COSET INTERSECTION PROBLEM AND APPLICATION TO 3-NETS

by

Nicola Pace

A Dissertation Submitted to the Faculty of

The Charles E. Schmidt College of Science

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

Florida Atlantic University

Boca Raton, FL

August 2012

COSET INTERSECTION PROBLEM

AND APPLICATION TO 3-NETS

by

Nicola Pace

This dissertation was prepared under the direction of the candidate's dissertation co-advisors, Dr. Gabor Korchmaros and Dr. Spyros Magliveras, Department of Mathematical Sciences, and has been approved by the members of his supervisory committee. It was submitted to the faculty of the Charles E. Schmidt College of Science and was accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

SUPERVISORY COMMITTEE:

Gabor Korchmaros, Ph.D.
Dissertation Co-Advisor

Spyros Magliveras, Ph.D.
Dissertation Co-Advisor

Stephen Locke, Ph.D.

Ronald Mullin, Ph.D.

Rainer Steinwandt, Ph.D.

Lee Klingler, Ph.D.
Chair, Department of Mathematical Sciences

Gary W. Perry, Ph.D.
Dean, The Charles E. Schmidt College of Science

Barry T. Rosson, Ph.D.
Dean, Graduate College

July 2, 2012
Date

ACKNOWLEDGEMENTS

First I would like to thank the faculty, graduate students and staff of the mathematics department at Florida Atlantic University (FAU). They have contributed to creating a comfortable atmosphere for working, learning and pursuing my research. I would like to specially thank all the professors I took courses from and also those that I worked with.

To my advisors, Dr. Gabor Korchmaros and Dr. Spyros Magliveras, I wish to express my deepest gratitude for their guidance and generosity. I had the privilege of working with Dr. Gabor Korchmaros before beginning my Ph.D. study at FAU. More than his tremendous impact in mentoring my research and supervising this dissertation, I would like to thank him for inspiring me to consider mathematics as a career. Dr. Spyros Magliveras has been much more than an advisor to me over these years at FAU. I feel blessed to have met him in Italy: I later joined him at FAU, and he has guided and followed my progress from the very first semester. The time spent together doing research has resulted in a few papers, but more than that, it has resulted in happy, memorable times doing math.

I also want to convey my deepest thanks to the other members of my committee: Dr. Stephen Locke, Dr. Ronald Mullin and Dr. Rainer Steinwandt. They were always willing to lend their time and expertise. Their thoughtful comments and feedback have guided me throughout my graduate study at FAU.

Finally, to Dr. Gabor Nagy, University of Szeged, thank you for your help with the computational results and software implementation.

ABSTRACT

Author:	Nicola Pace
Title:	Coset Intersection Problem and Application to 3-Nets
Institution:	Florida Atlantic University
Dissertation Co-Advisors:	Dr. Gabor Korchmaros Dr. Spyros Magliveras
Degree:	Doctor of Philosophy
Year:	2012

In a projective plane $PG(2, \mathbb{K})$ defined over an algebraically closed field $\mathbb{K}$ of characteristic $p = 0$, we give a complete classification of 3-nets realizing a finite group. The known infinite family, due to Yuzvinsky, arises from plane cubics and comprises 3-nets realizing cyclic and direct products of two cyclic groups. Another known infinite family, due to Pereira and Yuzvinsky, comprises 3-nets realizing dihedral groups. We prove that there is no further infinite family and list all possible sporadic examples. If p is larger than the order of the group, the same classification holds true apart from three possible exceptions: Alt_4, Sym_4 and Alt_5.

DEDICATION

To my family and Soledad.

COSET INTERSECTION PROBLEM

AND APPLICATION TO 3-NETS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

The notion of a 3-net comes from classical differential geometry via the combinatorial abstraction of the notion of a 3-web. A 3-net of order n is said to *realize a group* G of order n when it is coordinatized by G. There is a long history related to finite 3-nets in the combinatorial theory of affine planes, latin squares, loops and strictly transitive permutation sets. In recent years, finite 3-nets realizing a group in the complex plane have been investigated in connection with the cohomology of local systems on the complements of complex line arrangements, see [6, 25, 26].

In this dissertation, combinatorial methods are used to investigate finite 3-nets realizing a group. Since key examples, such as algebraic 3-nets and tetrahedron type 3-nets, arise naturally in the dual plane of $PG(2, \mathbb{K})$, it is convenient to work with the dual concept of a 3-net. Formally, a *dual 3-net* of order n in $PG(2, \mathbb{K})$ consists of a triple $(\Lambda_1, \Lambda_2, \Lambda_3)$ with $\Lambda_1, \Lambda_2, \Lambda_3$ pairwise disjoint point-sets of size n, called *components*, such that every line meeting two distinct components meets each component in precisely one point. A dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing a group is *algebraic* if its points lie on a plane cubic, and is of *tetrahedron type* if its components lie on the six sides (diagonals) of a non-degenerate quadrangle in such a way that $\Lambda_i = \Delta_i \cup \Gamma_i$ with Δ_i and Γ_i lying on opposite sides, for $i = 1, 2, 3$.

The main goal of this dissertation is to prove the following classification theorem.

Theorem 1.0.1. *Let* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *be a dual* 3*-net which realizes a group* G *of order* n*. If the characteristic of the field,* p*, is zero or is an odd number greater than* n*,*

then one of the following holds.

(I) $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is algebraic and* G *is cyclic or the direct product of two cyclic groups.*

(II) $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is of tetrahedron type and* G *is dihedral.*

(III) G *is the quaternion group of order* 8*.*

(IV) G *is the dicyclic group of order* 12*.*

(V) G *is the quaternion group of order* 16*.*

(VI) $G \cong C_3 \ltimes C_7$*.*

(VII) G *is the elementary abelian group of order* 25*.*

(VIII) G *is the unique group of order* 75 *containing an elementary abelian normal group of order* 25*.*

(IX) $G = W \ltimes (C_5 \times C_5)$ *with a subgroup* W *of order* $2, 4, 8, 16$ *where* $W \cong C_4 \times C_4$ *when* $|W| = 16$*.*

(X) $G \cong \mathrm{Sym}_4$*.*

(XI) $G \cong \mathrm{Alt}_4$*.*

(XII) $G \cong \mathrm{Alt}_5$*.*

Furthermore, if $p = 0$*, the cases (X),(XI),(XII) cannot occur.*

The proof relies on the classification of coset intersections of plane cubics, see [16] and Chapter 3, and also uses some previous results due to Yuzvinsky [26], Urzúa [23], and Blokhuis, Korchmáros and Mazzocca [2].

CHAPTER 2

PRELIMINARY NOTIONS

In this dissertation, we assume that the reader is familiar with basic group, ring, field and vector space theory. In particular, familiarity with elementary results on finite groups, finite fields and vector spaces of finite dimension is assumed.

2.1 LATIN SQUARES, GROUPS, QUASIGROUPS, AND LOOPS

Euler regarded *Latin squares* simply as square matrices with n^2 entries of n different elements, each occurring exactly once in each row and column. The index n is called the *order* of the Latin square. Much later it was shown by Cayley, when investigating multiplication tables of groups that a multiplication table of a group is indeed an appropriately boarded special Latin square. The multiplication table of a group is called its *Cayley table*. In the 1930's, when the theory of quasigroups and loops began to be developed as a generalization of the group concept, the idea of using Latin squares as multiplication tables arose again.

A *quasigroup* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$, such that for every a and b in Q, there exist unique elements x and y in Q such that: $a \cdot x = b$ and $y \cdot a = b$. If $(Q, \cdot)$ is a quasigroup of order n then its multiplicative table is a Latin square of order n, and the converse also holds. A *loop* is a quasigroup with an identity element e such that: $x \cdot e = x = e \cdot x$. It follows that the identity element e is unique, and that every element of Q has a unique left and right inverse.

Let $(Q, \cdot)$ and $(P, \star)$ be quasigroups. A quasigroup *homotopy* from Q to P is a

triple (α, β, γ) of maps from Q to P such that $\alpha(x) \star \beta(y) = \gamma(x \cdot y)$ for all $x, y \in Q$. A quasigroup *homomorphism* is just a homotopy for which the three maps are equal. An *isotopy* is a homotopy for which each of the three maps (α, β, γ) is a bijection. Two quasigroups are *isotopic* if there is an isotopy between them. In terms of Latin squares, an isotopy (α, β, γ) is given by a permutation of rows α, a permutation of columns β, and a permutation on the underlying element set γ.

Each quasigroup is isotopic to a loop (see, [4, Theorem 1.3.3]). If a loop is isotopic to a group, then it is isomorphic to that group and thus is itself a group (see, [4, Theorem 1.3.4] and its corollaries). However, a quasigroup which is isotopic to a group need not be a group. For instance, let $Q = \{1, 2, 3, 4\}$, we can consider the following multiplication tables:

$\star$	2	4	3	1
3	2	1	4	3
2	1	4	3	2
4	4	3	2	1
1	3	2	1	4

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

It is easy to see that $(Q, \star)$ is not a group. However, it is isotopic to the group $(Q, \cdot)$, where the isotopy (α, β, γ) is given by the following maps:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

For details, we refer the reader to [4, Chapter 1].

2.1.1 Preliminary Results on Loops

For two integers k and n, both greater than 1, let $(G, \cdot)$ be a group of order kn containing a normal subgroup $(H, \cdot)$ of order n. Let $\mathcal{G}$ be a Cayley table of $(G, \cdot)$.

Obviously, the rows and the columns representing the elements of $(H, \cdot)$ in $\mathcal{G}$ form a Latin square which is a Cayley table for $(H, \cdot)$. From $\mathcal{G}$, we can extract $k^2 - 1$ more Latin squares using the cosets of H in G. In fact, for any two such cosets H_1 and H_2, a Latin square $H_{1,2}$ is obtained by taking as rows (respectively columns) the elements of H_1 (respectively H_2).

Proposition 2.1.1. *The Latin square $H_{1,2}$ is a Cayley table for a quasigroup isotopic to the group H.*

Proof. Fix an element $t_1 \in H_1$. In $H_{1,2}$, label the row representing the element $h_1 \in H_1$ with $h_1' \in H$ where $h_1 = t_1 \cdot h_1'$. Similarly, for a fixed element $t_2 \in H_2$, label the column representing the element $h_2 \in H_2$ with $h_2' \in H$ where $h_2 = h_2' \cdot t_2$. The entries in $H_{1,2}$ come from the coset $H_1 \cdot H_2$. Now, label the entry h_3 in $H_1 \cdot H_2$ with the element $h_3' \in H$ where $h_3 = h_3' \cdot t_1 \cdot t_2$. Doing so, $H_{1,2}$ becomes a Cayley table for the quasigroup $(H, *)$ where $h_1' * h_2' = h_3'$ with $h_3' = t_1 \cdot h_1' \cdot h_2' \cdot t_1^{-1}$. In fact,

$$h_1 \cdot h_2 = t_1 \cdot h_1' \cdot h_2' \cdot t_2 = t_1 \cdot h_1' \cdot h_2' \cdot t_1^{-1} \cdot t_1 \cdot t_2 = h_3' \cdot t_1 \cdot t_2 = h_3.$$

Furthermore, $h_1' * h_2' = (t_1 \cdot h_1') \cdot (h_2' \cdot t_2)$. Since both maps $\gamma_1 : h_1 \to t_1 \cdot h_1'$ and $\gamma_2 : h_2 \to h_2' \cdot t_2$ are bijections, this can also be written as $h_1' * h_2' = \gamma(h_1') \cdot \gamma(h_2')$, whence the assertion follows. □

2.2 PROJECTIVE PLANES

In this section, we give a concise introduction to Desarguesian projective planes. To make this work as self–contained as possible, we provide some discussions, based on the content of [13], in a way that is more accessible to the nonspecialist. We adopt the same standard terminology as used in [13], and follow the same streamline of [13]. For more in depth discussions, we refer the reader to [13, Chapters I–IV].

2.2.1 Vector Spaces

Let V be a vector space over the field $\mathbb{K}$. If $v \in V$ is a vector and $k \in \mathbb{K}$, then the product $k \cdot v$ is defined as a vector of V, and all the usual associativity and distributivity properties holds. We also recall that all vector spaces of dimension n over $\mathbb{K}$ are isomorphic.

Let V and W be vector spaces over $\mathbb{K}$ and α be an automorphism of $\mathbb{K}$. If ϕ is a mapping of V into W with the properties that

1. $(v_1 + v_2)^\phi = v_1^\phi + v_2^\phi$, for every $v_1, v_2 \in V$,

2. $(k \cdot v)^\phi = k^\alpha \cdot v^\phi$, for every $v \in V$, $k \in \mathbb{K}$,

then ϕ is a *semi-linear transformation* from V to W with associated automorphism α. We say that ϕ is a *linear transformation* if its associated automorphism α is the identity.

Now, we can notice that the set of semi-linear transformations of a vector space V into itself is closed under a natural multiplication. Let ϕ_1, ϕ_2 be semi-linear transformations with associated automorphisms α_1, α_2. Then, $\phi_1\phi_2$ is defined by $v^{\phi_1\phi_2} = (v^{\phi_1})^{\phi_2}$, with associated automorphism $\alpha_1\alpha_2$. A semi-linear transformation of V to V is said to be *non–singular* if it is one-to-one and onto. The set of non–singular semi-linear transformations forms a group, denoted by $\Gamma L(V)$. One can map each element of $\Gamma L(V)$ onto its associated automorphism, and this mapping will be a homomorphism η into $Aut(\mathbb{K})$. It is not hard to show that η is onto. The kernel of η is the set of non–singular linear transformations, is called the *general linear group of* V and is denoted by $GL(V)$.

For the rest of the dissertation, we will assume that V is finite dimensional. Under this assumption, $Aut(\mathbb{K})$ is a subgroup of $\Gamma L(V)$ and we can state the following well-known results.

Proposition 2.2.1. *If V is a finite dimensional vector space over $\mathbb{K}$, then $\Gamma L(V) = A \cdot GL(V)$, where $GL(V)$ is normal in $\Gamma L(V)$, $A \cap GL(V) = 1$, and A is isomorphic to $Aut(\mathbb{K})$.*

If a basis of a vector space is chosen, then we can represent the vectors of the space in terms of their coefficients in that basis. So, if V is a finite dimensional vector space over $\mathbb{K}$, with a basis $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}$, then for each $\mathbf{v} \in V$ there is a unique n–tuple $(x_1, \ldots, x_n)$ such that $\mathbf{v} = x_1\mathbf{e_1} + x_2\mathbf{e_2} + \ldots + x_n\mathbf{e_n}$. A linear transformation of V is is completely determined by the images of $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}$, and hence we can represent it by a square matrix $(a_{i,j})$, where the image of the vector $(x_1, \ldots, x_n)$ under the linear transformation is the ordinary matrix product; that is, the row vector whose j^{th}–term is $\sum_i x_i a_{i,j}$.

Proposition 2.2.2. *The group $GL(V)$ is transitive on the bases of V, and the subgroup of $GL(V)$ fixing every vector in some chosen basis is the identity.*

It is well-known that, if A and B are matrices representing the same transformation in two different basis, then $det(A) = det(B)$. In fact, the determinant is an invariant of the linear transformation that goes with the matrix. Then, we can consider the mapping from $GL(V)$ to $\mathbb{K}$ that sends every element in $GL(V)$ to the determinant of its associated matrix. This mapping is known to be an epimorphism, and the kernel, the set of linear transformations of determinant one, is called the *special linear group of V*, and denoted by $SL(\mathbb{K})$.

Finally, we introduce the important concept of dual space. If V is a vector space over $\mathbb{K}$ then a *linear functional on V* is a mapping f' of V into $\mathbb{K}$ such that (i) for any $\mathbf{v}, \mathbf{w}$ in V, $f'(\mathbf{v} + \mathbf{w}) = f'(\mathbf{v}) + f'(\mathbf{w})$ and (ii) for any $\mathbf{v}$ in V and k in $\mathbb{K}$, $f'(k\mathbf{v}) = kf'(\mathbf{v})$. If f' and g' are two linear functionals, then we define $f' + g'$ by: $(f' + g')(\mathbf{v}) = f'(\mathbf{v}) + g'(\mathbf{v})$, while if f' is a linear functional and b is an element of

$\mathbb{K}$, then we define bf' by: $(bf')(\mathbf{v}) = b(f'(\mathbf{v}))$. Under this operations the set V' of linear functionals of V is a vector space over $\mathbb{K}$, called the *dual space of* V. We can also state the following result.

Proposition 2.2.3. *The dimension of V' is the same as the dimension of V, when V is finite dimensional. Furthermore, V'' is isomorphic to V.*

2.2.2 Projective Planes Coordinatized by a Field

Let V be a finite dimensional vector space over a field $\mathbb{K}$. The collection of subspaces of V, together with the natural containment relation, will be called the projective geometry $PG(V)$. We say that the subspace W *is incident with* the subspace U if either U contains W or W contains U. If V is $(n+1)$-dimensional over $\mathbb{K}$, we say that $PG(V)$ has *geometric dimension* (or g-dimension) n. Similarly, if W is a subspace of V of dimension $i+1$, then W is said to have g-dimension i. In this case, we will write $d(W) = i+1$ and $gd(W) = d(W) - 1 = i$. The subspaces of g-dimension $n-1$ will be called *hyperplanes*, those of g-dimension two will be called *planes*, those of g-dimension one will be called *lines*, and those of g-dimension zero will be called *points*. The intersection of two distinct points is the empty set, whose dimension is zero and whose g-dimension is -1. This is called the *empty space* in $PG(V)$.

