{1}{2}(q-3) > 0$. Let $r_1 \in H \setminus S$, so that $r_1^{-1} \in H \setminus S$. Since $-1 \notin S$ we have either $R(r_1) \in H \setminus S$ or $R(r_1^{-1}) = -R(r_1) \in H \setminus S$, and we may choose $r = r_1$ or r_1^{-1} accordingly.

Case (ii). Suppose that s, t do not both equal $\frac{1}{2}(q-1)$. If we define $H_s = \{x \in H : x^s = 1\}$ then $|H_s| \leq (q-1, s) - 1$ since $1 \notin H$, and similarly $|H_t| \leq (q-1, t) - 1$. Since R is bijective and

$$\begin{aligned} |H| - |H_s| - |H_t| &\geq (q-3) - (q-1, s) - (q-1, t) + 2 \\ &\geq (q-3) - \tfrac{1}{2}(q-1) - \tfrac{1}{3}(q-1) + 2 > 0, \end{aligned}$$

we may choose $r \in H \setminus \big(H_s \cup R^{-1}(H_t)\big)$. □

For a linear transformation φ, let $\mathrm{null}(\varphi)$ denote the dimension of its kernel.

3.2 Lemma. *Let φ be a nilpotent endomorphism of a finite dimensional vector space V, and suppose that for some chain of subspaces $0 = V_0 \leq V_1 \leq V_2 \leq \cdots \leq V_N = V$ we have $\varphi(V_i) \subseteq V_{i-2}$ for $i = 2, 3, \ldots, N$. Then*

$$\mathrm{null}(\varphi) \leq \sum_{i=1}^{N} \mathrm{null}(\varphi_i)$$

where $\varphi_i \in \mathrm{Hom}(V_i/V_{i-1}, V_{i-2}/V_{i-3})$ *is induced by* φ*. (For convenience we have let* $V_{-1} = V_{-2} = 0$*.)*

Proof. Choose a system of commuting projections $\pi_i : V \to V_i$. Composing π_i with the canonical map $V_i \to V_i/V_{i-1}$ gives $\rho_i : V \to V_i/V_{i-1}$, and we have an isomorphism

$$\rho : V \xrightarrow{\cong} \bigoplus_{i=1}^{N} V_i/V_{i-1}, \qquad \rho(v) = \rho_1(v) \oplus \cdots \oplus \rho_N(v).$$

Then $\rho \circ \varphi = \overline{\varphi} \circ \rho$ where

$$\overline{\varphi} \in \mathrm{End}\Big(\bigoplus_{i=1}^{N} V_i/V_{i-1}\Big), \qquad \overline{\varphi}(\overline{v_1} \oplus \cdots \oplus \overline{v_N}) = \varphi_3(\overline{v_3}) \oplus \varphi_4(\overline{v_4}) \oplus \cdots \oplus \varphi_N(\overline{v_N}) \oplus 0 \oplus 0.$$

Now $\mathrm{null}(\varphi) \le \mathrm{null}(\rho \circ \varphi) = \mathrm{null}(\overline{\varphi} \circ \rho) = \mathrm{null}(\overline{\varphi}) = \sum_{i=1}^{N} \mathrm{null}(\varphi_i)$ since ρ is surjective. $\square$

We now proceed to prove Theorem 1.1 for a Desarguesian plane Π' of order p, where p is an odd prime. Our notation follows that of §2. Since any plane of order 3 is Desarguesian, we may assume that $p > 3$. Let $K = \mathrm{GF}(p)$, so that Π' has points $\{(x,y,z) \ne (0,0,0) : x,y,z \in K\}$ and lines $\{(a,b,c)^{\mathrm{T}} \ne (0,0,0)^{\mathrm{T}} : a,b,c \in K\}$ in the usual homogeneous coördinates (i.e. $(\lambda x, \lambda y, \lambda z) = (x,y,z)$ for $\lambda \ne 0$, and similarly for lines) where T denotes transpose and $(x,y,z) \in (a,b,c)^{\mathrm{T}} \iff (x,y,z)(a,b,c)^{\mathrm{T}} = 0$. Let τ' be the homology represented by $\mathrm{diag}(-1,1,1)$; this has centre $O = (1,0,0)$ and axis $\infty = (1,0,0)^{\mathrm{T}}$. We denote a typical point of $\Sigma = \Pi'/\tau'$ by $(\overline{x}, y, z) = \{(x,y,z), (-x,y,z)\}$ where $x \ne 0$, $(y,z) \ne (0,0)$, and a typical line of Σ by $(\overline{a}, b, c)^{\mathrm{T}} = \{(a,b,c)^{\mathrm{T}}, (-a,b,c)^{\mathrm{T}}\}$ where $a \ne 0$, $(b,c) \ne (0,0)$, and where $x \mapsto \overline{x}$ is the canonical map $K^\times \to \overline{K^\times} = K^\times/\langle -1 \rangle$, $K^\times = K\backslash\{0\}$. Suppose that $\alpha \in \mathcal{C}^\perp \backslash \delta_0^\perp$. By 2.4 we may assume that α vanishes on $\mathcal{F}_0 = \mathcal{F} \cap \big((\mathcal{P} \times L_0^{||}) \cup (P_0^{\sim} \times \mathcal{L})\big)$ where $L_0^{||} = \{(\,\overline{1}, 0, c)^{\mathrm{T}} : c \in K^\times\}$ and $P_0^{\sim} = \Gamma(L_0^{||}) = \{(\,\overline{1}, y, 0) : y \in K^\times\}$. For $a, x, y \in K$ we have

$$(2) \qquad \alpha\big((\overline{x}, y, 1), (\overline{a}, 1, ax-y)^{\mathrm{T}}\big) + \alpha\big((\overline{x}, y, 1), (\overline{a}, 1, -ax-y)^{\mathrm{T}}\big) = 1 \qquad \text{whenever } ax \ne 0.$$

This follows from (1) for the digon formed by $(\overline{x},y,1)$, $(\,\overline{1},a,0)$, $(\overline{a},1,ax{-}y)^{\mathrm{T}}$, $(\overline{a},1,{-}ax{-}y)^{\mathrm{T}}$, using the assumption that α vanishes on $\mathcal{F}_0$. Also

$$\text{(3)}\qquad \alpha\big((\overline{x},y,1),(\overline{a},1,ax{-}y)^{\mathrm{T}}\big)+\alpha\big((\overline{x},y{-}2ax,1),(\overline{a},1,ax{-}y)^{\mathrm{T}}\big)=1 \quad \text{whenever } ax\neq 0.$$

This follows from (1) for the digon formed by $(\overline{x},y,1)$, $(\overline{x},y{-}2ax,1)$, $(\,\overline{1},0,x)^{\mathrm{T}}$, $(\overline{a},1,ax{-}y)^{\mathrm{T}}$, using the assumption that α vanishes on $\mathcal{F}_0$. Adding (2) and (3) gives $\alpha\big((\overline{x},y,1),(\overline{a},1,{-}ax{-}y)^{\mathrm{T}}\big)=\alpha\big((\overline{x},y{-}2ax,1),(\overline{a},1,ax{-}y)^{\mathrm{T}}\big)$ whenever $ax\neq 0$. Since $2\neq 0$, by induction we have $\alpha\big((\overline{x},y,1),(\overline{a},1,-ax{-}y)^{\mathrm{T}}\big)=\alpha\big((\overline{x},y{-}2nax,1),(\overline{a},1,(2n{-}1)ax{-}y)^{\mathrm{T}}\big)$ whenever $ax\neq 0$ and n is an integer. Since $|K|=p$ is prime we have $\alpha\big((\overline{x},y,1),(\overline{a},1,-ax{-}y)^{\mathrm{T}}\big)=\alpha\big((\overline{x},y{-}c,1),(\overline{a},1,c{-}ax{-}y)^{\mathrm{T}}\big)$ whenever $ax\neq 0$ and $c\in K$. We define a new function $g_\alpha:\overline{K^\times}\times K^\times\to F=\mathrm{GF}(2)$ by $g_\alpha(\overline{x},y)=\alpha\big((\overline{x},y,1),(\,\overline{y/x},1,0)^{\mathrm{T}}\big)$ whenever $xy\neq 0$. By what we have just seen,

$$\text{(4)}\qquad \alpha\big((\overline{x},y,1),(\,\overline{(y{+}c)/x},1,c)^{\mathrm{T}}\big)=g_\alpha(\overline{x},y{+}c)\qquad \text{whenever } x(y{+}c)\neq 0.$$

Let $A=F\big[\,\overline{K^\times}\times K^\times\big]\cong F\big[\,\overline{K^\times}\,\big]\otimes F\big[K^\times\big]$ be the group algebra, with basis $\big\{d_{\overline{a}}\otimes e_b : \overline{a}\in\overline{K^\times},\ b\in K^\times\big\}$ and multiplication defined by $(d_{\overline{a}}\otimes e_b)(d_{\overline{c}}\otimes e_d)=d_{\overline{ac}}\otimes e_{bd}$. Thus $\dim_F A=\big|\overline{K^\times}\times K^\times\big|=\frac{1}{2}(p-1)^2$ and we may view A as the vector space of all functions $\overline{K^\times}\times K^\times\to F$ via the action

$$\big(d_{\overline{a}}\otimes e_b\big)(\overline{x},y)=\begin{cases}1, & \overline{x}=\overline{a}\ \text{and}\ y=b,\\ 0, & \text{otherwise.}\end{cases}$$

Since (4) gives $\alpha(P,L)$ for every flag $(P,L)\in\mathcal{F}\setminus\mathcal{F}_0$, we see that g_α uniquely determines α, and $\alpha\mapsto g_\alpha$ defines an injective F-homomorphism $\langle\mathcal{C},\mathcal{C}_0\rangle^\perp\to A$.