Let U and W be subspaces of a given vector space V. The following formula, known as Grassman's identity, is a well-known result from the theory of vector spaces:

$$d(U+W) + d(D \cap W) = d(U) + d(W). \tag{2.1}$$

Obviously, the same formula holds for the g–dimension:

$$gd(U+W) + gd(D \cap W) = gd(U) + gd(W). \tag{2.2}$$

The identity 2.2 has the following immediate consequences.

Proposition 2.2.4. *Let P and Q be distinct points in $PG(V)$. There is a unique line of $PG(V)$ which contains P and Q.*

Proposition 2.2.5. *If E be a line and W be a hyperplane in $PG(V)$, then either E lies in W or E and W meet in a unique point.*

Proposition 2.2.6. *Let E and F be distinct lines in $PG(V)$. Either E and F meet in a unique point, in which case E and F lie in a unique plane of $PG(V)$, or E and F have no point in common, in which case E and F are contained in a unique space of g-dimension three in $PG(V)$.*

Proposition 2.2.7. *If $PG(V)$ has g-dimension two, then every pair of distinct lines meet in a unique point.*

If we are dealing with projective geometries of g-dimension two or more, the definitions of isomorphism and automorphism are very natural. An *isomorphism* from $PG(V)$ to $PG(W)$ is a one-to-one mapping α of the subspaces of $PG(V)$ onto the subspaces of $PG(W)$ which preserves the incidence relation. So, $E < F$ in $P(V)$ if and only if $E^\alpha < F^\alpha$ in $PG(W)$. If $PG(V) = PG(W)$, then the isomorphism α is called an *automorphism*, or a *collineation*, of $PG(V)$. A collineation of order two is called *involution*. An *anti-isomorphism* is a one-to-one mapping β from $PG(V)$ to $PG(W)$ such that $E < F$ in $PG(V)$ if and only if $F^\beta < E^\beta$ in $PG(W)$. If $PG(V) = PG(W)$, then an anti-isomorphism β is called a *correlation* and is a *polarity* when it has order two. If the g-dimension is one, we would need some further discussion. These considerations are out of the scope of this dissertation and we will simply refer the interested reader to [13, II.5].

Now, we state two important theorems.

Theorem 2.2.8. *Let $PG(V)$ have g-dimension two. Then the points and lines of $PG(V)$ satisfy:*

(i) every pair of distinct points are incident with a unique common line;

(ii) every pair of distinct lines are incident with a common point;

(iii) $PG(V)$ contains a set of four points with the property that no three of them lie on a common line.

Theorem 2.2.9 (Desargues' Theorem)**.** *Let $PG(V)$ have g-dimension $d \geq 2$. We say that two triangles are perspective from a point P (resp., from a line L) if their corresponding vertices are on lines through P (resp., edges meet on L). If the two triangles in $PG(V)$ are perspective from a point if and only if they are perspective from a line.*

Because of the importance of Theorems 2.2.8 and 2.2.9, we want to provide some further insight. First of all, one can extend our notion of projective geometry defining a more general $PG(W)$, where W is a (left or right) vector space over a skewfield (not necessarily a field) $\mathbb{S}$. Most of the results stated in this chapter, and, in particular, Theorems 2.2.8 and 2.2.9, still hold in this more general case. At this point, one can formulate the abstract notion of *projective plane*, that consists of two sets (a set of lines and a set of points), and a relation between them, called incidence, and satisfying properties (i),(ii),(iii) of Theorem 2.2.8. A projective geometry $PG(W)$ of g-dimension ≥ 2 is a particular instance of a projective plane. At one time it was thought that these three properties characterized projective planes, that is, a collection of abstract points and lines satisfying them must be of the type $PG(W)$, where W is a (left or right) vector space over a skewfield . This was shown not to be case by Hilbert and Mouton ([10, 17]). An important concern was then to study what else must be assumed, besides properties (i),(ii),(iii) of Theorem 2.2.8, in order to give us a projective geometry of g-dimension two (defined over a skewfield $\mathbb{S}$). It turns

out that the additional feature that characterizes projective geometry of g-dimension two is Theorem 2.2.9, see [24] for details.

Following the terminology introduced by Hilbert ([10]), we will say that a projective plane is *Desarguesian* if Theorem 2.2.9 holds. Then, every projective geometry $PG(V)$ of g-dimension two is a Desarguesian projective plane. For the rest of the dissertation, we will restrict our attention to these planes. If V is a vector space of dimension $n+1$ over a field $\mathbb{K}$, we can always refer to the basis $\mathbf{e_1} = (1, 0, \ldots, 0), \mathbf{e_2} = (0, 1, \ldots, 0), \ldots, \mathbf{e_{n_1}} = (0, \ldots, 0, 1)$. In this case, we will denote $PG(V)$ by $PG(n, \mathbb{K})$.

2.2.3 Dual Planes

If V is a vector space of dimension $n+1$ over the field $\mathbb{K}$, then the dual space V' of V is a vector space of the same dimension over $\mathbb{K}$ (Section 2.2.1). This means that the two projective geometries $PG(V)$ and $PG(V')$ are isomorphic. We want to study further connections between their subspaces through the mapping a_V defined as follows: if $W \subset V$ then

$$W^{a_V} = \{v' \in V' \mid wv' = 0 \text{ for all } w \in W\}.$$

We can also consider the dual mapping $a_{V'}$ from the subspaces of $PG(V')$ to the subspaces of $PG(V)$ (note $V'' = V$). Both a_V and $a_{V'}$ are anti-isomorphism and we can state the following theorem.

Theorem 2.2.10. *The mappings a_V and $a_{V'}$ are anti-isomorphisms (respectively from $PG(V)$ to $PG(V')$ and from $PG(V')$ to $PG(V)$), and $a_V a_{V'} = 1 = a_{V'} a_V$. Here, with an abuse of notation, we use 1 for both the identity map of $PG(V)$ and the identity map of $PG(V')$.*

Corollary 2.2.11. *$PG(V)$ always possesses polarities.*

Suppose V is a vector space of dimension $n+1$ over $\mathbb{K}$. Then a_V maps subspaces of V of dimension i onto subspaces of V' of dimension $n+1-i$ and, in particular, it sends points (respectively hyperplanes) of $PG(V)$ to hyperplanes (respectively points) of $PG(V')$. By Theorem 2.2.10, $a_{V'}$ sends those hyperplanes (respectively points) points back onto the points (respectively hyperplanes) which are their pre-images under a_V.

Let E be a point and U be an hyperplane of $PG(V)$. Recalling the definition of a_V we see that the point E is on the hyperplane U if and only if $\mathbf{eu'} = 0$ for every $\mathbf{e}$ in E and for every $\mathbf{u'}$ in U^{a_V}. Since both E and U^{a_V} have algebraic dimension one, we can represent E by any of its non-zero vectors $\mathbf{e}$, and the hyperplane U by any of the non-zero vectors $\mathbf{u'}$ in U^{a_V}. Then, the incidence will be given by the rule: E is on U if and only if $\mathbf{eu'} = 0$.

In particular, we can consider $PG(2, \mathbb{K})$, where a point $E =< (x, y, z) >$ in $PG(2, \mathbb{K})$ and a line ℓ in $PG(2, \mathbb{K})$, represented by $< (a, b, c) >$ in the dual space, are incident if and only if $ax + by + cz = 0$. That is, the ordinary inner product of (x, y, z) and (a, b, c) is zero. For this reason, from now on, we will represent any point E in $PG(2, \mathbb{K})$ by (x, y, z) and any line ℓ in $PG(2,)$ by a linear form $F(X, Y, Z) = aX + bY + cZ$. However, we have to keep in mind that $< (x, y, z) >=< (kx, ky, kz) >$ and $< (a, b, c) >=< (ka, kb, kc) >$ for every $k \in \mathbb{K}^*$, hence they represent the same point and line. We say that (x, y, z) are *homogeneous coordinates* of E in $PG(2, \mathbb{K})$.

Let $PG(V)$ be a g-dimension n. A *frame* is an ordered set of $n + 2$ points in $PG(V)$ such that no $n+1$ are contained in a hyperplane. The concept of frame plays a role analogous to the role of a basis in the study of vector spaces. As stated in the following lemma, frames always exist.

Lemma 2.2.12. *Let V be an $(n + 1)$-dimensional vector space over a field $\mathbb{K}$ and let $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_{n+1}}$ be a basis for V. Then $E_1 =< \mathbf{b_1} >, E_2 =< \mathbf{b_2} >, \ldots, E_{n+1} =< \mathbf{b_{n+1}} >, E_{n+2} =< \mathbf{b_1} + \mathbf{b_2} + \ldots + \mathbf{b_{n+1}} >$ is a frame for $PG(V)$.*

In fact, as stated in the next lemma, Lemma 2.2.12 provides the most general possible example of frame.

Lemma 2.2.13. *If $PG(V)$ have g-dimension n, and $E_1, \ldots, E_{n+2}$ is a frame in $PG(V)$, then there exists a basis $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_{n+1}}$ such that $E_i =< \mathbf{b_i} >$, for $i = 1, \ldots, n+1$, and $E_{n+2} =< \mathbf{b_1} + \mathbf{b_2} + \ldots + \mathbf{b_{n+1}} >$.*

Furthermore, we have the following propositions.

Proposition 2.2.14. *If $E_1, E_2, \ldots, E_{n+2}$ is a frame in $PG(V)$, then no set of $r+1$ points of the frame, $r < n+1$, lies in a space of g–dimension $r-1$.*

Proposition 2.2.15. *Let $PG(V)$ have g–dimension one. Then three points E_1, E_2, E_3 are a frame if and only if they are distinct.*

Proposition 2.2.16. *Let $PG(V)$ have g–dimension two. Then four points E_1, E_2, E_3, E_4 are a frame if and only if no three of the points are collinear.*

An important application of this concept of frame is the *coordinatization* of a Desarguesian projective plane $PG(V)$. Although this is not essential for this dissertation, as we could always refer to the plane $PG(2, \mathbb{K})$, we want to illustrate this technique. Indeed, similar ideas can be extended to any projective plane, not necessarily Desarguesian, to study its algebraic properties, see [13, Chapter V] for details. Let V be a three-dimensional vector space over $\mathbb{K}$, and let E_1, E_2, E_3, E_4 be a frame for $PG(V)$. By Lemma 2.2.13, there exists a basis $\mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}$ such that $E_1 =< \mathbf{b_1} >, E_2 =< \mathbf{b_2} >, E_3 =< \mathbf{b_3} >, E_4 =< \mathbf{b_1} + \mathbf{b_2} + \mathbf{b_3} >$. Let denote by $E_1 + E_2$ the line in $PG(V)$ passing through E_1 and E_2, that corresponds to the two dimensional subspace of V spanned by $\mathbf{b_1}$ and $\mathbf{b_2}$. Thus, every point of $E_1 + E_2$ has the form $< y_1\mathbf{b_1} + y_2\mathbf{b_2} >$, where $y_1, y_2 \in \mathbb{K}$ and $y_2 \in \mathbb{K}$. Furthermore, $< y_1\mathbf{b_1} + y_2\mathbf{b_2} >=< z_1\mathbf{b_1} + z_2\mathbf{b_2} >$ if and only if there exists $k \in \mathbb{K}$ such that $z_1 = ky_1$

and $z_2 = ky_2$. This implies that every point of $E_1 + E_2$, other than E_1, has the form $< x\mathbf{b_1} + \mathbf{b_2} >$ for a unique $x \in \mathbb{K}$. We can note that $< \mathbf{b_1} + \mathbf{b_2} >$ is the point of intersection of the lines $E_1 + E_2$ and $E_3 + E_4$ ($\mathbf{b_1} + \mathbf{b_2} = -\mathbf{b_3} + (\mathbf{b_1} + \mathbf{b_2} + \mathbf{b_3}) \in (E_3 + E_4)$. Every point on $E_3 + E_4$, other than $< \mathbf{b_1} + \mathbf{b_2} >$, can be uniquely represented in the form $< x\mathbf{b_1} + x\mathbf{b_2} + \mathbf{b_3} >$.

Any arbitrary point P not on the line $E_1 + E_2$ has a unique representation $< x\mathbf{b_1} + y\mathbf{b_2} + \mathbf{b_3} >$. The line from E_2 to $< x\mathbf{b_1} + \mathbf{b_3} >$ meets $E_3 + E_4$ in $< x\mathbf{b_1} + x\mathbf{b_2} + \mathbf{b_3} >$; similarly the line from E_1 to $< y\mathbf{b_2} + \mathbf{b_3} >$ meets $E_3 + E_4$ in $< y\mathbf{b_1} + y\mathbf{b_2} + \mathbf{b_3} >$. Therefore, the line $E_2 + P$ meets $E_1 + E_3$ in $< x\mathbf{e_1} + \mathbf{e_3} >$, while the line $E_1 + P$ meets $E_2 + E_3$ in $< y\mathbf{e_2} + \mathbf{e_3} >$. In this way, we set up a coordinatization of the points of $PG(V)$ not on $E_1 + E_2$. The points on the line $E_1 + E_2$ other than E_1 have the form $< m\mathbf{e_1} + e_2 >$, where $m \in \mathbb{K}$.

2.2.4 Fundamental Theorem of Projective Geometry

In this section, we consider the problem of determining all isomorphisms, automorphisms and correlations of Desarguesian projective planes. The solution of this problem is well-known and, like in the previous sections, we will simply state key results (most of the proofs can be found in [13, II.4]).

Suppose V and W are two vector spaces over $\mathbb{K}$, and β is a semi-linear transformation from V onto W. Then, since β preserves the relation of incidence among subspaces, β induces a homomorphisms of $PG(V)$ onto $PG(W)$. If V and W have the same dimension, then β induces an isomorphism from $PG(V)$ onto $PG(W)$. Surprisingly, all isomorphisms from $PG(V)$ to $PG(W)$ are induced by a semi-linear transformation from V to W. Indeed, we can state the following theorem.

Theorem 2.2.17. *Let V and W be vector spaces of dimension $n > 1$ over the field*

$\mathbb{K}$. *Every isomorphism from* $PG(V)$ *to* $PG(W)$ *is induced by a semi-linear transformation from* V *onto* W.

Corollary 2.2.18. *The group of all automorphism of a projective plane* $PG(V)$ *onto itself is induced by the group of all non-singular semi-linear transformations of* V *onto* V.

Let V be a finite-dimensional vector space over the field $\mathbb{K}$. Let $\Gamma L(V)$ be the group of all non-singular semi-linear transformations of V onto W and $GL(V)$ be the subgroup consisting of all non-singular linear transformations. Moreover, we define $SL(V)$ to be the subgroup of $GL(V)$ consisting of elements of determinant one. Each of these groups induces a group of automorphisms of $PG(V)$ onto itself, which we will indicate by $P\Gamma L(V), PGL(V), PSL(V)$, respectively.

The nature of these induced groups is also well-known.

Theorem 2.2.19. *Let* V *be a vector space over* $\mathbb{K}$ *and* $N = \{\gamma \in \Gamma L(V) | < \mathbf{v}^{\gamma} >= \mathbf{v}$ *for all* $\mathbf{v} \in V$ $\}$. *Then* $P\Gamma L(V) \cong \Gamma L(V)/N$, $PGL(V) \cong GL(V)/(N \cap GL(V))$, *and* $PSL(V) \cong SL(V)/(N \cap SL(V))$.

Theorem 2.2.20. *Let* V *be a vector space over* $\mathbb{K}$, $\mathrm{Aut}\mathbb{K}$ *be the automorphism group of* $\mathbb{K}$, *and* $\mathrm{In}\mathbb{K}$ *be the group of inner automorphisms of* $\mathbb{K}^*$. *Then* $GL(V)$ *is normal in* $\Gamma L(V)$ *and* $SL(V)$ *is normal in* $GL(V)$; *hence* $PGL(V)$ *is normal in* $P\Gamma L(V)$, *and* $PSL(V)$ *is normal in* $PGL(V)$. *Furthermore*

1. $\Gamma L(V)/GL(V) \cong \mathrm{Aut}\mathbb{K}$,

2. $P\Gamma L(V)/PGL(V) \cong \mathrm{Aut}\mathbb{K}/ \in \mathrm{In}\mathbb{K}$,

3. $GL(V)/SL(V) \cong K^*$.

We conclude the section with a series of results on the action of these groups on objects in $PG(V)$.