Suppose that $\alpha\in\langle\mathcal{C},\mathcal{C}_0\rangle^\perp$, and that $\beta=\alpha+\chi_{(\overline{1},b,0)}+\sum\{\chi_L : L \text{ contains } (\,\overline{1},b,0)\}$ and $\gamma=\alpha+\chi_{(\overline{1},0,c)^{\mathrm{T}}}+\sum\{\chi_P : P\in(\,\overline{1},0,c)^{\mathrm{T}}\}$ for some $b,c\in K^\times$. Then $\beta,\gamma\in\mathcal{C}^\perp$ since they are both equivalent to α, and furthermore $\beta,\gamma\in\mathcal{C}_0^\perp$. We easily obtain

$$g_\beta=g_\alpha+\sum_{a\in K^\times} d_{\overline{a}}\otimes e_{ab},\qquad g_\gamma=g_\alpha+\sum_{a\in K^\times} d_{\overline{c}}\otimes e_a.$$

Since the map $\alpha\mapsto g_\alpha$ is injective we have the following.

(5) If $\alpha, \alpha' \in \langle \mathcal{C}, \mathcal{C}_0 \rangle^{\perp}$ and $g_{\alpha'} \equiv g_\alpha \bmod \mathcal{E}$, then α' is equivalent to α, where

$$\mathcal{E} = \Big\langle \sum_{a \in K^\times} d_{\overline{a}} \otimes e_{ab}\,,\ \sum_{a \in K^\times} d_{\overline{c}} \otimes e_{a}\ :\ b, c \in K^\times \Big\rangle < A.$$

Note that $\Big\langle \sum_{a \in K^\times} d_{\overline{a}} \otimes e_{ab} : b \in K^\times \Big\rangle$ and $\Big\langle \sum_{a \in K^\times} d_{\overline{c}} \otimes e_{a} : c \in K^\times \Big\rangle$ both have dimension $\frac{1}{2}(p-1)$, and that their intersection is $\Big\langle \sum_{\overline{a} \in \overline{K^\times}} \sum_{b \in K^\times} d_{\overline{a}} \otimes e_{b} \Big\rangle$ of dimension 1. Therefore

(6) $\dim \mathcal{E} = p - 2.$

From (2) and (3) we obtain

(7) $g_\alpha(\overline{x}, y) + g_\alpha(\overline{x}, -y) = 1$ whenever $xy \neq 0$.

Now

(8) $$g_\alpha(\overline{x}, y) + g_\alpha(\overline{x}, y/R) + g_\alpha(\overline{x/r}, y/r) + g_\alpha(\overline{x/r}, y/rR) = 0$$
whenever $(r{+}1)(r{-}1)rxy \neq 0$, where $R = R(r) = (r{+}1)/(r{-}1)$.

To see this, apply (1) to the digon formed by $(\overline{x/r}, 0, 1)$, $(\overline{x}, y(1{-}r^{-1}), 1)$, $(\overline{y/x}, 1, y/r)^{\mathrm{T}}$, $(\overline{y/Rx}, 1, {-}y/rR)^{\mathrm{T}}$, then express in terms of g_α using (4), and use the fact from (7) that $g_\alpha(\overline{x/r}, y/rR) + g_\alpha(\overline{x/r}, -y/rR) = 1$. Now $g(\overline{x}, y) + g(\overline{x/r}, y/r) + g(\overline{x}, y/R) + g(\overline{x/r}, y/rR) = (\phi_r g)(\overline{x}, y)$ where $\phi_r \in \mathrm{End}_F(A)$ is defined by

$$\phi_r g = \big(1 + d_{\overline{r}} \otimes e_r\big)\big(1 + d_{\overline{1}} \otimes e_R\big) g \quad \text{for all } g \in A,\ r \in K^\times \setminus \{-1, 1\},$$
$$\text{where } R = R(r) = (r{+}1)/(r{-}1).$$

Here $1 = d_{\overline{1}} \otimes e_1$ is the identity of A. Hence we may rewrite (8) in the form

(8′) $$g_\alpha \in \bigcap_{r \in H} \ker \phi_r, \qquad H = K^\times \setminus \{-1, 1\}.$$

We claim that

(9) $$\bigcap_{r \in H} \ker \phi_r = \mathcal{E} + \Big\langle \sum_{\overline{a} \in \overline{K^\times}} \sum_{b \in S} d_{\overline{a}} \otimes e_{b} \Big\rangle, \quad \text{where } S = \{x^2 : x \in K^\times\}.$$

Clearly $\bigcap_{r\in H}\ker\phi_r \supseteq \mathcal{E}+\Big\langle \sum_{\overline{a}\in\overline{K^\times}}\sum_{b\in S} d_{\overline{a}}\otimes e_b\Big\rangle$. Before proving (9) we show how it yields the desired conclusion. Combining (5) with the results of §2 we see that $(\Pi,\tau)\cong\Sigma^\alpha$ for some $\alpha\in\langle\mathcal{C},\mathcal{C}_0\rangle^\perp\setminus\delta_0^\perp$ such that $g_\alpha\in\Big\langle \sum_{\overline{a}\in\overline{K^\times}}\sum_{b\in S} d_{\overline{a}}\otimes e_b\Big\rangle$. But the latter subspace of A is one-dimensional and $g_\alpha\neq 0$ since $\alpha\neq 0$ and the map $\alpha\mapsto g_\alpha$ is an F-monomorphism. Therefore $g_\alpha=\sum_{\overline{a}\in\overline{K^\times}}\sum_{b\in S} d_{\overline{a}}\otimes e_b$, which determines α, so we are done. Indeed, by (4) we have

$$\alpha\big((\overline{x},y,z),(\overline{a},b,c)^{\mathrm{T}}\big)=\begin{cases}1, & bz\neq 0,\ \dfrac{y}{z}+\dfrac{c}{b}\in S,\\ 0, & \text{otherwise}\end{cases}$$

for every flag $\big((\overline{x},y,z),(\overline{a},b,c)^{\mathrm{T}}\big)\in\mathcal{F}$ (i.e. $by+cz=\pm ax\neq 0$).

We now prove (9). Since $\sum_{\overline{a}\in\overline{K^\times}}\sum_{b\in S} d_{\overline{a}}\otimes e_b\notin\mathcal{E}$, in view of (6) it suffices to prove that

$$(9')\qquad \dim_F \bigcap_{r\in H}\ker\phi_r \le p-1.$$

We write $p-1=2^{n+1}m$ where m,n are integers, m odd, $n\geq 0$. Let $E=F(\theta)$ be an extension of F in which θ is a primitive m-th root of 1. Extend A to the E-algebra

$$B=E\big[\,\overline{K^\times}\,\big]\otimes_E E\big[K^\times\big]=\Big\{\sum_{\overline{a},b}\lambda_{\overline{a},b}\,d_{\overline{a}}\otimes e_b \,:\, \lambda_{\overline{a},b}\in E \text{ for all } \overline{a}\in\overline{K^\times},\, b\in K^\times\Big\}\cong A\otimes_F E.$$

Clearly $(9')$ is equivalent to

$$(9'')\qquad \dim_E \bigcap_{r\in H}\ker\Phi_r \le p-1,$$

where $\Phi_r\in\mathrm{End}_E(B)$ uniquely extends $\phi_r\in\mathrm{End}_F(A)$, and $\dim_E$ indicates dimension over E. It therefore suffices to prove $(9'')$.

Now $K^\times=\langle\mu\nu\rangle=\langle\mu\rangle\times\langle\nu\rangle$ where μ,ν has order $m,2^{n+1}$ respectively. Furthermore

$$E[K^\times]=E[e_{\mu\nu}]=\Big\{\sum_{i=0}^{p-2}\lambda_i e_{\mu\nu}^i : \lambda_i\in E \text{ for all } i\Big\}\cong E[e_\mu]\otimes_E E[e_\nu],$$

where the latter isomorphism of E-algebras is determined by $e_{\mu\nu} \mapsto e_\mu \otimes e_\nu$. (Hereinafter $\otimes$ means $\otimes_E$, and all vector spaces and homomorphisms are over the field E.) Similarly we have $E\big[\,\overline{K^\times}\,\big] = E[d_{\overline{\mu\nu}}] = E[d_{\overline{\mu}}] \otimes E[d_{\overline{\nu}}]$.

(10) For any odd integer s, the map $x \mapsto (1+e_\nu^s)x$ defines an E-endomorphism of $E[e_\nu]$ whose kernel is the one-dimensional ideal of $E[e_\nu]$ generated by $\sum\limits_{a\in\langle\nu\rangle} e_a$.