Theorem 2.2.21. *The group $PGL(V)$ (and hence $P\Gamma L(V)$) is transitive on the frames of $PG(V)$. The subgroup of $PGL(V)$ fixing a frame pointwise is isomorphic to $Inn(\mathbb{K})$ and the subgroup of $P\Gamma L(V)$ fixing a frame pointwise is isomorphic to $Aut(\mathbb{K})$*

Theorem 2.2.22. *Let V be a two-dimensional vector space over a field $\mathbb{K}$. Then, the group $PSL(V)$ is two-transitive on the points of $PG(V)$ but not in general three-transitive, while $PGL(V)$ is sharply-transitive, in every case.*

Lemma 2.2.23. *Let V be a two-dimensional vector space over a field $\mathbb{K}$. Then, $PSL(V)$ is three-transitive if and only if $PSL(V) = PGL(V)$, which is equivalent to demanding that every non-zero element of the field $\mathbb{K}$ is a square.*

2.2.5 Collineations of Projective Planes and Polarities

In this section, we consider the group of automorphisms, or collineations, of a projective plane $PG(V)$, where V is a vector space of dimension three over $\mathbb{K}$. By Theorem 2.2.20, we have that this group is $P\Gamma L(PG(V))$, that is, every collineation is induced by a semi-linear transformation in $\Gamma L(V)$. Not only we will consider the action of $P\Gamma L(V)$ (and its subgroups) on points of $PG(V)$, but also its action on the lines of $PG(V)$.

If a collineation fixes all the points of a line in a projective plane $PG(V)$, then the collineation is called a *perspectivity*, and the line of fixed point is the *axis*. By [13, Theorem 4.9], for a non-identity perspectivity there must be a special point, called *center*, such that all lines passing through this point are fixed. There are no fixed object in $PG(V)$ other than those already listed. Two possibilities arise: if the center and axis are incident, we have an *elation*, and if the center and axis are not incident we have an homology. For convenience, the identity automorphism is regarded as

both elation and homology, and considered to be a perspectivity with any line as axis and any point as center.

Lemma 2.2.24. *Let W_1 and W_2 be two projective lines in a projective plane $PG(V)$ and X a point not on either line. Then there exists a perspectivity with center X that sends W_1 to W_2. Furthermore, there is a unique involutory homology with center X which interchanges W_1 and W_2.*

The dual of Lemma 2.2.24 is also true.

Lemma 2.2.25. *Given two points X_1 and X_2 and a line W passing through neither, there is a perspectivity with axis W sending X_1 to X_2. Furthermore, there is a unique involutory perspectivity which interchanges X_1 and X_2.*

We can also state some result on the transitivity of $PSL(V)$ on the points a projective plane $PG(V)$.

Theorem 2.2.26. *If $PG(V)$ is a Desarguesian projective plane, then the following hold.*

(i) If an element α of $PGL(V)$ induces a perspectivity of $PG(V)$ whose center is on its axis (elation), then α is in $PSL(V)$.

(ii) The group $PSL(V)$ is two-transitive on the points and lines of $PG(V)$.

We conclude this subsection, with a characterization of correlations and polarities in a projective plane $PG(V)$.

Theorem 2.2.27. *Let V a vector space of dimension three over a field $\mathbb{K}$. If β is any correlation of $P(V)$ then there is a semi-linear transformation θ from V to V' such that $\beta = \theta a_{V'}$.*

2.2.6 Affine Planes

Let $PG(V)$ be a projective geometry and W a hyperplane in $PG(V)$. We define the *affine geometry* $PG(V)^W$ to be the set of objects in $PG(V)$ which are not contained in W. The collineation group of $PG(V)$ is transitive on frames and it is transitive on hyperplanes, so there is an isomorphism between $PG(V)^W$ and $PG(V)^U$, for any two different hyperplanes W and U. For this reason, we could simply refer to $PG(V)^W$ as $AG(V)$. Moreover, we can refer to $PG(n, \mathbb{K})$ as $AG(n, \mathbb{K})$.

In particular, let $PG(V)$ be a projective plane and let ℓ be a line of $PG(V)$, then $PG(V)^\ell$ is the set of point and lines of $PG(V)$ obtained by deleting the line ℓ and all the points incident with it. The structure that we obtain is an *affine plane*. An *affine plane* $\mathcal{A}$ is a set of points and lines together with an incidence relation between the points and lines such that

(i) any two distinct points lie on a unique line,

(ii) given any line l and any point P not on l there is a unique line m such that P is on m, and l and m have no common point,

(iii) there are three non-collinear points.

We say that $PG(V)^\ell$ is the affine plane *associated with* $PG(V)$ *and* ℓ.

2.3 PROJECTIVE PLANE CURVES

Let $\mathbb{K}$ be an algebraically closed field. Let $F(X, Y, Z)$ be a *form*, that is, a homogeneous polynomial in $\mathbb{K}[X, Y, Z]$. The graph of this form, $\mathcal{C} = \{(x, y, z) \in PG(2, \mathbb{K}) \mid F(x, y, z) = 0\}$, is a *(projective plane) curve* in the projective plane $PG(2, \mathbb{K})$. The *degree* of the curve $\mathcal{C}$ is simply defined as the degree of the form. The curve is *irreducible* if $F(X, Y, Z)$ does not factor in $\mathbb{K}[X, Y, Z]$. A point P lying on

a curve is a *singular point* of the curve if there is more than one tangent line to the curve through P, [12, Section 1.3]. If no such point exists in $PG(2, \mathbb{K})$, that is, if there is a unique tangent line at each point of the curve, then the curve is *non-singular*. This means that it is impossible to find a point P on $\mathcal{C}$ such that the three partial derivatives of F with respect to X, Y, and Z are all zero at P. If a curve $\mathcal{C}$ has a singular point then the curve $\mathcal{C}$ is *singular*.

A *point of inflexion* P of a curve is one for which the tangent at P has triple contact with the curve, [12, Section 1.3]. Given a form $F(X, Y, Z)$ of degree n, its Hessian $\mathcal{H}$ is defined as the curve given by the form H that is the determinant of the second-order partial derivatives of F:

$$H = \begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{vmatrix}.$$

Thus, the Hessian is a curve of degree $3(n-2)$.

Theorem 2.3.1. *Suppose $F(X, Y, Z) \in \mathbb{K}[X, Y, Z]$ is a form of degree n and that* $\mathrm{char}(\mathbb{K})$ *does not divide* $2(n-1)$*. A non-singular point P lying on the curve $\mathcal{C}$ defined by F is an inflexion point of $\mathcal{C}$ if and only if its Hessian form H vanishes at P.*

Remark 2.3.2. *If* $\mathrm{char}(\mathbb{K})$ *divides* $2(n-1)$ *then H is identically zero.*

The theory of projective plane curves is very rich and deep. There are many questions in the theory of plane algebraic curves for which the answer is not known. In this dissertation, we will focus on projective plane curves of degree $n \leq 3$. However, theory of plane curves of degree $n = 2, 3$ is already very deep. For this reason, we will cover what is strictly needed for our discussion, and, for details, we refer the reader to [1, 12, 13].

2.3.1 Cubics

Let $F(X,Y,Z)$ be a form of degree 3, that is, $F(X,Y,Z) = a_{3,0,0}X^3 + a_{2,1,0}X^2Y + a_{2,0,1}X^2Z + a_{1,2,0}XY^2 + a_{1,1,1}XYZ + a_{1,0,2}XZ^2 + a_{0,3,0}Y^3 + a_{0,2,1}Y^2Z + a_{0,1,2}YZ^2 + a_{0,0,3}Z^3$, where $a_{i,y} \in \mathbb{K}$. The corresponding curve $\mathcal{C}$ is a *cubic*.

If $\mathbb{K}$ is an algebraically closed field of characteristic greater than 3, then the Hessian curve $\mathcal{H}(\mathcal{C})$ of a nonsingular cubic $\mathcal{C}$ is a plane cubic curve. There are 9 points of inflections, given by the points in the set $\mathcal{H}(\mathcal{C}) \cap \mathcal{C}$, and they have interesting properties. By a suitable choice of coordinates, the configuration of these 9 points is always of the type $\mathcal{K}_9$, where ω is a primitive cube root of unity in $\mathbb{K}$:

$$\begin{aligned} \mathcal{K}_9 \ = \{ \ & (0,1,-1), (0,1,-\omega), (0,1,-\omega^2), && (2.3)\\ & (1,0,-1), (1,0,-\omega^2), (1,0,-\omega), && (2.4)\\ & (1,-1,0), (1,-\omega,0), (1,-\omega^2,0) \ \}. && (2.5) \end{aligned}$$

This set $\mathcal{K}_9$ is called a *Hessian configuration* for the nonsingular cubic $\mathcal{E}_\lambda$ with form $E_\lambda = X^3 + Y^3 + Z^3 - \lambda XYZ$, with $\lambda \in \mathbb{K}$. The curve $\mathcal{E}_\infty$ is determined by the form $E_\infty = XYZ$. The set $\{\mathcal{E}_\lambda \mid \lambda \in \mathbb{K} \cup \{\infty\}\}$ is a one-dimensional linear system of plane cubic curves called *Hesse pencil*. The points in $\mathcal{K}_9$ form an affine plane isomorphic to $AG(2, \mathrm{GF}(3))$. For details, we refer the reader to the survey [1].

2.3.2 Operation on Plane Cubic Curves

It is well recognized in classical algebraic geometry that several interesting features of an irreducible plane cubic are encoded in the abelian group defined over its non–singular points in such a way that $P + Q + R = 0$ if and only if P, Q, R are collinear points. This phenomenon is characteristic-free in the sense that the a group law on an irreducible cubic can analogously be defined in any projective plane $PG(2, \mathbb{K})$ defined over a field $\mathbb{K}$ of arbitrary characteristic. In recent years, relevant applications,

especially in Cryptography, gave a strong motivation for the study of such groups and their cyclic subgroups.

In a projective plane $PG(2, \mathbb{K})$ over an algebraically closed field $\mathbb{K}$ of characteristic $p \geq 0$, let $\mathcal{F}$ be an irreducible cubic. The definition of the abelian group $(\mathcal{F}, +)$ of $\mathcal{F}$ is available in the classical literature and recalled here in the following two propositions.

Proposition 2.3.3. [12, Theorem 6.104] *A non–singular plane cubic $\mathcal{F}$ can be equipped with an additive group $(\mathcal{F}, +)$ on the set of all its points. If an inflection point P_0 of $\mathcal{F}$ is chosen to be the identity 0, then three distinct points $P, Q, R \in \mathcal{F}$ are collinear if and only if $P + Q + R = 0$. For a prime number $d \neq p$, the subgroup of $(\mathcal{F}, +)$ consisting of all elements g with $dg = 0$ is isomorphic to $C_d \times C_d$ while for $d = p$ it is either trivial or isomorphic to C_p according as $\mathcal{F}$ is supersingular or not.*

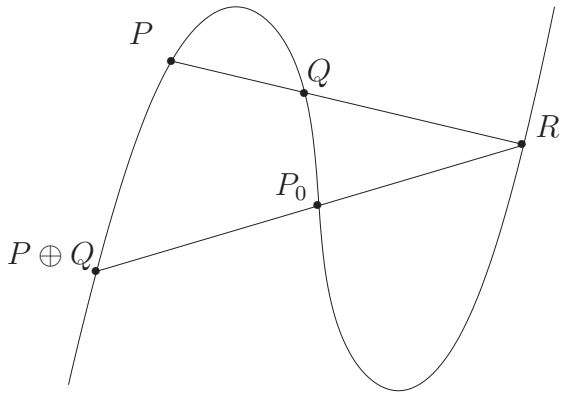

Figure 2.1: Abelian group law on an elliptic curve

Proposition 2.3.4. [25, Proposition 5.6, (1)] *Let $\mathcal{F}$ be an irreducible singular plane cubic with its unique singular point U, and define the operation $+$ on $\mathcal{F} \setminus \{U\}$ in exactly the same way as on a non–singular plane cubic. Then $(\mathcal{F}, +)$ is an abelian group isomorphic to the additive group of $\mathbb{K}$, or the multiplicative group of $\mathbb{K}$, according as P is a cusp or a node.*

2.3.3 Some Useful Results on Plane Cubic Curves

A classical *Lame configuration* consists of two triples of distinct lines in $PG(2, \mathbf{F})$, say ℓ_1, ℓ_2, ℓ_3 and r_1, r_2, r_3, such that no line from one triple passes through the common point of two lines from the other triple. For $1 \leq j, k \leq 3$, let R_{jk} denote the common point of the lines ℓ_j and r_k. There are nine such common points, and they are called the *points of the Lame configuration.*

Proposition 2.3.5 (Lame's Theorem)**.** *If eight points from a Lame configuration lie on a plane cubic curve then the ninth also does.*

Proposition 2.3.6. [12, Theorem 3.13, (Bézout's Theorem)] *If the projective plane curves $\mathcal{F}$ and $\mathcal{G}$ have degrees m and n, and no common component, then they have at most $m \cdot n$ points in common.*

Corollary 2.3.7. *If two projective plane cubics have no common component, then they have at most* 9 *points in common.*

CHAPTER 3

COSET INTERSECTION PROBLEM

In a projective plane $PG(2, \mathbb{K})$ over an algebraically closed field $\mathbb{K}$ of characteristic $p \geq 0$, let $\mathcal{F}$ be an irreducible cubic equipped with its group law $+$ defined on the set of its non–singular points. The resulting group $(\mathcal{F}, +)$ is usually referred to as the group of $\mathcal{F}$. Every subgroup T of $(\mathcal{F}, +)$ together with its cosets form a partition of the set of non–singular points of $\mathcal{F}$. The components of the partition are called T-members of $\mathcal{F}$. Now consider another irreducible cubic $\mathcal{F}'$ with its abelian group $(\mathcal{F}', \boxplus)$, and take a subgroup T' of $(\mathcal{F}', \boxplus)$. Some T'-member of $\mathcal{F}'$ may happen to coincide with a T-member of $\mathcal{F}$, and in this case $\mathcal{F}$ and $\mathcal{F}'$ have a common coset in their intersection.

For a given pointset Ω of size $n \geq 5$ in $PG(2, \mathbb{K})$, the coset intersection problem is to determine the family $\mathbf{F}$ of irreducible cubics in $PG(2, \mathbb{K})$ for which Ω is a common T-member for every $\mathcal{F} \in \mathbf{F}$, that is, Ω is a coset of a subgroup T of $(\mathcal{F}, +)$ for every $\mathcal{F} \in \mathbf{F}$. In the non-trivial case, $|\mathbf{F}| > 1$, such subgroups T have the same order n where $n \leq 9$ by Bézout's theorem. It seems plausible that $\mathbf{F}$ consists of few cubics only, with some exceptions however. An interesting exceptional example (for $p \neq 3$), related to the Hesse pencil, arises when Ω is taken to be the set of the nine inflection points of a non–singular cubic $\mathcal{F}$. For this choice, Ω coincides with the (unique) elementary abelian subgroup G of order 9 in $(\mathcal{F}, +)$, and it can also be viewed as a trivial coset of G. Therefore Ω is a common coset of the non–singular cubics lying in the Hesse pencil of the cubics through the points in Ω.

The goal in this chapter is a complete solution to the coset intersection problem. The main result is stated in the following theorem.

Theorem 3.0.8. *In $PG(2,\mathbb{K})$, let Ω be a point-set of size n with $5 \leq n \leq 9$. Let $\mathbf{F}$ be the family of irreducible cubics $\mathcal{F}$ for which Ω coincides with a coset of a subgroup T of the group of $\mathcal{F}$. Assume that $|\mathbf{F}| \geq 2$.*

If Ω contains three collinear points then one of the following holds.

(A1) *$n = 9$, $T \cong C_9$, and $|\mathbf{F}| = 2$.*

(A2) *$n = 9$, $T \cong C_3 \times C_3$, $p \neq 3$, Ω is the Hesse configuration, and $\mathbf{F}$ consists of all non–singular cubics in the relative Hesse pencil.*

(C1) *$n = 7$, $T \cong C_7$, and $|\mathbf{F}| = 2$.*

(D1) *$n = 6$, $T \cong C_6$, $|\mathbf{F}| \leq 3$, and Ω contains three collinear points but no point in Ω is an inflection point of any cubic in $\mathbf{F}$.*

(D2) *$n = 6$, $T \cong C_6$, and $\mathbf{F}$ consists of the irreducible cubics lying in the pencil through Ω and Ω contains three collinear points that are common inflection points for the cubics in $\mathbf{F}$ each of these three points being the center of an involutory projectivity preserving every cubic in $\mathbf{F}$.*

(E1) *$n = 5$, $T \cong C_5$, $\mathbf{F}$ consists of the non–singular cubics lying in the pencil through Ω where Ω contains three collinear points. It also contains one common inflection point for the cubics in $\mathbf{F}$, that is, the center of an involutory projectivity preserving every cubic in $\mathbf{F}$.*

If Ω contains no three collinear points then one of the following holds.

(B) *$n = 8$, $T \cong C_8$, and $|\mathbf{F}| = 2$.*

(C2) $n = 7$, $T \cong C_7$, *and* $|\mathbf{F}| \leq 5$.