To verify (10), note that $e_\nu^s = e_{\nu^s}$. Since $\langle\nu^s\rangle = \langle\nu\rangle$ for s odd, we may suppose that $s=1$. If $x = \sum\limits_{a\in\langle\nu\rangle} \lambda_a e_a$ satisfies $(1+e_\nu)x = 0$ then comparing coefficients gives the result. The same argument obtains

(11) for any odd integer s, the map $x \mapsto (1+d_{\overline{\nu}}^s \otimes e_\nu^s)x$ is an E-endomorphism of $E[d_{\overline{\nu}}] \otimes E[e_\nu]$ whose kernel is the ideal of $E[d_{\overline{\nu}}] \otimes E[e_\nu]$ generated by $\sum\limits_{a\in\langle\nu\rangle} d_{\overline{a}} \otimes e_a$, having dimension 2^n.

The map $x \mapsto e_\mu x$ is an E-endomorphism of $E[e_\mu]$ with characteristic polynomial $X^m + 1 = \prod_{j=0}^{m-1}(X+\theta^j)$, as may be computed from the action on the basis $\{e_\mu^j : 0 \le j < m\}$ of $E[e_\mu]$. Therefore we may choose a new basis $\{v_j : 0 \le j < m\}$ such that $e_\mu v_j = \theta^j v_j$ for all j.

The map $x \mapsto e_\nu x$ is an E-endomorphism of $E[e_\nu]$ with characteristic polynomial $X^{2^{n+1}} + 1 = (X+1)^{2^{n+1}}$, as may be computed from the action on the basis $\{e_\nu^\ell : 0 \le \ell < 2^{n+1}\}$. By (10) the map $x \mapsto (1+e_\nu)x$ has nullity equal to 1, and so the Jordan canonical form of $x \mapsto e_\nu x$ has a single block for the eigenvalue 1, and we may choose a new basis $\{z_\ell : 0 \le \ell < 2^{n+1}\}$ of $E[e_\nu]$ such that

$$(1+e_\nu)z_\ell = \begin{cases} 0, & \ell = 0, \\ z_{\ell-1}, & 1 \le \ell < 2^{n+1}. \end{cases}$$

For any integer s,

$$(12) \qquad e_\nu^s z_\ell = \big(1 + (1+e_\nu)\big)^s z_\ell = z_\ell + s z_\ell + \binom{s}{2} z_{\ell-2} + \binom{s}{3} z_{\ell-3} + \cdots ,$$

where the binomial coefficients are interpreted modulo 2, and the general term $\binom{s}{h}z_{\ell-h}$ is zero for $h > \min\{s,\ell\}$. Similarly $E[d_{\overline{\mu}}]$, $E[d_{\overline{\nu}}]$ have respective bases $\{u_i : 0 \le i < m\}$, $\{w_k : 0 \le k < 2^n\}$ such that

$$d_{\overline{\mu}} u_i = \theta^i u_i, \quad 0 \le i < m, \qquad\qquad (1+d_{\overline{\nu}})w_k = \begin{cases} 0, & k=0, \\ w_{k-1}, & 1 \le k < 2^n. \end{cases}$$

Since the tensor product is associative and commutative (to within E-algebra isomorphism) we may rewrite

$$B = E[d_{\overline{\mu}}] \otimes E[e_\mu] \otimes E[d_{\overline{\nu}}] \otimes E[e_\nu] = \bigoplus_{i=0}^{m-1} \bigoplus_{j=0}^{m-1} u_i \otimes v_j \otimes E[d_{\overline{\nu}}] \otimes E[e_\nu],$$

where each summand is invariant under $\Phi_r \in \mathrm{End}_E(B)$ defined by

$$\Phi_r(x) = (1 + d_{\overline{\mu}}^s \otimes e_\mu^s \otimes d_{\overline{\nu}}^s \otimes e_\nu^s)(1 + d_{\overline{1}} \otimes e_\mu^t \otimes d_{\overline{1}} \otimes e_\nu^t)x \quad \text{for all } x \in B,$$
$$\text{where } r = (\mu\nu)^s \in H,\ R = R(r) = (r{+}1)/(r{-}1) = (\mu\nu)^t.$$

(Here $1 = d_{\overline{1}} \otimes e_1 \otimes d_{\overline{1}} \otimes e_1$ is the identity of B.) Thus

$$\text{(13)} \qquad \dim \bigcap_{r\in H} \ker \Phi_r = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \dim \bigcap_{r\in H} \ker \Phi_r\big|_{u_i \otimes v_j \otimes E[d_{\overline{\nu}}] \otimes E[e_\nu]}.$$