(D3) $n = 6$, $T \cong C_6$, $|\mathbf{F}| \leq 4$, *and* Ω *is not a Clebsch hexagon.*

(D4) $n = 6$, $T \cong C_6$, $|\mathbf{F}| = 10$, *and* Ω *is a Clebsch hexagon.*

(E2) $n = 5$, $T \cong C_5$, $|\mathbf{F}| = 6$, *and* Ω *is any pentagon.*

The proof is divided in two parts, see Sections 3.2 and 3.3, according as Ω contains three collinear points or does not. Our notation and terminology are standard. Backgrounds on plane cubics in any characteristic are found in [20, 12, 11]. A recent survey paper about the Hesse pencil is [1]. For results on Clebsch hexagons used in this dissertation, the reader is referred to [5].

3.1 SOME PRELIMINARY RESULTS

In a projective plane $PG(2, \mathbb{K})$ over an algebraically closed field $\mathbb{K}$ of characteristic $p \geq 0$, let $\mathcal{F}$ be an irreducible cubic. The definition of the abelian group $(\mathcal{F}, +)$ of $\mathcal{F}$ is available in the classical literature and recalled in the Propositions 2.3.3 and 2.3.4.

Let P be a non–singular point of $\mathcal{F}$. If P is not an inflection point of $\mathcal{F}$, then the tangent to $\mathcal{F}$ at P meets $\mathcal{F}$ at point P' other than P. P' is called the *tangential* point of P.

Throughout the chapter, T is assumed to be a subgroup of $(\mathcal{F}, +)$ of order n with $n \geq 5$. For an element g, the symbol $T + g$ is used to denote the set of all points of $\mathcal{F}$ lying in the coset of $T + g$, that is,

$$T + g = \{t + g | t \in T\}.$$

In fact, the geometric properties of $T + g$ heavily depend upon whether $3g \in T$ or $3g \notin T$.

Lemma 3.1.1. *For $|T| \geq 5$, the coset $T + g$ contains three distinct collinear points if and only if $3g \in T$.*

Proof. If t_1+g, t_2+g, and t_3+g are three distinct points in $T+g$, then $t_1+t_2+t_3+3g = t_1 + g + t_2 + g + t_3 + g = 0$ and hence $3g \in T$. If $3g = t^* \in T$ and $|T| \geq 5$, there exist three distinct elements in T whose sum equals $-t^*$, and the three points represented by these elements are collinear. □

3.2 Ω WITH THREE COLLINEAR POINTS

Lemma 3.2.1. *Let $3g \in T$. Then*

(i) *every line through two distinct points in the coset $T + g$ is either tangent to $\mathcal{F}$ at one of these points, or it meets $T + g$ in three distinct points;*

(ii) *the tangential point of any point in $T + g$ is also in $T + g$.*

Proof. Assume that $3g = t^* \in T$, and let $P_1 = t_1 + g$ and $P_2 = t_2 + g$ be two distinct points from $T + g$. Let P_3 be the third common point of $\mathcal{F}$ with the line ℓ through P_1 and P_2. If $P_3 = u$, then $u = -(t_1 + g) - (t_2 + g) = -(t_1 + t_2) - 2g = -(t_1 + t_2 + t^*) + g$. Therefore $P_3 \in T + g$. This holds true when $P_1 = P_2$ and ℓ is the tangent to $\mathcal{F}$ at P_1; in this case P_3 is the tangential point of P_1. □

3.2.1 n=9

Lemma 3.2.2. *If T is a cyclic subgroup of $(\mathcal{F}, +)$ of order 9 and $g \in (\mathcal{F}, +)$ such that $3g \in T$, then for the configuration of the points in $T + g$ one of the following two cases must occur:*

(i) *$T + g$ contains exactly three inflection points of $\mathcal{F}$. They are collinear, but none of them is the tangential point of another point in $T + g$. The remaining six*

points are the vertices of two disjoint triangles whose sides are tangent to $\mathcal{F}$, any side being tangent to $\mathcal{F}$ at one of its two vertices.

(ii) *$T+g$ contains no inflection point of $\mathcal{F}$ and each point in $T+g$ is the tangential point of exactly one other point in $T+g$. Furthermore, $T+g$ can be viewed as a nonagon $P_0P_1\dots P_8$ such that the side P_iP_{i+1} is tangent to $\mathcal{F}$ at P_i for every index i with $P_9=P_0$.*

Proof. Let $t^*=3g$, and identify T with $(\mathbb{Z}/9\mathbb{Z},+)$, where $(\mathbb{Z}/n\mathbb{Z},+)$ denotes the additive group of integers modulo n. We begin with the case where $3t'=t^*$ for some $t'\in T$. From $3g=3t'$ we conclude that $T+g=T+(g-t')$. Working with the set $T+(g-t')$ instead of $T+g$ allows us to consider $3g=\bar{0}$. The tangential point of the point $g+t$ is $-2g-2t$ which can be written as $-2t+g$ showing that the tangential point is also in $T+g$. Since $-2t=t$ only happens when $3t=0$, that is, t is in the unique subgroup M of T of order 3, the point $t+g$ is an inflection point if and only if $t\in M$. Moreover, $\sum_{t\in M}(t+g)=0$ showing that these three inflection points are collinear.

Now, fix an element $t\in T\setminus M$. Since $M=\{0,3t,-3t\}$ and

$$T+g=\{g,t+g,-t+g\}\cup\{3t+g,2t+g,4t+g\}\cup\{-3t+g,-2t+g,-4t+g\},$$

the points in $T+g$ lie on three lines, and hence on a completely reducible cubic $\mathcal{G}$. Therefore $T+g$ consists of the base points of the pencil generated by $\mathcal{F}$ and $\mathcal{G}$. Since three of these points, namely the above inflection points, are collinear, the remaining six points in $T+g$ lie on a conic $\mathcal{C}$.

The above six points can be identified with the vertices of the triangles $\Delta_1=\{t+g,-2t+g,4t+g\}$ and $\Delta_2=\{-t+g,2t+g,-4+g)\}$. The tangent at the point $rt+g$ with $r\in\{1,-1,2,-2,4,-4\}$ meets $\mathcal{F}$ in the point $-2rt+g$. Hence the

tangent at $rt + g$ coincides with a side of the triangle. In particular, no vertex is an inflection point. Furthermore, a similar computation shows that every line containing two vertices from different triangles also contains an inflection point in $T + g$. From this, no three vertices are collinear and the conic $\mathcal{C}$ is irreducible. The configuration of Ω is illustrated in Figure 3.1.

Now, suppose that $t^* = 3t'$ does not happen for $t' \in T$. Then $-2g - 2t \neq g + t$ for any $t \in T$, that is, $T + g$ contains no inflection point. Furthermore, the tangential point of $t + g$ is $-2t - t^* + g$. This shows that each point in $T + g$ is the tangential point of exactly one other point in $T + g$. Let

$$P_0 = 0,\ P_1 = 8t^*,\ P_2 = t^*,\ P_3 = 6t^*,\ P_4 = 5t^*,$$
$$P_5 = 7t^*,\ P_6 = 3t^*,\ P_7 = 2t^*,\ P_8 = 4t^*.$$

A straightforward computation shows that the nonagon $P_0P_1 \dots P_8$ has the property stated in (ii). The configuration of Ω is illustrated in Figure 3.2. □

Lemma 3.2.3. *Let $p \neq 3$. If T is an elementary abelian subgroup of $(\mathcal{F}, +)$ of order 9 and $g \in G$ such that $3g \in T$ then for the configuration of the points in $T + g$ two cases occur:*

(i) *$T + g$ consists of the nine inflection points of $\mathcal{F}$;*

(ii) *$T + g$ contains no inflection point of $\mathcal{F}$ and each point in $T + g$ is the tangential point of exactly one other point in $T + g$. A line through two distinct points in $T + g$ either passes through a third point of $T + g$, or it is a tangent to $\mathcal{F}$ at one of the two points.*

Proof. Let $t^* = 3g$. As $p \neq 3$ and T is an elementary abelian group of order 9, we have that T consists of all 3-torsion points of $(\mathcal{F}, +)$. If $t^* = 0$ then $3g = 0$. Hence $g \in T$, that is, $T + g = T$. Therefore, (i) occurs. If $t^* \neq 0$, then the tangential point

$t - t^* + g$ of $t + g$ is distinct from $t + g$, and (ii) occurs. The configuration of Ω in case (ii) is illustrated in Figure 3.2 where $[i + 3j]$ stands for (i, j) with $0 \leq i, j \leq 2$ modulo 3. □

Proposition 3.2.4. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 9 containing three collinear points. Let $\mathbf{F}$ be a family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup T of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$. Then either $T \cong C_9$ and $|\mathbf{F}| \leq 2$, or $p \neq 3$, $T \cong C_3 \times C_3$, Ω consists of the nine common inflection points of each $\mathcal{F} \in \mathbf{F}$, and $\mathbf{F}$ consists of all non–singular points of the pencil through Ω.*

Proof. Let $T + g$ be the coset of a subgroup T of $(\mathcal{F}, +)$ for some $\mathcal{F} \in \mathbf{F}$. From Lemma 3.1.1, $3g \in T$ holds. Comparing the configurations in Lemmas 3.2.2 and 3.2.3 shows that there are two cases for T depending upon whether $T \cong C_9$ or $T \cong C_3 \times C_3$, and the same case occurs for every $\mathcal{F} \in \mathbf{F}$. Therefore, either Lemma 3.2.2 or Lemma 3.2.3 applies to every $\mathcal{F} \in \mathbf{F}$.

Apart from case (i) in Lemma 3.2.3, Ω has some bisecants. If ℓ is the bisecant through the points $P, Q \in \Omega$, then either P or Q is the tangency point of ℓ in $\mathcal{F}$. Since any two $\mathcal{F} \in \mathbf{F}$ have nine common points, they do not have the same tangent at a common point. Therefore $|\mathbf{F}| \leq 2$.

If T is elementary abelian we only need the following result. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two irreducible cubics. Assume that there is an elementary abelian collineation group E of order 9 which preserves both. If the restriction of E on $\mathcal{F}_i$ is a subgroup of $(\mathcal{F}_i, +)$ for $i = 1, 2$, then $\mathcal{F}_1$ and $\mathcal{F}_2$ have the same inflection points. For the proof, observe that the Hesse configuration of the nine inflection points of $\mathcal{F}_1$ can be viewed as an affine subplane π of $PG(2, \mathbb{K})$ of order 3 so that E acts on π as the group of all translations, see [1]. Therefore, the unique invariant triangle of a non-trivial

element in E has its vertices outside π while its sides are in π each side carrying three inflection points of $\mathcal{F}_1$. Every inflection point lies on four such sides arising from four different subgroups of E of order 3. This shows that the inflection points of $\mathcal{F}_1$ are uniquely determined by the twelve lines preserved by the four non-trivial subgroups of E. Therefore $\mathcal{F}_1$ and $\mathcal{F}_2$ share their inflection points. □

3.2.2 n=8

Lemma 3.2.5. *Let T be a cyclic subgroup of $(\mathcal{F}, +)$ of order 8 and $g \in G$ such that $3g \in T$. Then $T + g$ contains exactly one inflection point, and this point is the tangential point of exactly one other point in $T + g$. Also, three of the points in $T + g$ are the tangential points of exactly two points in $T + g$ while the remaining four points are not tangential points of points in $T + g$.*

Proof. Let $t^* = 3t$, and identify T with $(\mathbb{Z}/8\mathbb{Z}, +)$. Since $t \mapsto 3t$ is an automorphism of T, $t^* = 3t_1$ holds for some $t_1 \in T$. Replacing g with $g - t_1$ allows us to assume $3g = \bar{0}$. Then $g = g + \bar{0}$ is an inflection point while, for $i \neq 0$, the tangential point of $g + \bar{i}$ is $g - 2\bar{i}$. The equation $2x = \bar{u}$ in $(\mathbb{Z}/8\mathbb{Z}, +)$ has either two or zero solutions, according as u is even or odd. From this the assertion follows. The configuration of Ω in case (ii) is illustrated in Figure 3.4. □

Lemma 3.2.6. *For $p \neq 2$, let T be a subgroup of $(\mathcal{F}, +)$ of order 8 isomorphic to $C_2 \times C_4$. Let $g \in (\mathcal{F}, +)$ be for which $3g \in T$. Then $T + g$ contains exactly one inflection point, and this point is the tangential point of exactly three points in $T + g$. One of these three points is the unique point in $T + g$ which is the tangential point of exactly four points in $T + g$, while the remaining six points are not tangential points of points in $T + g$.*

Proof. Again, we may assume that $3g = 0$, since $t \mapsto 3t$ is an automorphism of T. Arguing as in the preceding proof, the equation $2x = u$ in T has to be solved. Looking at the group table of $C_2 \times C_4$ we may observe that there are four solutions for two values of u, namely when $u = 0$ and the non-zero solutions are the involutions in $C_2 \times C_4$, and when u is the unique involution of C_4 and the solutions are the elements of order 4. Moreover, the equation has no solution for each of the other six elements in $T + g$. From this the assertion follows. The configuration of Ω in case (ii) is illustrated in Figure 3.5 where $[i + 2j]$ stands for (i, j) with $0 \leq i \leq 1$ modulo 2, and $0 \leq i \leq 3$ modulo 6. □

Proposition 3.2.7. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 8 containing three collinear points. Let $\mathbf{F}$ be the family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup T of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$. Then $|\mathbf{F}| \leq 1$.*

Proof. From Lemma 3.1.1, $3g \in T$ for every $\mathcal{F} \in \mathbf{F}$. The argument used in the proof of Proposition 3.2.4 can be adapted to show that either Lemma 3.2.5 or Lemma 3.2.6 applies to every $\mathcal{F} \in \mathbf{F}$.

Assume that $T \cong C_8$ for some $\mathcal{F} \in \mathbf{F}$. Comparing the configurations described in Lemmas 3.2.5 and 3.2.6 shows that $T \cong C_8$ for every $\mathcal{F} \in \mathbf{F}$. From Lemma 3.2.5, Ω contains four points, say P_i, lying in exactly one bisecants ℓ_i, with $1 \leq i \leq 4$. One of these bisecants, say ℓ_1 passes through the inflection point of $\mathcal{F}$ in Ω and is tangent to $\mathcal{F}$ at a different point in Ω. Each of the other three bisecants ℓ_i, with $i \geq 2$, is tangent to $\mathcal{F}$ at P_i. Then Ω contains no point that is the tangential point of four points in Ω. By Lemmas 3.2.5 and 3.2.6, T is cyclic for every $\mathcal{F} \in \mathbf{F}$. Therefore, the above argument remains valid for any $\mathcal{G} \in \mathbf{F}$. If $|\mathbf{F}| > 1$ were true then there would exist two irreducible cubics $\mathcal{F}$ and $\mathcal{G}$ with eight common points which also share two

tangents at two common points, contradicting Bézout's theorem.

Assume that $T \cong C_2 \times C_4$ for some $\mathcal{F} \in \mathbf{F}$. From Lemma 3.2.5, Ω contains six points, say P_i, lying in exactly one bisecants ℓ_i, with $1 \leq i \leq 6$. Also, each bisecant ℓ_i is tangent to $\mathcal{F}$ at P_i. Since $T \cong C_2 \times C_4$ for every $\mathcal{F} \in \mathbf{F}$, the same holds true for every $\mathcal{G} \in \mathbf{F}$. If $|\mathbf{F}| > 1$ were true then there would exist two irreducible cubics $\mathcal{F}$ and $\mathcal{G}$ with eight common points which also share six tangents at six common points contradicting Bézout's theorem. □

3.2.3 n=5,7.

Lemma 3.2.8. *For $n \in \{5, 7\}$, let T be a subgroup of $(\mathcal{F}, +)$ of order n. Let $g \in G$ be such that $3g \in T$. Then $T + g$ contains exactly one inflection point P_0, and P_0 is not the tangential point of another point in $T + g$. Each of the remaining $p - 1$ points is the the tangential point of exactly one point in $T + g$. These $p - 1$ points may be viewed as the vertices of a $(p-1)$-gon $P_0P_1 \dots P_{p-1}$ such that the side P_iP_{i+1} is tangent to $\mathcal{F}$ at P_i for every i with $P_{p-1} = P_0$.*

Proof. The arguments in proving Lemma 3.2.5 applies to both $n = 5, 7$. This time, equation $2x = u$ in T has exactly one solution. From this the assertion follows. □

Proposition 3.2.9. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 7 containing three collinear points. Let $\mathbf{F}$ be the family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup T of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$. Then $|\mathbf{F}| \leq 2$.*

Proof. From Lemma 3.2.1, $3g \in T$ for every $\mathcal{F} \in \mathbf{F}$. The argument in the proof of Proposition 3.2.4 shows that Lemma 3.2.8 applies to every $\mathcal{F} \in \mathbf{F}$. Divide the family $\mathbf{F}$ into two subfamilies, say $\mathbf{F}_1$ and $\mathbf{F}_2$, in the following way. For every $j = 0, 1, \dots, 5$

and $P_0 = P_6$, the side P_jP_{j+1} of the hexagon is the tangent to $\mathcal{F}$ at P_j when $\mathcal{F} \in \mathbf{F}_1$, and at P_{j+1} when $\mathcal{F} \in \mathbf{F}_2$. Whenever one of these subfamilies contained at least two cubics, these cubics would have seven common points and also would share six tangents at six common points, contradicting Bézout's theorem. The configuration of Ω in case (ii) is illustrated in Figure 3.6. □

Lemma 3.2.10. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 5 containing three collinear points. Let $\mathbf{F}$ be the family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup T of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$. Then the cubics in $\mathbf{F}$ have a common inflection point P_0 and there is an involutory homology with center P_0 that preserves each cubic in $\mathbf{F}$.*

Proof. Arguing as in the proof of Proposition 3.2.9, each of the two subfamilies of $\mathbf{F}$ comprises cubics with the same five common points and four tangents at four of those common points. Therefore, both $\mathbf{F}_1$ and $\mathbf{F}_2$ form a pencil. Fix a projective frame with homogeneous coordinates (X, Y, Z) in such a way that

$$P_1 = (0, 0, 1),\ P_2 = (1, 0, 0),\ P_3 = (1, 1, 1),\ P_4 = (0, 1, 0).$$

Then $P_0 = (1, 1, 0)$.