Using (12) and an analogous expression for $d_{\overline{\nu}}^s w_k$, we compute

$$\Phi_r(u_i \otimes v_j \otimes w_k \otimes z_\ell) \equiv \big(1+\theta^{(i+j)s}\big)\big(1+\theta^{jt}\big) u_i \otimes v_j \otimes w_k \otimes z_\ell$$
$$\bmod u_i \otimes v_j \otimes \langle w_{k+1}, w_{k+2}, \ldots, w_{2^n-1}\rangle \otimes \langle z_{\ell+1}, z_{\ell+2}, \ldots, z_{2^{n+1}-1}\rangle$$

and so the matrix representing $\Phi_r\big|_{u_i \otimes v_j \otimes E[d_{\overline{\nu}}] \otimes E[e_\nu]}$ is triangular with respect to the lexicographically ordered basis $\{u_i \otimes v_j \otimes w_k \otimes z_\ell : 0 \le k < 2^n, 0 \le \ell < 2^{n+1}\}$. Therefore the only nonzero terms in (13) arise when the diagonal coefficient $\big(1{+}\theta^{(i+j)s}\big)\big(1{+}\theta^{jt}\big) = 0$ for all $r \in H$, i.e. when $(i{+}j)s \equiv 0$ or $jt \equiv 0 \mod m$ for all $r \in H$, i.e. when $r^{2^{n+1}(i+j)} = 1$ or $R^{2^{n+1}j} = 1$ for all $r \in H$. By Lemma 3.1, this is equivalent to $i+j \equiv 0$ or $j \equiv 0 \mod m$. Therefore

$$(13') \qquad \dim \bigcap_{r\in H} \ker \Phi_r = \sum_{i=0}^{m-1} \dim \bigcap_{r\in H} \ker \Phi_r \big|_{u_i \otimes v_0 \otimes E[d_{\overline{\nu}}] \otimes E[e_\nu]} + \sum_{j=1}^{m-1} \dim \bigcap_{r\in H} \ker \Phi_r \big|_{u_{m-j} \otimes v_j \otimes E[d_{\overline{\nu}}] \otimes E[e_\nu]} \cdot$$

We show first that

$$(14) \qquad \dim \bigcap_{r\in H} \ker \Phi_r \big|_{u_{m-j} \otimes v_j \otimes E[d_{\overline{\nu}}] \otimes E[e_\nu]} \leq 2^n \ \text{ whenever } 1 \leq j < m.$$

For if $1 \leq j < m,\ x \in E[d_{\overline{\nu}}] \otimes E[e_\nu]$ then we compute

$$\Phi_r(u_{m-j} \otimes v_j \otimes x) = u_{m-j} \otimes v_j \otimes \big((1+\theta^{jt} d_{\overline{1}} \otimes e_\mu^t)(1+d_{\overline{\nu}}^s \otimes e_\nu^s)x\big)$$

where $r = (\mu\nu)^s,\ R = R(r) = (\mu\nu)^t$. By Lemma 3.1 we may choose $r \in H$ such that $r^{2^n m} \neq 1$ and $R^{2^{n+1}j} \neq 1$, i.e. s is odd and $\theta^{jt} \neq 1$. Suppose that $\Phi_r(u_{m-j} \otimes v_j \otimes x) = 0$. We claim that $(1+d_{\overline{\nu}}^s \otimes e_\nu^s)x = 0$, which in view of (11) would yield (14). But if $(1+d_{\overline{\nu}}^s \otimes e_\nu^s)x \neq 0$, we may write

$$(1+d_{\overline{\nu}}^s \otimes e_\nu^s)x = \sum_{k=0}^{2^n-1} \sum_{\ell=0}^{2^{n+1}-1} \lambda_{k,\ell}\, w_k \otimes z_\ell, \qquad \lambda_{k,\ell} \in E,$$

and we may suppose for some k', ℓ' that $\lambda_{k',\ell'} \neq 0,\ \lambda_{k',\ell} = 0$ whenever $\ell > \ell'$. Then the coefficient of $u_{m-j} \otimes v_j \otimes w_{k'} \otimes z_{\ell'}$ in $\Phi_r(u_{m-j} \otimes v_j \otimes x)$ is $(1+\theta^{jt})\lambda_{k',\ell'} \neq 0$, a contradiction, and so (14) follows. Next we show that

$$(15) \qquad \dim \bigcap_{r\in H} \ker \Phi_r \big|_{u_i \otimes v_0 \otimes E[d_{\overline{\nu}}] \otimes E[e_\nu]} \leq 2^n \ \text{ whenever } 1 \leq i < m.$$

For if $1 \leq i < m,\ x \in E[d_{\overline{\nu}}] \otimes E[e_\nu]$ then

$$\Phi_r(u_i \otimes v_0 \otimes x) = u_i \otimes v_0 \otimes \big((1+\theta^{-is} d_{\overline{\nu}}^s \otimes e_\nu^s)(1+d_{\overline{1}} \otimes e_\mu^t)x\big)$$

where $r = (\mu\nu)^s$, $R = R(r) = (\mu\nu)^t$. By Lemma 3.1 we may choose r such that $r^{2^{n+1}i} \neq 1$ and $R^{2^n m} \neq 1$, i.e. $\theta^{is} \neq 1$ and t is odd. Suppose that $\Phi_r(u_i \otimes v_0 \otimes x) = 0$. We claim that $(1+d_{\overline{1}} \otimes e_\mu^t)x = 0$, which in view of (10) would yield $x \in E[d_{\overline{\nu}}] \otimes \sum_{a\in\langle\nu\rangle} e_a$, a space of dimension 2^n, from which (15) would follow. However if $(1+d_{\overline{1}} \otimes e_\mu^t)x \neq 0$ then we obtain a contradiction as in the proof of (14) above, and so (15) holds. Finally we show that

$$(16)\qquad \dim \bigcap_{r\in H} \ker \Phi_r\big|_{u_0\,\otimes\, v_0\,\otimes\, E[d_{\overline{\nu}}]\,\otimes\, E[e_\nu]} \le 2^{n+1}.$$

For if $x \in E[d_{\overline{\nu}}] \otimes E[e_\nu]$ then

$$\phi_r(u_0 \otimes v_0 \otimes x) = u_0 \otimes v_0 \otimes \big((1 + d_{\overline{\nu}}^s \otimes e_\nu^s)(1 + d_{\overline{1}} \otimes e_\mu^t)x\big),$$

where $r = (\mu\nu)^s$, $R = R(r) = (\mu\nu)^t$. By Lemma 3.1 we may choose $r \in H$ such that $r^{2^n m} \ne 1$ and $R^{2^n m} \ne 1$, i.e. $s \equiv t \equiv 1 \mod 2$. Fixing such an r, it suffices to show that $\mathrm{null}(\varphi) \le 2^{n+1}$ where $\varphi\, x = (1 + d_{\overline{\nu}}^s \otimes e_\nu^s)(1 + d_{\overline{1}} \otimes e_\mu^t)x$, $\varphi \in \mathrm{End}_E\big(E[d_{\overline{\nu}}] \otimes E[e_\nu]\big)$. For $0 \le h < 3{\cdot}2^n$ define U_h to be the subspace of $E[d_{\overline{\nu}}]\otimes E[e_\nu]$ spanned by $\{w_k \otimes z_\ell : k+\ell < h\}$. This gives a chain of φ-invariant subspaces, namely

$$0 = U_0 < U_1 < \cdots < U_{3\cdot 2^n - 1} = E[d_{\overline{\nu}}] \otimes E[e_\nu].$$

Indeed for $2 \le k < 2^n$, $1 \le \ell < 2^{n+1}$, we compute

$$\begin{aligned}
&\varphi(w_k \otimes z_\ell) \in w_k \otimes z_{\ell-2} + w_{k-1} \otimes z_{\ell-1} + U_{k+\ell-2},\\
&\varphi(w_0 \otimes z_\ell) \in w_0 \otimes z_{\ell-2} + U_{\ell-2},\\
&\varphi(w_k \otimes z_1) \in w_{k-1} \otimes z_0 + U_{k-1},\\
&\varphi(w_k \otimes z_0) = 0 = \varphi(w_0 \otimes z_1) = \varphi(w_0 \otimes z_0).
\end{aligned}$$

These relations follow from (12) together with a variant of (12) expressing $d_{\overline{\nu}}^s w_k$, and using $\binom{s}{2} + \binom{t}{2} + \binom{s+t}{2} \equiv 1 \mod 2$ whenever $s \equiv t \equiv 1 \mod 2$. Thus $\varphi(U_h) \subseteq U_{h-2}$ and φ induces $\varphi_h \in \mathrm{Hom}_E(U_h/U_{h-1}, U_{h-2}/U_{h-3})$ for $h = 2, 3, \ldots, 3{\cdot}2^n{-}1$. By the above relations we easily see that

$$\mathrm{null}\,\varphi_h = \begin{cases} 1, & h = 1,\\ 2, & 2 \le h \le 2^n,\\ 1, & h = 2^n{+}1,\\ 0, & 2^n{+}2 \le h < 3{\cdot}2^n. \end{cases}$$

By Lemma 3.2 we have $\mathrm{null}\,\varphi \le 2^{n+1}$ and so (16) holds. Combining ($13'$), (14), (15), (16) we have

$$\dim \bigcap_{r\in H} \ker \Phi_r \le \sum_{j=1}^{m-1} 2^n + \sum_{i=1}^{m-1} 2^n + 2^{n+1} = 2^{n+1}m = p - 1,$$

which proves ($9''$), as required. □

4. Further Remarks

The problem of classifying projective planes of a given order n admitting an involutory homology, decomposes naturally into the following two steps: (a) classify all homology semibiplanes of order n, and (b) 'lift' each such semibiplane to as many distinct projective planes as possible. Matulić-Bedenić [9] showed the uniqueness of the homology semibiplane of order 11, and of the corresponding projective plane with involutory homology. Thus Theorem 1.1 gives a generalization of step (b) of [9]. Unfortunately step (a) is evidently much more difficult than step (b) in general, and so we are still very far from classifying projective planes of prime order admitting an involutory collineation. It is widely conjectured that any projective plane of prime order is Desarguesian.