The pencil $\mathcal{P}_1$ consisting of the cubics in $\mathbf{F}_1$ is generated by the cubics $\mathcal{G}$ and $\mathcal{D}$ with equations $Y(X - Z)Z = 0$ and $X(Y - X)(Y - Z) = 0$, respectively. Therefore it consists of cubics G_λ with equation

$$Y^2X - X^2Y + (\lambda - 1)XYZ + X^2Z - \lambda YZ^2 = 0,$$

together with $\mathcal{G} = \mathcal{G}_\infty$. Since the line $Z = 0$ contains three distinct base points of the pencil, P_0 is a non–singular point of $\mathcal{G}_\lambda$ for every $\lambda \in \mathbb{K}$, the tangent ℓ_λ to $\mathcal{G}_\lambda$ at P_0 has equation $-X + Y + \lambda Z = 0$. Assume that P_0 is an inflection point

of $\mathcal{G}_\lambda$. Then ℓ_λ contains no point $P = (X, Y, 1)$ from $\mathcal{G}_\lambda$, that is, the polynomials $Y^2X - X^2Y(\lambda-1)XY + X^2 - \lambda Y = 0$ and $-X + Y + \lambda = 0$ have no common solutions. On the other hand, eliminating Y from these polynomials gives λ^2. This shows that P_0 is an inflection point for every irreducible cubic in $\mathcal{P}_1$. Furthermore, if P_0 is chosen to be the zero of $(\mathcal{F}, +)$, then P_1, P_2, P_3, P_4 are 5-torsion points. Furthermore, the involutory homology

$$\varphi : (X, Y, Z) \mapsto (-Y + Z, -X + Z, Z)$$

with center P_0 preserves each cubic in $\mathcal{P}_1$.

The above argument also applies to the pencil $\mathcal{P}_2$ consisting of all cubics in $\mathbf{F}_2$. In the present case, $\mathcal{P}_2$ comprises the cubics G_λ of equation

$$X^2Y - Y^2X + (\lambda - 1)XYZ + Y^2Z - \lambda XZ^2 = 0,$$

together with $\mathcal{G} = \mathcal{G}_\infty$. □

The argument used in the proof of Lemma 3.2.10 also provides the following result.

Proposition 3.2.11. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 5 containing three collinear points. Let $\mathbf{F}$ be the family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup T of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$. Then $\mathbf{F}$ comprises all irreducible cubics of a pencil.*

3.2.4 n=6.

Lemma 3.2.12. *Let T be a subgroup of $(\mathcal{F}, +)$ of order 6 and let $g \in G$ be such that $3g \in T$. Then one of the following holds:*

(i) *$T + g$ contains exactly three inflection points. They are collinear and each of them is the tangential point of exactly one point in $T + g$. The three points of*

$T + g$ other than the inflection points are the vertices of a triangle whose sides contain the inflection points.

(ii) *No point in $T + g$ is an inflection point. The configuration of $T + g$ splits into two triangles $P_0P_2P_4$ and $P_1P_3P_5$ such that no vertex of $P_0P_2P_4$ is a tangential point of a point in $T + g$ while every vertex in $P_1P_3P_5$ is the tangential points of two points in $T + g$, one from $P_0P_2P_4$ the other from $P_1P_3P_5$. The common tangential point of P_{2i+1} and P_{2i+4} is P_{2i+3} for $i = 0, 1, 2$ the indices being considered modulo 6. Each point P_j with j even is incident with three lines of the configuration, while this intersection number is four when j is odd.*

Proof. Let $3g = t^* \in T$ and identify T with $(\mathbb{Z}/6\mathbb{Z}, +)$. Two cases are distinguished according as either $t^* = 3t_1$ holds with $t_1 \in T$ or does not.

In the former case, $t^* = 0$ may be assumed after replacing g by $g - t_1$. Therefore, $3\bar{m} = 0$ for $m \in \{0, 2, 4\}$ which shows that the points $g + \bar{0}$, $g + \bar{2}$ and $g + \bar{4}$ are inflection points. Also, these points are collinear. For $m \in \{1, 3, 5\}$, the tangential point of $g + \bar{m}$ is $g - 2\bar{m}$ and hence it is one of the above inflection points. The configuration of Ω in case (i) is illustrated in Figure 3.7.

Assume that $t^* = 3t_1$ has no solution in $t_1 \in T$. Then $3t^* = \bar{1}$ may be assumed after replacing g by some $g - \bar{m}$ where $m \in \{1, 3, 5\}$. No point in $T + g$ is an inflection point, and a direct computation proves assertion (ii) with $P_j = g + \bar{j}$ where $j = 0, \ldots, 5$. The configuration of Ω in case (ii) is illustrated in Figure 3.8. □

Proposition 3.2.13. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 6 containing three collinear points. Let $\mathbf{F}$ be the family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup T of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$.*

If (i) *of Lemma 3.2.12 occurs then* $\mathbf{F}$ *consists of all irreducible cubics of a pencil which share three inflection points, each is the center of an involutory homology preserving every* $\mathcal{F} \in \mathbf{F}$*. More precisely, if*

$$\Omega = \{P_0, P_1, P_2, P_3, P_4, P_5\}$$

with P_0, P_2, P_4 *being the common inflection points, then the intersection divisor of the cubics in* $\mathcal{F}$ *is* $P_0 + P_1 + P_2 + 2P_1 + 2P_3 + 2P_5$*.*

If (ii) *of Lemma 3.2.12 occurs then* $|\mathbf{F}| \leq 3$*.*

Proof. We first consider case (i) of Lemma 3.2.12. Fix a projective frame with homogeneous coordinates (X, Y, Z) in such a way that

$$P_0 = (1, 0, 1),\ P_1 = (0, 0, 1),\ P_2 = (0, 1, 1),$$
$$P_3 = (0, 1, 0),\ P_4 = (-1, 1, 0),\ P_5 = (1, 0, 0).$$

Using the notation introduced in the proof of Lemma 3.2.12, we suppose that $P_i = g + \bar{i}$ for $i = 0, 1, \ldots 5$. A straightforward computation shows that the irreducible cubics $\mathcal{F} \in \mathbf{F}$ consistent with the configuration described in (i) of Lemma 3.2.12 are those of the pencil $\mathcal{P}$ comprising the cubics $\mathcal{G}_\lambda$ of equation

$$(X - Z)(Y - Z)(X + Y) + \lambda XYZ = 0, \quad \lambda \in \mathbb{K},$$

together with the cubic $\mathcal{G}_\infty$ of equation $XYZ = 0$. The intersection divisor of the cubics in $\mathcal{P}$ is $P_0 + P_2 + P_4 + 2P_1 + 2P_3 + 2P_5$.

Moreover, the points P_0, P_2, P_4 are inflection points of all irreducible cubics in $\mathcal{P}$, and

$$\varphi_0 : (X, Y, Z) \to (Z, -Y, X),$$
$$\varphi_2 : (X, Y, Z) \to (-X, Z, Y),$$
$$\varphi_4 : (X, Y, Z) \to (Y, X, Z),$$

are the involutory homologies preserving every cubic in $\mathcal{P}$, the center of φ_i being P_i, for $i = 0, 2, 4$. Furthermore, the action of T on Ω is generated by the permutation $(P_0P_1P_2P_3P_4P_5)$.

Assume that case (ii) of Lemma 3.2.12 occurs. If $\mathbf{F}$ contained three cubics then two of them would have six common points with the same tangent at each of these six points, contradicting Bézout's theorem. □

3.3 Ω WITH NO THREE COLLINEAR POINTS

Lemma 3.3.1. *If $3g \notin T$ then the following hold:*

(i) *The satellite set $\Psi = T - 2g = \{t - 2g | t \in T\}$ is disjoint from $T + g$ and contains the tangential point of each point in $T + g$.*

(ii) *If $3 \nmid |T|$ then Ψ contains at most one inflection point.*

(iii) *any line r joining a point $P \in T + g$ with a satellite point S is either a tangent to $\mathcal{F}$ at P or $r \cap \mathcal{F} = \{P, S, Q\}$ where Q is a point in $T + g$ other than P.*

Proof. Since $3g \neq 3t$ for any $t \in T$, no point in $T + g$ is an inflection point of $\mathcal{F}$. For a point $P = t + g$ with $t \in T$, the tangential point of P is $P' = -2t - 2g \in \Psi$. Also, $3g \notin T$ implies that no point in Ψ is in $T + g$. This completes the proof of (i). A satellite point $-2g + t$ is an inflection point if and only if $6g = 3t$. If two satellite points are inflection points, then $3t = 3t'$ for distinct $t, t' \in T$ whence $3(t - t') = 0$. Therefore $|T|$ is divisible by 3, and this proves (ii). Let $P = t + g$ and $S = t_1 - 2g$. Then $-(t + g + t_1 - 2g) = -(t + t_1) + g$. If $2t + t_1 = 0$ then S is the tangential point of P. Otherwise, the point $Q = -(t + t_1) + g$ is a point in $T + g$ distinct from P. Therefore (iii) holds. □

Let Ω be a point-set of size $n \leq 9$ containing no three collinear points. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two irreducible cubics passing through every point in Ω.

We investigate the case where Ω coincides with two cosets, one, say $T_1 + g_1$, of a subgroup T_1 of $(\mathcal{F}_1, +)$, and another, say $T_2 \boxplus g_2$, of a subgroup T_2 of $(\mathcal{F}_2, \boxplus)$. Furthermore, assume that $T_1 \cong T_2$, and let π denote a bijection $T_2 \mapsto T_1$ such that $(u \boxplus v)^\pi = u^\pi + v^\pi$ for any $u, v \in T_2$. After identifying the elements of T_1 and T_2 with the first n positive integers, π becomes a permutation π on $\mathcal{I}_n = \{1, 2, \ldots, n\}$.

Now, take x_1, x_2, x_3, x_4 from $\mathcal{I}_n$ such that $x_1 \boxplus x_2 = x_3 \boxplus x_4$. Then

$$x_1^\pi + x_2^\pi = (x_1 \boxplus x_2)^\pi = (x_3 \boxplus x_4)^\pi = x_3^\pi + x_4^\pi. \tag{3.1}$$

Conversely, $x_1^\pi + x_2^\pi = x_3^\pi + x_4^\pi$ implies that $x_1 \boxplus x_2 = x_3 \boxplus x_4$.

Lemma 3.3.2. *The cubics $\mathcal{F}_1$ and $\mathcal{F}_2$ have a common point other than those in Ω provided that the following condition is fulfilled.*

$$\begin{gathered} \textit{For every permutation } \pi \textit{ on } \mathcal{I}_n\textit{, there exists a quadruple of integers} \\ (x_1, x_2, x_3, x_4), \\ \textit{with } 1 \leq x_1 < x_2,\ x_1 < x_3,\ x_3 < x_4 \leq n\textit{, such that both} \\ x_1 + x_2 = x_3 + x_4 \textit{ and } x_1^\pi + x_2^\pi = x_3^\pi + x_4^\pi \textit{ hold.} \end{gathered} \tag{3.2}$$

Proof. Let Ψ_1 (respectively Ψ_2) denote the satellite set of $T_1 + g_1$ (respectively $T_2 \boxplus g_2$). Obviously, every point $P \in \Psi_1 \cap \Psi_2$ is also a common point of $\mathcal{F}_1$ and $\mathcal{F}_2$. By Lemma 3.3.1, $P \notin \Omega$, and it is called an *extra-point* (for $\mathcal{F}_1 \cap \mathcal{F}_2$). We show that such an extra-point exists provided that (3.2) holds.

From $x_1 + x_2 = x_3 + x_4$,

$$(x_1 + g_1) + (x_2 + g_1) = (x_3 + g_1) + (x_4 + g_1). \tag{3.3}$$

To restate this equation in geometric terms, assume that $x_1 < x_2, x_1 < x_3$, $x_3 < x_4$, and consider the line ℓ_{12} joining the points $P_1 = x_1 + g_1$ and $P_2 = x_2 + g_1$ together

with the line ℓ_{34} joining the points $P_3 = x_3 + g_1$ and $P_4 = x_4 + g_1$. Then (3.3) implies that lines ℓ_{12} and ℓ_{34} meet at the point

$$P = -2g_1 - (x_1 + x_2) = -2g_1 + (x_3 + x_4)$$

lying in Ψ_1. Let $y_i = x_i^\pi$ for $i \in \mathcal{I}_n$. The condition $y_1 \boxplus y_2 = y_3 \boxplus y_4$ implies that Ψ_2 contains the common point Q of the lines r_{12} and r_{34} where r_{12} is the line through the points $Q_1 = y_1 \boxplus g_2$ and $Q_2 = y_2 \boxplus g_2$ while r_{34} is the line through the points $Q_3 = y_3 \boxplus g_2$ and $Q_4 = y_3 \boxplus g_2$.

Obviously $P = Q$ when $P_i = Q_i$ for $i = 1, 2, 3, 4$, and then P is an extra-point. This is certainly the case if (3.2) holds.

□

Since $n \leq 9$, such a test can be done with a computer aided exhaustive search. The results are reported in the following lemma.

Lemma 3.3.3. *With the above notation the results below hold.*

(i) *For $n = 8, 9$ there is at least one extra-point for any permutation π.*

(ii) *For $n = 8$, if $T \cong C_2 \times C_4$ then there exist at least two extra-points for any permutation π.*

(iii) *For $n = 7$, if neither π_1 nor π_2 provides an extra-point then $\pi_1^{-1}\pi_2$ does.*

3.3.1 n=9.

For $n = 9$, as a consequence of assertion (i), one has the following corollary.

Proposition 3.3.4. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 9 containing no three collinear points. Let $\mathbf{F}$ be a family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$. Then $|\mathbf{F}| \leq 1$.*

3.3.2 n=8.

Similarly, assertion (ii) gives the following result for $n = 8$.

Proposition 3.3.5. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size $n = 8$ containing no three collinear points. Let $\mathbf{F}$ be the family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup isomorphic to $C_2 \times C_4$ of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$. Then $|\mathbf{F}| \leq 1$.*

For $T \cong C_8$, assertion (i) only ensures one extra-point for every permutation π. Nevertheless, with some more effort, this is enough to prove a result analogous to Proposition 3.3.5. For this purpose, the following technical lemma is useful.

Lemma 3.3.6. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 8 containing no three collinear points. Let $\mathbf{F}$ be the family of irreducible cubics passing through every point in Ω such that Ω coincides with a coset of a cyclic subgroup of the group of $\mathcal{F}$ for every $\mathcal{F} \in \mathbf{F}$. Then the assertions below hold.*

(i) *The cubics in $\mathbf{F}$ have a common inflection point S.*

(ii) *There is an involutory homology φ with center S preserving each cubic in $\mathbf{F}$.*

(iii) *Each of the four lines joining S and a point in Ω is a bisecant of Ω.*

Proof. Let $\mathcal{F}_1, \mathcal{F}_2 \in \mathbf{F}$ be two distinct cubics. From Proposition 3.3.2, there exist four distinct points P_1, P_2, P_3, P_4 in Ω such that the meeting point S of the lines ℓ_1 and ℓ_2 is a common point of $\mathcal{F}_1$ and $\mathcal{F}_2$. Here ℓ_1 stands for the line through P_1 and P_2, while ℓ_2 for that through P_3 and P_4.

The pencil generated by $\mathcal{F}_1$ and $\mathcal{F}_2$ has all its base points in $\Omega \cup \{S\}$. For a non-base point $L_1 \in \ell_1$, the pencil contains a (unique) cubic curve $\mathcal{D}_1$ passing through L_1. Obviously, $\mathcal{D}_1$ is reducible as it contains the line ℓ_1. Hence $\mathcal{D}_1$ splits into ℓ_1 and

a conic $\mathcal{C}_1$. Since no three points in Ω are collinear, $\mathcal{C}_1$ contains six points, namely $P_3, P_4, P_5, P_6, P_7, P_8$, no three of them collinear. Therefore $\mathcal{C}_1$ is an irreducible conic, and it does not contain S. For $5 \leq i \leq 8$, S is the tangential point of a point P_i if and only if the line through S and P_i is tangent to $\mathcal{C}_1$ at P_i. So, at most two such points P_i exist. This and Lemma 3.3.1, imply that there is a point, say P_5, such that the line through S and P_5 meets Ω in a point, say P_6, other than P_5. Let ℓ_3 denote that line.