Hughes [3], [4] showed that the more general problem of determining all projective planes of given order n which admit a given abstract group G as a collineation group, is equivalent to determining all possible matrices A with entries in the group algebra $\mathbb{Q}G$ over the rational field, whose rows and columns satisfy certain 'inner product' relations. (Strictly speaking, these relations also involve the choices of point and line stabilizers; moreover, additional conditions must be imposed if G is to act faithfully.) These relations on A yield relations on the integral matrix $\phi(A)$ obtained by applying to each entry the ring homomorphism $\phi : \mathbb{Q}G \to \mathbb{Q}$, $\left(\sum a_g g\right) \mapsto \sum a_g$ (see [3]). Given n and G, the problem of finding all nonequivalent pairs (Π, ρ) such that Π is a projective plane of order n and $\rho : G \to \operatorname{Aut}\Pi$ is a faithful action, splits naturally into two steps: (a) determine all possibilities for $\phi(A)$, and (b) for each such candidate for $\phi(A)$, determine all possibilities for A. This scheme has been successfully followed by Shull [10], Whitesides [11], Ho [2] and others. In the case G is a homology group of order 2, candidates for $\phi(A)$ correspond to homology semibiplanes, and 'lifting' $\phi(A)$ to A corresponds to 'lifting' a homology semibiplane to a projective plane. Namely, $\phi(A)$ is determined by a submatrix thereof which is necessarily the incidence matrix M of a homology semibiplane Σ, and each nonzero entry of M corresponds to a unique flag in $\mathcal{F}$. Therefore lifting $\phi(A)$ (or essentially M) to A amounts to finding a suitable map $\alpha : \mathcal{F} \to G \cong F$ (considering $F = \mathrm{GF}(2)$ as an additive group). 'Suitable' here means that A satisfies the relations of Hughes, which are equivalent to requiring that α satisfy (1) or (1′).

The proof in [8] for planes of order 9 suggests that Theorem 1.1 may be true more generally for any Desarguesian plane Π' of odd order. We anticipate that our methods lead to such a generalization, although thus far the linear algebra involved has defeated us. Moreover, it is expected that analogues of Theorem 1.1 may be found for elation semibiplanes and Baer semibiplanes (see [5], [7]) using GF(2)-vector space techniques similar to those of §2. Since any involutory collineation is either a perspectivity or a Baer collineation, step (b) would seem to be tractable whenever $|G| = 2$. This invokes the more well-known distinguishing feature of involutory collineations: a very special fixed substructure. Yet there is a more subtle way in which involutions are unique among collineations: no approach to step (b) as simple as §2 is known for $|G| > 2$, *even assuming* that G is generated by a perspectivity.

References

1. P. Dembowski, "Finite Geometries", Springer-Verlag, Berlin, 1968.
2. C. Y. Ho, Characterization of projective planes of small prime orders, *J. Comb. Theory Series A* **41** (1986) No.2, 189–220.
3. D. R. Hughes, Generalized incidence matrices over group algebras, *Ill. J. Math.* **1** (1957), 545–551.
4. ——————, Collineations and generalized incidence matrices, *Trans. Amer. Math. Soc.* **86** (1957), 284–296.
5. ——————, Biplanes and semibiplanes, *in* "Combinatorics", Lecture Notes in Mathematics No.686, pp.55–58, Springer-Verlag, Berlin, 1978.
6. D. R. Hughes and F. C. Piper, "Design Theory", Cambridge University Press, Cambridge, 1985, pp.196–211.

7. Z. Janko and T. V. Trung, Two new semibiplanes, *J. Comb. Theory Series A* **33** (1982) No.1, 102–105.
8. ———————, The classification of projective planes of order 9 which possess an involution, *J. Comb. Theory Series A* **33** (1982) No.1, 65–75.
9. I. Matulić-Bedenić, The classification of projective planes of order 11 which possess an involution, *Radovi Matematički* **1** (1985), 149–157.
10. R. Shull, Collineations of projective planes of order 9, *J. Comb. Theory Series A* **37** (1984) No.2, 99–120.
11. S. H. Whitesides, Collineations of projective planes of order 10, Part II, *J. Comb. Theory Series A* **26** (1979) No.3, 269–277.

G. Eric Moorhouse
Dept. of Mathematics
University of Wyoming
Laramie, WY 82071–3036