Let τ_1 be the (unique) involutory homology with center S that preserves $\mathcal{C}_1$. Then τ_1 interchanges P_5 with P_6. Furthermore, τ_1 preserves ℓ_1 and hence it preserves $\mathcal{D}_1$, as well.

The above argument may be repeated for ℓ_2. There is a (unique) involutory homology τ_2 with center S that preserves an irreducible conic $\mathcal{C}_2$ through the six points in $P_1, P_2, P_5, P_6, P_7, P_8$. The action of τ_2 on $\{P_5, P_6, P_7, P_8\}$ is the same as τ_1. Furthermore, τ_2 preserves ℓ_2 and hence it preserves $\mathcal{D}_2$, as well.

Therefore $\tau_1\tau_2$ fixes four points, no three of them collinear. This is only possible when $\tau_1 = \tau_2$.

Similarly, replacing ℓ_1 with ℓ_3 in the previous argument provides the existence of a (unique) involutory homology τ_3 with center S that preserves an irreducible conic $\mathcal{C}_3$ through the six points in $P_1, P_2, P_3, P_4, P_7, P_8$. Furthermore, τ_3 preserves ℓ_3 and hence it preserves $\mathcal{D}_3$, as well. Again, $\tau_1 = \tau_3$.

Let $\varphi = \tau_1$. Then φ preserves $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$ which are three members of the pencil generated by $\mathcal{F}_1$ and $\mathcal{F}_2$. Therefore, τ_1 preserves each member. In particular, φ preserves both $\mathcal{F}_1$ and $\mathcal{F}_2$. The center of an involutory homology preserving a non–singular cubic $\mathcal{F}$ is an inflection point of $\mathcal{F}$. Therefore, S is a common inflection point of $\mathcal{F}_1$ and $\mathcal{F}_2$. Since $3 \nmid |T|$, Lemma 3.3.1 shows that S is determined by $\mathcal{F}_1$, that is, S is not changed when $\mathcal{F}_2$ is replaced by another cubic from $\mathbf{F}$.

Since φ fixes no point in Ω, the final assertion is also proven. $\square$

Proposition 3.3.7. *Let Ω be a point-set of size 8 containing no three collinear points. Let $\mathbf{F}$ be the family of pairwise distinct cubics passing through every point in Ω, where Ω coincides with a coset of a cyclic subgroup of $(\mathcal{F}, +)$ for every $\mathcal{F} \in \mathbf{F}$. Then $|\mathbf{F}| \leq 2$.*

Proof. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two distinct cubics from $\mathbf{F}$. With the notation introduced in the proof of Lemma 3.3.6, S is the (unique) common inflection point of $\mathcal{F}_1$ and $\mathcal{F}_2$, and the points in Ω are $P_0, P_1, \ldots, P_7$ such that the each of the four chords $P_1P_6, P_2P_5, P_3P_4, P_7P_0$ passes through Q. In terms of the relative group laws where S is assumed to be the zero element of the group,

$$0 = P_1 + P_6 = P_2 + P_5 = P_3 + P_4 = P_7 + P_0$$
$$0 = P_1 \boxplus P_6 = P_2 \boxplus P_5 = P_3 \boxplus P_4 = P_7 \boxplus P_0.$$

By hypothesis, there exists $g \in (\mathcal{F}_1, +)$ such that $P_i = g + t_i$ for $i = 0, 1, \ldots 7$. Then $2g = -(t_i + t_{7-i}) = t^* \in T_1$ for $i = 0, 1, 2, 3$. Since the points P_i are pairwise distinct, the equation $t^* = 2t$ is unsolvable in T_1. Let e be the involution in T_1. Then e is the third point in $\mathcal{F}_1$ of the chord of Ω through the points $g - t^* - t$ and $g + e + t$, for any $t \in T_1$. So e, like S, is the common point of four chords of Ω.

To do some more computation, it is useful to identify T_1 with $(\mathbb{Z}/8\mathbb{Z}, +)$. Then $t^* \in \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, and $e = \bar{4}$. As the automorphism group of $(\mathbb{Z}/8\mathbb{Z}, +)$ acts transitively on the set $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, relabeling the elements in T_1 allows us to assume that $t^* = \bar{1}$. With our choice, the chords of Ω through $\bar{4}$ are the lines joining the points $g + \overline{7 - i}$ and $g + \overline{4 + i}$ while either $P_i = g + \bar{i}$ or $P_i = g + \overline{7 - i}$ for every $0 \leq i \leq 7$. The latter ambiguity gives rise to sixteen possibilities. If

$$(P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7) =$$
$$(g + \bar{0}, g + \bar{1}, g + \bar{2}, g + \bar{3}, g + \bar{4}, g + \bar{5}, g + \bar{6}, g + \bar{7});$$

then the four chords of Ω through $\bar{4}$ are

$$g+\bar{0}, g+\bar{3};\ g+\bar{1}, g+\bar{2};\ g+\bar{5}, g+\bar{6};\ g+\bar{4}, g+\bar{7},$$

that is, P_0P_3; P_1P_2; P_5P_6; P_4P_7. Similarly, for

$$\begin{aligned}&(P_0, P_1, P_2, P_3, P_4, P_5.P_6, P_7) =\\ &(g+\bar{7}, g+\bar{1}, g+\bar{2}, g+\bar{3}, g+\bar{4}, g+\bar{5}, g+\bar{6}, g+\bar{0}),\end{aligned}$$

the four chords of Ω through $\bar{4}$ are P_7P_3; P_1P_2; P_5P_6; P_4P_0.

Now, a straightforward computation shows that the sixteen possibilities provide only four cases, namely

$$\begin{aligned}&P_1P_2;\ P_3P_0;\ P_4P_7;\ P_5P_6;\ \ P_1P_5;\ P_2P_6;\ P_3P_0;\ P_4P_7;\\ &P_1P_2;\ P_3P_7;\ P_4P_0;\ P_5P_6;\ \ P_1P_5;\ P_2P_6;\ P_3P_7;\ P_4P_0.\end{aligned} \tag{3.4}$$

Obviously, the first with the third, and the second with the forth are inconsistent.

The above argument applies to $\mathcal{F}_2$ (and to every cubic $\mathcal{F} \in \mathbf{F}$). If $\mathbf{F}$ contained at least three cubics then (3.4) would yield that two of them have two extra-points, but this is impossible as they are distinct. □

3.3.3 n=7.

To deal with the case $n = 7$, a similar approach is used.

Lemma 3.3.8. *In $PG(2, \mathbb{K})$, let Ω be a point-set of size 7 containing no three collinear points. Let $\mathbf{F}$ be the family of pairwise distinct cubics passing through every point in Ω which Ω coincides with a coset of a cyclic subgroup of every $\mathcal{F} \in \mathbf{F}$. Assume that $\mathbf{F}$ contains at least six cubics. Then at least five of any six cubics in $\mathbf{F}$ form a subfamily $\mathbf{F}'$ in which* (i) *and* (ii) *of Lemma 3.3.6 hold but* (iii) *in that Lemma is to be replaced by*

(iii') *One line joining S to a point in Ω is a tangent to every $\mathcal{F} \in \mathbf{F}$ at that point while each of the other three lines joining S and a point in Ω is a bisecant of Ω.*

Proof. Let $\mathcal{F}_1, \mathcal{F}_2 \in \mathbf{F}$ be two distinct cubics which have a common extra-point. Then the proof of Lemma 3.3.6 can be adapted with just one formal change, namely P_7 and P_8 denote the same point while P_7P_8 stands for the common tangent to $\mathcal{F}_1$ and $\mathcal{F}_2$ at P_7. Therefore, (i), (ii) and (iii') hold within the subfamily $\mathbf{F}'$ of $\mathbf{F}$ consisting of all cubics $\mathcal{F}$ such that $\mathcal{F}_1$ and $\mathcal{F}$ have an extra-point S. Furthermore, $\Omega \setminus \{P_0\}$ lies in an irreducible conic $\mathcal{C}_1$ where P_7S is the common tangent to $\mathcal{F}_1$ and $\mathcal{F}_2$ at P_7.

Take four cubics $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \mathcal{F}_4$ such that $\mathcal{F}_2 \in \mathbf{F}'$ and $\mathcal{F}_4$ in the subfamily $\mathbf{F}'_1$ of $\mathbf{F}$ consisting of all cubics $\mathcal{F}$ such that $\mathcal{F}_3$ and $\mathcal{F}$ have an extra-point. We prove that $\mathcal{F}_3, \mathcal{F}_4 \in \mathbf{F}'$.

For this purpose, observe that the results so far proved apply to $\mathcal{F}_3$ and $\mathcal{F}_4$. In particular, $\Omega \setminus \{P'_7\}$ lies in an irreducible conic $\mathcal{C}_2$ where S' the extra-point of $\mathcal{F}_3$ and $\mathcal{F}_4$ so that $S'P'_7$ is their common tangent at P'_7. Since $\Omega \setminus \{P_7, P'_7\}$ contains five distinct points, $\mathcal{C}_1 = \mathcal{C}_2$ must hold. Hence $\mathcal{C}_1$ must contain Ω. On the other hand $\mathcal{C}_1$ meets $\mathcal{F}_1$ in at most six points. This is only possible when $S = S'$ and $P_7 = P'_7$. Therefore S is a common extra-point of $\mathcal{F}_1$, $\mathcal{F}_3$ and $\mathcal{F}_4$.

Now take six pairwise distinct cubics from $\mathcal{F}_1, \mathcal{F}_2 \in \mathbf{F}$. They are considered as the six vertices of a graph $\mathcal{G}_6$ in which two vertices are connected by an edge if and only if they represent cubics with a common extra-point. From (iii) of Lemma 3.3.3, the subgraph of three distinct vertices in the graph contains at least one edge. Now look at a subgraph of four vertices, briefly called a quadrangle, and interpret the previous result on $\mathbf{F}'$: In any quadrangle, if the edges cover each of the four vertices, then the quadrangle is clique, that is the quadrangle is the complete graph. Therefore, either $\mathcal{G}_6$ is itself the complete graph, or there is a unique isolated vertex, that is, deleting it from $\mathcal{F}_6$ produces the complete graph $\mathcal{G}_5$. This shows that there are at least five

cubics all having the same extra-point S. $\square$

Proposition 3.3.9. *In $PG(2,\mathbb{K})$, let Ω be a point-set of size 7 containing no three collinear points. Let $\mathbf{F}$ be the family of pairwise distinct cubics passing through every point in Ω which Ω coincides with a coset of a subgroup of every $\mathcal{F} \in \mathbf{F}$. Then $|\mathbf{F}| \leq 5$.*

Proof. Assume on the contrary that $\mathbf{F}$ contains at least six cubics. From Lemma 3.3.8, there exists $\mathcal{F}_1$ such that $\mathbf{F}'$ contains five cubics; these cubics have the same extra-point S and the same tangent SP_0 at a point $P_0 \in \Omega$. Let $\mathcal{F}_1, \mathcal{F}_2$ denote any two of those cubics, equipped with the relative group laws $(\mathcal{F}_1, +)$ and $(\mathcal{F}_2, \boxplus)$.

From (ii) Lemma 3.3.6 and Lemma 3.3.8, S is a common inflection point of $\mathcal{F}_i$. The points in Ω are $P_0, P_1, \ldots, P_6$ such that the each of the three chords P_1P_6, P_2P_5, P_3P_4 passes through S, and SP_0 is the common tangent at the point P_0. In terms of group laws where S is assumed to be zero element of the group, two points Ω are collinear with S if and only if they are opposite to each other. Therefore,

$$0 = 2P_0 = P_1 + P_6 = P_2 + P_5 = P_3 + P_4$$
$$0 = 2P_0 = P_1 \boxplus P_6 = P_2 \boxplus P_5 = P_3 \boxplus P_4.$$

Let $P_0 = t + g \in \Omega$. Then $2(g+t) = 0$, and replacing g with $g+t$ allows us to assume that $2g = 0$, that is, $t^* = 0$.

To do computation, it is useful to identify T_1 with $(\mathbb{Z}/7\mathbb{Z}, +)$. Then either $P_i = g + \bar{i}$ or $P_i = g + \overline{7-i}$ for every $1 \leq i \leq 6$. Relabeling the indices of the points in $\Omega \setminus \{P_0\}$ allows us to set $P_i = g + \bar{i}$ for $i = 1, \ldots, 6$.

Let π be the permutation on $\Omega = \mathcal{I}_7$ arising from π. Then

$$0 = 0^\pi = 1^\pi + 6^\pi = 2^\pi + 5^\pi = 3^\pi + 4^\pi \pmod 7.$$

There exist 48 such permutations and they form a subgroup M of Sym_7. The elements of M are considered as the 48 vertices of a graph $\mathcal{G}_{48}$ in which two vertices π, σ are

connected by an edge if and only if both equations

$$x_1^\pi + x_2^\pi = x_3^\pi + x_4^\pi \pmod 7 \text{ and } x_1^\sigma + x_2^\sigma = x_3^\sigma + x_4^\sigma \pmod 7$$

with $1 \leq x_1 < x_2$, $x_1 < x_3$, $x_3 < x_4 \leq 7$ only hold when

$$x_1 + x_2 = x_3 + x_4 = 0 \pmod 7.$$

A computer aided exhaustive search performed by MAGMA shows that $\mathcal{G}_{48}$ contains no clique with more than four vertices. This implies that we have only four choices for $\mathcal{F}_2$ in $\mathbf{F}'$, a contradiction. □

Proposition 3.3.10. *In $PG(2,\mathbb{K})$, let Ω be a point-set of size 6 containing no three collinear points. Let $\mathbf{F}$ be the family of pairwise distinct cubic cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup of every $\mathcal{F} \in \mathbf{F}$. Then either $|\mathbf{F}| \leq 4$, or $|\mathbf{F}| = 10$ and Ω is a Clebsch hexagon.*

Proof. Given a cubic $\mathcal{F} \in \mathbf{F}$, let T be a (cyclic) subgroup of $(\mathcal{F}, +)$ which has a coset coinciding with Ω, and identify T with $(\mathbb{Z}/6\mathbb{Z}, +)$ and Ω with $P_i = g + \bar{i}$ for $0 \leq i \leq 5$. The projection of Ω onto itself from a satellite point $Q_i = -2g + \bar{i}$ defines an involutory permutation τ_{6-i} for every $i = 0, 1, \ldots, 5$ where

$$\begin{aligned} &\tau_0 = (P_0)(P_3)(P_1P_5)(P_2P_4); \quad \tau_1 = (P_0P_1)(P_2P_5)(P_3P_4); \\ &\tau_2 = (P_0P_2)(P_1)(P_3P_5)(P_4); \quad \tau_3 = (P_0P_3)(P_1P_2)(P_4P_5); \\ &\tau_4 = (P_0P_4)(P_1P_3)(P_2)(P_5); \quad \tau_5 = (P_0P_5)(P_1P_4)(P_2P_3). \end{aligned} \tag{3.5}$$

A straightforward computation shows that the permutation group $D(\mathcal{F})$ on Ω generated by all τ_i is a dihedral group of order 12. This gives rise to a map

$$\mu_{12} : \mathcal{F} \to D(\mathcal{F})$$

from $\mathbf{F}$ to the set of dihedral subgroups of order 12 in the symmetric group Sym_Ω on Ω. Observe that μ_{12} is injective because two distinct cubics in $\mathbf{F}$ have at most three common satellite points.

Furthermore, the map $x \to x + \bar{2}$ preserving $\mathcal{F}$ has order 3 and hence it is the restriction of a projectivity $\sigma(\mathcal{F})$ on $\mathcal{F}$. Obviously, $\sigma(\mathcal{F})$ has order 3 and acts on Ω as the even permutation

$$\tau = (P_0P_2P_4)(P_1P_3P_5).$$

Also, $D(\mathcal{F})$ is in the normalizer N of the subgroup M generated by τ. Let $\Sigma(\mathcal{F})$ denote the projectivity group generated by $\sigma(\mathcal{F})$. It may happen that $\Sigma(\mathcal{F}) = \Sigma(\mathcal{F}')$ for another $\mathcal{F} \in \mathbf{F}$ and we investigate this possibility first.

For a $\mathcal{F} \in \mathbf{F}$, let $\mathbf{F}'$ be the subfamily of $\mathbf{F}$ consisting of all $\mathcal{F}'$ for which $\Sigma(\mathcal{F}) = \Sigma(\mathcal{F}')$. The above discussion about $\mathcal{F}$ holds true for any $\mathcal{F}' \in \mathbf{F}'$. Therefore, $D(\mathcal{F}')$ is a dihedral group of order 12 and it is contained in N. From a straightforward computation, N has order 36 and it has only three dihedral subgroups of order 12 containing $\sigma(\mathcal{F})$. This shows that $|\mathbf{F}'| \leq \mathbf{3}$, that is, we have only two possibilities for $\mathcal{F}' \in \mathbf{F}'$ other than $\mathcal{F}$, say $\mathcal{F}'$ and $\mathcal{F}''$. A straightforward computation shows that $D(\mathcal{F})$, $D(\mathcal{F}')$ and $D(\mathcal{F}'')$ are pairwise conjugate in Alt_Ω as

$$\begin{aligned} D(\mathcal{F}') &= u_1^{-1}D(\mathcal{F})u_1, \quad \text{with } u_1 = (P_1P_5)(P_2P_0), \\ D(\mathcal{F}'') &= u_2^{-1}D(\mathcal{F})u_2, \quad \text{with } u_2 = (P_2P_4)(P_3P_5). \end{aligned} \tag{3.6}$$

Furthermore, the non-central involutory permutations in $\mathcal{D}(\mathcal{F}')$ are

$$\begin{aligned} \tau_0' &= (P_1P_5)(P_4P_0)(P_2)(P_3); \quad \tau_1' = \tau_1; \\ \tau_2' &= (P_1P_3)(P_2P_0)(P_4)(P_5); \quad \tau_3' = \tau_3; \\ \tau_4' &= (P_0)(P_1)(P_2P_4)(P_3P_5); \quad \tau_5' = \tau_5; \end{aligned} \tag{3.7}$$

while those in $\mathcal{D}(\mathcal{F}'')$ are

$$\begin{aligned} \tau_0'' &= (P_1P_3)(P_2P_4)(P_0)(P_5); \quad \tau_1'' = \tau_1; \\ \tau_2'' &= (P_1)(P_2)(P_3P_5)(P_4P_0); \quad \tau_3'' = \tau_3; \\ \tau_4'' &= (P_1P_5)(P_2P_0)(P_3)(P_4); \quad \tau_5'' = \tau_5; \end{aligned} \tag{3.8}$$

The involutory permutations τ_i' (resp. τ_i'') uniquely determine the satellite points of $\mathcal{F}'$ and $\mathcal{F}''$, respectively. This shows that the satellite point $Q_i = -2g + \bar{i}$ of $T + g$ for $i = 1, 3, 5$ is also common points of $\mathcal{F}$, $\mathcal{F}'$ and $\mathcal{F}''$.

Therefore, the map

$$\mu_3 : \mathcal{F} \to \Sigma(\mathcal{F})$$

may not be injective. If this happens then either two or three cubics from $\mathbf{F}$ have the same image under μ_3.

Now the case where $\mathbf{F}$ contains two cubics $\mathcal{F}_1, \mathcal{F}_2$ with $\Sigma(\mathcal{F}_1) \neq \Sigma(\mathcal{F}_2)$ is investigated. Consider the projectivity group $\Gamma(\mathbf{F})$ generated by all $\Sigma(\mathcal{F})$ with $\mathcal{F} \in \mathbf{F}$. Obviously, $\Gamma(\mathbf{F})$ preserves Ω and acts faithfully on it as a permutation group. Therefore, $\Gamma(\mathbf{F})$ is isomorphic to a subgroup of Alt_6 and such a subgroup is generated by a set of permutations of order 3 each being the product of two disjoint 3-cycles.

It is known from classical geometry that Alt_6 cannot act as a projectivity group with an invariant point-set $\mathcal{M}$ consisting of six points no three of them collinear.

A short proof valid in characteristic $p \neq 2$ relies on the fact that the 2-point stabilizer of Alt_6 has three involutions while a projectivity group preserving $\mathcal{M}$ and fixing two distinct points, say P, Q, in $\mathcal{M}$ contains at most one involution. The existence of two such involutions, φ_1, φ_2, leads indeed to a contradiction due to the following argument. The center C_1 of φ_1 is outside $\mathcal{M}$ otherwise, for any point $R \in \mathcal{M}$ other than those fixed by φ_1, the points $R, \varphi_1(R)$ and C_1 would be collinear in $\mathcal{M}$, a contradiction. Therefore, the line ℓ_1 through P and Q is the axis of φ_1. The same holds for the axis ℓ_2 and the center C_2 of φ_2. Since $\ell_1 = \ell_2$, the projectivity $\varphi_1\varphi_2$ also fixes ℓ_1 pointwise. By $p \neq 2$, both C_1 and C_2 are outside ℓ_1. Note that $C_1 = C_2$ would imply that φ_1 and φ_2 are two involutions in the perspectivity group (C_1, ℓ_1) which is cyclic. Hence $C_1 \neq C_2$, and the subgroup generated by φ_1 and φ_2 contains a elation τ with axis ℓ. Again, for any point $R \in \mathcal{M}$ other than those fixed by τ, the

points $R, \tau(R)$ and $\tau^2(R)$ would be collinear points in $\mathcal{M}$, and hence τ^2 would be the identity. On the other hand, the order of any elation is equal to p. But this would imply $p = 2$, a contradiction.

From the classification of subgroups of Alt_6, there are only two possibilities for the abstract structure of $\Gamma(\mathbf{F})$, namely $\Gamma(\mathbf{F}) \cong \mathrm{Alt}_4$ or $\Gamma(\mathbf{F}) \cong \mathrm{Alt}_5$.

We begin with the case $\Gamma(\mathbf{F}) \cong \mathrm{Alt}_4$.

A straightforward computation shows that $\sigma(\mathcal{F})$ is contained in three subgroups of Sym_Ω which are isomorphic to Alt_4, namely

$$\begin{aligned} V_1 &= \langle \sigma(\mathcal{F}), (P_0P_1P_4)(P_2P_3P_5) \rangle; \\ V_2 &= \langle \sigma(\mathcal{F}), (P_0P_4P_3)(P_1P_5P_2) \rangle; \\ V_3 &= \langle \sigma(\mathcal{F}), (P_0P_5P_4)(P_1P_3P_2) \rangle. \end{aligned} \tag{3.9}$$

The set $\{Q_1, Q_3, Q_5\}$ is contained in three sets of size 6 each being a point-orbit of one of the projectivity groups V_1, V_2 and V_3. In terms of projection on Ω, these points other than Q_1, Q_3, Q_5 are determined by the conjugates $\alpha_i, \alpha_i', \alpha_i''$ of the involutions τ_1, τ_3, τ_5 under the elements in V_i with $i = 1, 2, 3$:

$$\alpha_1 = (P_0P_4)(P_1P_2)(P_3P_5), \alpha_1' = (P_0P_2)(P_1P_5)(P_3P_4), \alpha_1'' = (P_0P_5)(P_1P_3)(P_2P_4),$$
$$\alpha_2 = (P_0P_2)(P_1P_3)(P_4P_5), \alpha_2' = (P_0P_4)(P_1P_5)(P_2P_3), \alpha_2'' = (P_0P_1)(P_2P_4)(P_3P_5),$$
$$\alpha_3 = (P_0P_3)(P_2P_4)(P_1P_5), \alpha_3' = (P_0P_4)(P_1P_3)(P_2P_5), \alpha_3'' = (P_0P_3)(P_1P_5)(P_2P_4).$$

Comparing α_1 and τ_2'' shows that the chord P_1P_2 must pass through the satellite point Q_2''. But this is impossible, since $Q_2''P_1$ and $Q_2''P_2$ are tangent to $\mathcal{F}''$ at the points P_1 and P_2. This contradiction shows that if V_1 occurs then $\mathcal{F}''$ does not exist. Similarly, V_2 and $\mathcal{F}'$, as well as, V_3 and $\mathcal{F}$ are inconsistent.

Therefore, if V_1 occurs then $\mathbf{F}$ comprises either two cubics, namely $\mathcal{F}, \mathcal{G}$ or four cubics $\mathcal{F}, \mathcal{G}, \mathcal{F}', \mathcal{G}'$ where $\mathcal{G}$ (resp. $\mathcal{G}'$) is the image of $\mathcal{F}$ (resp. $\mathcal{F}'$) by a projectivity from $V_1 \setminus \Sigma(\mathcal{F})$. Analog result holds for V_2 and V_3. In the former case, μ_3 is injective, while, in the latter case, two different cubics from $\mathcal{F}$ have the same image.

Next we deal with case $\Gamma(\mathbf{F}) \cong \mathrm{Alt}_5$.

A direct computer aided computation shows that $\sigma(\mathcal{F})$ is contained in exactly three subgroups of Alt_Ω isomorphic to Alt_5, namely $G_{ij} = \langle V_i, V_j \rangle$ with $1 \le i < j \le 3$. From the preceding discussion, $\mathbf{F}$ contains just one from the cubics $\mathcal{F}, \mathcal{F}', \mathcal{F}''$ according as $\Gamma(\mathbf{F})$ coincides with G_{12}, G_{13} or G_{23}. In particular, the map μ_3 is injective. Hence, any two cubics in $\mathbf{F}$ are projectively equivalent under $\Gamma(\mathbf{F})$ as any two product of disjoint 3-cycles on Ω are conjugate under Sym_6.

Assume that $\Gamma(\mathbf{F}) = G_{12}$. With the classical terminology, see [5], Ω is a Clebsch hexagon, and $-2g + \bar{i}$ with $i = 1, 3, 5$ are three of the ten Brianchon points, while $-2g + \bar{i}$ with $i = 0, 2, 4$ are the centers of three of the fifteen involutory perspectivities in $\Gamma(\mathbf{F})$. In the latter case, if the point $-2g + \bar{2}j$ with $j = 1, 3, 5$ is the center of such an involutory perspectivity σ_i then the fixed points in Ω are $g - \bar{j}$ and $g - \overline{(3 + j)}$.

Since Alt_5 has exactly ten dihedral subgroups of order 6 each containing three involutions, the centers of the fifteen involutory perspectivities $\Gamma(\mathbf{F})$ lie on ten lines each containing three such centers. Every Brianchon point is by the definition the intersection of three chords of Ω and hence it defines an odd involution on Ω. Therefore, the ten involutions arising from Brianchon points are exactly those in the unique overgroup $H_{12} \cong \mathrm{Sym}_5$ containing Alt_5 but not in Alt_5 itself. As every dihedral subgroup of Alt_5 of order 6 is a subgroup of a dihedral group of Sym_5 of order 12, we obtain ten subsets each consisting of the 6 non-central involutions of a dihedral subgroup of H_{12} of order 12.

As the map μ_3 is injective, this yields that $|\mathbf{F}| \le 10$. On the other hand, the image of any $\mathcal{F} \in \mathbf{F}$ under the action of a projectivity in $\Gamma(\mathbf{F}) \cong \mathrm{Alt}_5$ is still in $\mathbf{F}$. We have already pointed out that the subgroup $\Sigma(\mathcal{F})$ of $\Gamma(\mathbf{F})$ of order 3 preserves $\mathcal{F}$. In Alt_5, a subgroup of order 3 is contained in a dihedral subgroup of order 6 but is not properly contained in another subgroup. Therefore, every $\mathcal{F}$ is preserved by

a subgroup of $\Gamma(\mathbf{F})$ of order 6 and $|\mathbf{F}| = 10$. As a byproduct, every satellite point $-2g+\bar{i}$ of $T+g$ with $i = 0, 2, 4$ is the center of an involutory perspectivity preserving $\mathcal{F}$ and hence it is an inflection point of $\mathcal{F}$. □

3.3.4 n=5.

Proposition 3.3.11. *Let Ω be a point-set of size 5 containing no three collinear points. Let $\mathbf{F}$ be the family of pairwise distinct cubics passing through every point in Ω such that Ω coincides with a coset of a subgroup of every $\mathcal{F} \in \mathbf{F}$. Then either $\mathbf{F} = \emptyset$ or $|\mathbf{F}| = 6$.*

Proof. Given a cubic $\mathcal{F} \in \mathbf{F}$, let T be the (cyclic) subgroup of the group of $\mathcal{F}$ which has a coset coinciding with Ω. We may identify T with $(\mathbb{Z}/5\mathbb{Z}, +)$ and Ω with $P_i = g+\bar{i}$ for $0 \le i \le 5$. The projection of Ω onto itself from a satellite point $Q_i = -2g + \bar{i}$ defines an involutory permutation τ_{5-i} for every $i = 0, 1, \ldots, 5$ where

$$\begin{aligned} &\tau_0 = (P_0)(P_1P_4)(P_2P_3); \quad \tau_1 = (P_0P_2)(P_1)(P_3P_4); \\ &\tau_2 = (P_0P_4)(P_1P_3)(P_2); \quad \tau_3 = (P_0P_1)(P_3)(P_2P_4); \\ &\tau_4 = (P_0P_3)(P_1P_2)(P_4). \end{aligned} \tag{3.10}$$

A straightforward computation shows that the permutation group $D(\mathcal{F})$ on Ω generated by all τ_i is a dihedral group of order 10. This gives rise to a map

$$\mu_{10} : \mathcal{F} \to D(\mathcal{F})$$

from $\mathbf{F}$ to the set of dihedral subgroups of order 10 in Sym_Ω on Ω. Observe that μ_{10} is injective because two distinct cubics in $\mathbf{F}$ have at most four common satellite points. Since Sym_5 has six dihedral groups of order 10, this yields that $|\mathbf{F}| \le 6$. We show that this upper bound is attained.

In a suitable projective reference system (X_1, X_2, X_3) in $PG(2, \mathbb{K})$, let

$$P_1 = (1, 0, 0),\ P_2 = (0, 1, 0),\ P_3 = (0, 0, 1),\ P_4 = (1, 1, 1),\ P_0 = (a, b, 1)$$

where $a, b \in \mathbb{K}$ and each of the elements $a, a-1, b, b-1, a-b$ is distinct from zero.

Let $\Delta = \{M_0, M_1, M_2, M_3, M_4\}$ with

$$M_0 = (a, a, 1), M_1 = (1, b, 1), M_2 = (0, 1, 1), M_3 = (a-b, 0, 1-b), M_4 = (a, b, 0).$$

Since $\Delta \cap \Omega = \emptyset$, the projection of Ω onto itself from M_i defines an involutory permutation μ_i on Ω for every $0 \leq i \leq 4$. A straightforward computation shows that

$$\mu_0 = \tau_1,\ \mu_1 = \tau_3,\ \mu_2 = \tau_0,\ \mu_3 = \tau_2,\ \mu_4 = \tau_4,$$

with τ_i as in (3.10). Furthermore, the plane cubic $\mathcal{F}$ with equation

$$\begin{aligned} &b(b-1)X_1^2X_2 + a(1-b)X_1X_2^2 + ab(1-b)X_1^2X_3 + a(b-a)X_2^2X_3 + \\ &ab(b-a)X_1X_3^2 + a(a-b)X_2X_3^2 + (a^2b - a - b^2 - b)X_1X_2X_3 = 0 \end{aligned} \tag{3.11}$$

passes through the ten points in $\Omega \cup \Delta$, and Ω is a coset of a subgroup of $(\mathcal{F}, +)$ of order 5 whose satellite points are those in Δ.

Analog results hold for five more sets Δ each providing a plane cubic in $\mathbf{F}$.

$$M_0 = (a, b, a), M_1 = (0, b, 1), M_2 = (1, 1, 0), M_3 = (a, 1, 1), M_4 = (a-b, 0, 1-b)$$

with

$$\begin{aligned} &\mu_0 = (P_1)(P_2P_4)(P_0P_3); \quad \mu_1 = (P_4)(P_0P_1)(P_2P_3); \\ &\mu_2 = (P_0)(P_1P_2)(P_3P_4); \quad \mu_3 = (P_0P_2)(P_3)(P_1P_4); \\ &\mu_4 = (P_0P_4)(P_1P_3)(P_2). \end{aligned}$$

and the plane cubic $\mathcal{F}$ of equation

$$\begin{aligned} &a(b-1)X_1^2X_2 + a(1-b)X_1X_2^2 + b(1-b)X_1^2X_3 + a(b-a)X_2^2X_3 + \\ &b(b-a)X_1X_3^2 + ab(a-b)X_2X_3^2 + (ab^2 - a^2b + a^2 - b)X_1X_2X_3 = 0; \end{aligned}$$

$$M_0 = (a, a, 1), M_1 = (1, 0, 1), M_2 = (1-a, 1-b, 0), M_3 = (0, b, 1), M_4 = (a, b, b)$$

with

$$\mu_0 = (P_1)(P_2P_0)(P_3P_4); \quad \mu_1 = (P_0)(P_1P_3)(P_2P_4);$$
$$\mu_2 = (P_3)(P_0P_4)(P_1P_2); \quad \mu_3 = (P_0P_1)(P_4)(P_2P_3);$$
$$\mu_4 = (P_0P_3)(P_1P_4)(P_2);$$

and the plane cubic $\mathcal{F}$ of equation

$$b(b-1)X_1^2X_2 + b(b-a)X_1X_2^2 + ab(b-1)X_1^2X_3 + a(a-1)X_2^2X_3 +$$
$$ab(b-1)X_1X_3^2 + ab(1-b)X_2X_3^2 + (a^2b - a^2 + a - b^2)X_1X_2X_3 = 0.$$

$M_0 = (a, b, a), M_1 = (0, 1, 1), M_2 = (a, 0, 1), M_3 = (b, b, 1), M_4 = (1-a, 1-b, 0)$

with

$$\mu_0 = (P_1)(P_2P_4)(P_0P_3); \quad \mu_1 = (P_0)(P_1P_4)(P_2P_3);$$
$$\mu_2 = (P_4)(P_0P_2)(P_1P_3); \quad \mu_3 = (P_0P_5)(P_2)(P_3P_4);$$
$$\mu_4 = (P_0P_4)(P_1P_2)(P_3);$$

and the plane cubic $\mathcal{F}$ of equation

$$a(b-1)X_1^2X_2 + a(1-a)X_1X_2^2 + b(b-1)X_1^2X_3 + ab(a-1)X_2^2X_3 +$$
$$ab(b-1)X_1X_3^2 + ab(1-b)X_2X_3^2 + (a^2 - ab^2 + b^2 - b)X_1X_2X_3 = 0.$$

$M_0 = (0, a-b, a-1), M_1 = (1, 1, 0), M_2 = (a, b, b), M_3 = (1, b, 1), M_4 = (a, 0, 1)$

with

$$\mu_0 = (P_1)(P_2P_3)(P_0P_4); \quad \mu_1 = (P_0)(P_1P_2)(P_3P_4);$$
$$\mu_2 = (P_2)(P_1P_4)(P_0P_3); \quad \mu_3 = (P_0P_1)(P_3)(P_2P_4);$$
$$\mu_4 = (P_0P_2)(P_1P_3)(P_4);$$

and the plane cubic $\mathcal{F}$ of equation

$$b(a-1)X_1^2X_2 + b(b-a)X_1X_2^2 + b(b-a)X_1^2X_3 + a(a-1)X_2^2X_3 +$$
$$ab(a-b)X_1X_3^2 + a(b-a)X_2X_3^2 + (-a^2b + ab^2 + a - b^2)X_1X_2X_3 = 0.$$

$$M_0 = (0, a-b, a-1), M_1 = (b, b, 1), M_2 = (1, 0, 1), M_3 = (a, b, 0), M_4 = (a, 1, 1)$$

with

$$\mu_0 = (P_1)(P_2P_3)(P_0P_4); \quad \mu_1 = (P_2)(P_0P_1)(P_3P_4);$$
$$\mu_2 = (P_0)(P_1P_3)(P_2P_4); \quad \mu_3 = (P_0P_3)(P_4)(P_1P_2);$$
$$\mu_4 = (P_0P_2)(P_1P_4)(P_3);$$

and the plane cubic $\mathcal{F}$ of equation

$$a(b-1)X_1^2X_2 + a(a-1)X_1X_2^2 + b(b-a)X_1^2X_3 + ab(a-1)X_2^2X_3 +$$
$$b(a-b)X_1X_3^2 + ab(b-a)X_2X_3^2 + (a^2 - ab^2 + b^2 - b)X_1X_2X_3 = 0.$$

□

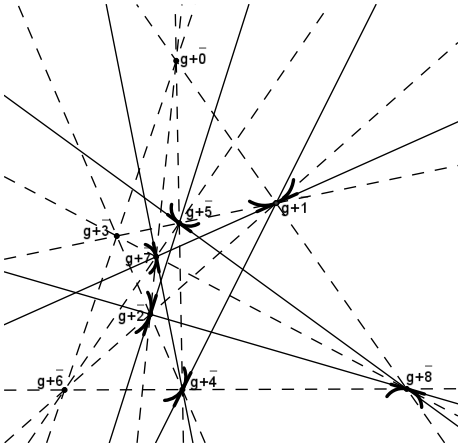

Figure 3.1: $T \cong (\mathbb{Z}/9\mathbb{Z}, +),\ 3g = \bar{0}$

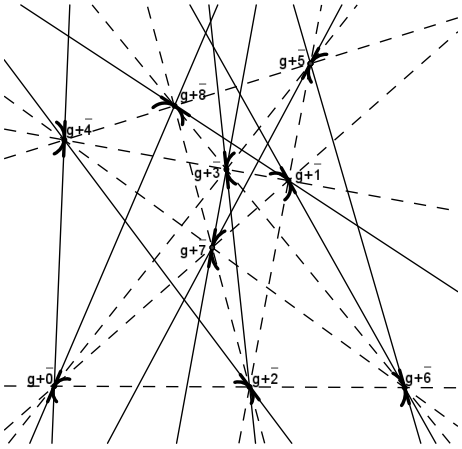

Figure 3.2: $T \cong (\mathbb{Z}/9\mathbb{Z}, +),\ 3g = \bar{1}$

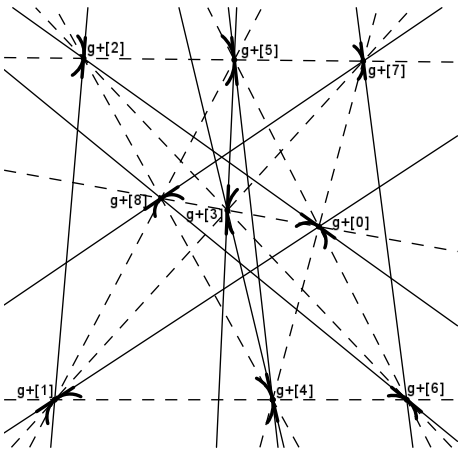

Figure 3.3: $T \cong (\mathbb{Z}/3\mathbb{Z}, +) \times (\mathbb{Z}/3\mathbb{Z}, +),\ 3g = \bar{1}$

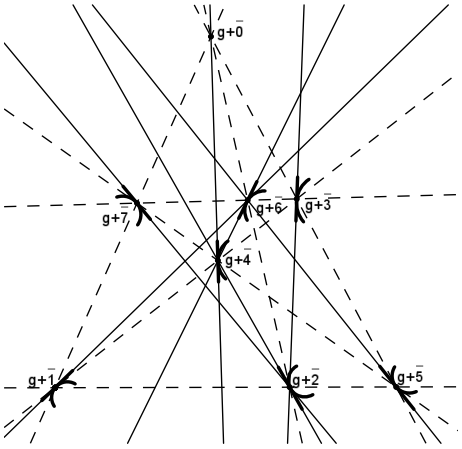

Figure 3.4: $T \cong (\mathbb{Z}/8\mathbb{Z}, +),\ 3g = \bar{0}$

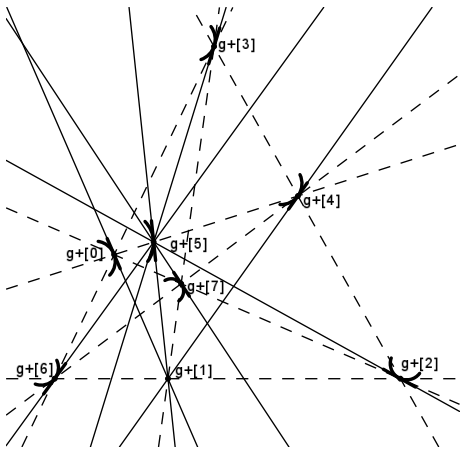

Figure 3.5: $T \cong (\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/4\mathbb{Z}, +),\ 3g = \bar{1}$

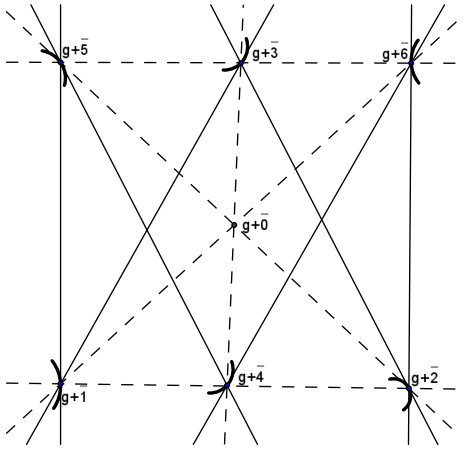

Figure 3.6: $T \cong (\mathbb{Z}/7\mathbb{Z}, +),\ 3g = \bar{0}$

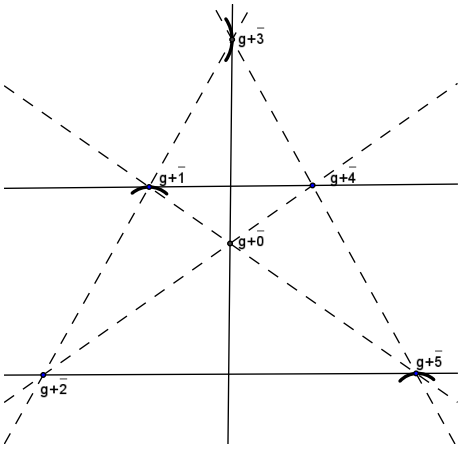

Figure 3.7: $T \cong (\mathbb{Z}/6\mathbb{Z}, +),\ 3g = \bar{0}$

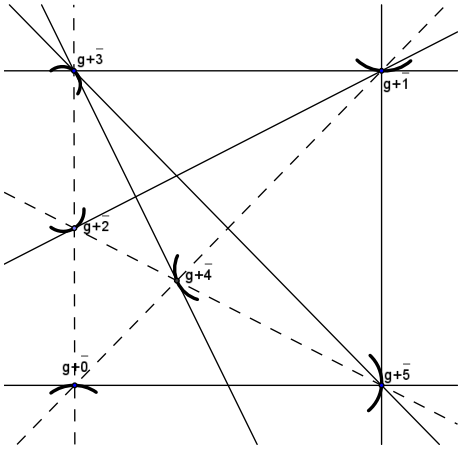

Figure 3.8: $T \cong (\mathbb{Z}/6\mathbb{Z}, +),\ 3g = \bar{1}$

CHAPTER 4

CLASSIFICATION OF 3–NETS

A 3-*net of order* n is a point-line incidence structure consisting of a set $\mathcal{X}$ consisting of n^2 points together with three classes of lines, each consisting of n, lines such that

(i) any two lines from different classes are incident;

(ii) no two lines from the same class are incident;

(iii) any point in $\mathcal{X}$ is incident with exactly one line from each class.

In this chapter, combinatorial methods are used to investigate finite 3-nets embedded in a projective plane $PG(2, \mathbb{K})$ over a field $\mathbb{K}$ of characteristic $p = 0$ or $p > n$. Moreover, we will use the solution of the Coset Intesection Problem (Theorem 3.0.8) to prove Proposition 4.5.1, that is one of the key results in this chapter. We are interested in 3-nets of $PG(2, \mathbb{K})$ which are coordinatized by a group G. If this is the case, we say that the 3-net realizes the group G. In terms of dual 3-nets where $\Lambda_1, \Lambda_2, \Lambda_3$ are the three components, the meaning of this condition is as follows: There exists a triple of bijective maps from G to $(\Lambda_1, \Lambda_2, \Lambda_3)$, say

$$\alpha : G \to \Lambda_1, \beta : G \to \Lambda_2, \gamma : G \to \Lambda_3$$

such that $a \cdot b = c$ if and only if $\alpha(a), \beta(b), \gamma(c)$ are three collinear points, for any $a, b, c \in G$.

Since key examples, such as algebraic 3-nets and tetrahedron type 3-nets, arise naturally in the dual plane of $PG(2, \mathbb{K})$, it is convenient to work with the dual concept

of a 3-net. For this purpose, it is convenient to regard 3-nets in the dual plane of $PG(2,\mathbb{K})$; equivalently consider a dual 3-net in $PG(2,\mathbb{K})$. Here *a dual* 3*-net embedded in* $PG(2,\mathbb{K})$ is a triple $\{\mathcal{A},\mathcal{B},\mathcal{C}\}$ with $\mathcal{A},\mathcal{B},\mathcal{C}$ pairwise disjoint point-sets of size n, called *components*, such that every line meeting two distinct components meets each component in precisely one point. A dual 3-net $(\Lambda_1,\Lambda_2,\Lambda_3)$ realizing a group is *algebraic* if its points lie on a plane cubic, and is of *tetrahedron type* if its components lie on the six sides (diagonals) of a non-degenerate quadrangle in such a way that $\Lambda_i = \Delta_i \cup \Gamma_i$ with Δ_i and Γ_i lying on opposite sides, for $i = 1, 2, 3$.

The main goal of this Chapter is proving that, if $(\Lambda_1,\Lambda_2,\Lambda_3)$ is a dual 3-net which realizes a group G of order n, then one of the following holds.

(I) $(\Lambda_1,\Lambda_2,\Lambda_3)$ is algebraic and G is cyclic or the direct product of two cyclic groups.

(II) $(\Lambda_1,\Lambda_2,\Lambda_3)$ is of tetrahedron type and G is dihedral.

(III) G is the quaternion group of order 8.

(IV) G is the dicyclic group of order 12.

(V) G is the quaternion group of order 16.

(VI) $G \cong C_3 \ltimes C_7$.

(VII) G is the elementary abelian group of order 25.

(VIII) G is the unique group of order 75 containing an elementary abelian normal group of order 25.

(IX) $G = W \ltimes (C_5 \times C_5)$ with a subgroup W of order $2, 4, 8, 16$ where $W \cong C_4 \times C_4$ when $|W| = 16$.

(X) $G \cong \mathrm{Sym}_4$.

(XI) $G \cong \mathrm{Alt}_4$.

(XII) $G \cong \mathrm{Alt}_5$.

Furthermore, if $p = 0$ then the cases (X),(XI),(XII) cannot occur.

4.1 3-NETS, QUASIGROUPS AND LOOPS

In terms of a dual 3-net, the relationship between 3-nets and quasigroups can be described as follows. Let $(L, \cdot)$ be a loop arising from an embeddable 3-net, and consider its dual 3-net with its components $\Lambda_1, \Lambda_2, \Lambda_3$. For $i = 1, 2, 3$, the points in Λ_i are bijectively labeled by the elements of L. Let (A_1, A_2, A_3) with $A_i \in \Lambda_i$ denote the the triple of the points corresponding to the element $a \in L$. With this notation, $a \cdot b = c$ holds in L if and only if the points A_1, B_2 and C_3 are collinear. In this way, points in Λ_3 are *naturally labeled* when $a \cdot b$ is the label of C_3. Let (E_1, E_2, E_3) be the triple for the unit element e of L. From $e \cdot e = e$, the points E_1, E_2 and E_3 are collinear. Since $a \cdot a = a$ only holds for $a = e$, the points A_1, A_2, A_3 are the vertices of a (non-degenerate) triangle whenever $a \neq e$. Furthermore, from $e \cdot a = a$, the points E_1, A_2 and A_3 are collinear; similarly, $a \cdot e = a$ yields that the points A_1, E_2, and A_3 are collinear. However, the points A_1, A_2 and E_3 form a triangle in general; they are collinear if and only if $a \cdot a = e$, i.e. a is an involution of L.

In some cases, it is useful to relabel the points of Λ_3 replacing the above bijection $A_3 \to a$ from Λ_3 to L by the bijection $A_3 \to a'$ where a' is the inverse of a in $(L, \cdot)$. Doing so, three points A_1, B_2, C_3 with $A_1 \in \Lambda_1$, $B_2 \in \Lambda_2$, $C_3 \in \Lambda_3$ are collinear if and only if $a \cdot b \cdot c = e$ with e being the unit element in $(L, \cdot)$. This new bijective labeling will be called a *collinear relabeling* with respect to Λ_3.

Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net that realizes a group $(G, \cdot)$ of order kn containing a subgroup $(H, \cdot)$ of order n. Then the left cosets of H provide a partition of each

component Λ_i into k subsets. Such subsets are called left H-members and denoted by $\Gamma_i^{(1)}, \ldots, \Gamma_i^{(k)}$, or simply Γ_i when this does not cause confusion. The left translation map $\sigma_g : x \mapsto x \cdot g$ preserves every left H-member. The following lemma shows that every left H-member Γ_1 determines a dual 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ that realizes H.

Lemma 4.1.1. *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net that realizes a group $(G, \cdot)$ of order kn containing a subgroup $(H, \cdot)$ of order n. For any left coset gH of H in G, let $\Gamma_1 = gH$, $\Gamma_2 = H$ and $\Gamma_3 = gH$. Then $(\Gamma_1, \Gamma_2, \Gamma_3)$ is a 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realizes H.*

Proof. For any $h_1, h_2 \in H$ we have that $(g \cdot h_1) \cdot h_2 = g \cdot (h_1 \cdot h_2) = g \cdot h$ with $h \in H$. Hence, any line joining a point of Γ_1 with a point of Γ_2 meets Γ_3. □

Similar results hold for right cosets of H. Therefore, for any right coset Hg, the triple $(\Gamma_1, \Gamma_2, \Gamma_3)$ with $\Gamma_1 = H$, $\Gamma_2 = Hg$ and $\Gamma_3 = Hg$ is a 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realizes H.

The dual 3-subnets $(\Gamma_1, \Gamma_2, \Gamma_3)$ introduced in Lemma 4.1.1 play a relevant role. When g ranges over G, we obtain as many as k such dual 3-nets, each being called *a dual 3-net realizing the subgroup H as a subgroup of G*.

Obviously, left cosets and right cosets coincide if and only if H is a normal subgroup of G, and if this is the case we may use the shorter term of coset.

Now assume that H is a normal subgroup of G. Take two H-members from different components, say Γ_i and Γ_j with $1 \leq i < j \leq 3$. From Proposition 2.1.1, there exists a member Γ_m from the remaining component Λ_m, with $1 \leq m \leq 3$ and $m \neq i, j$, such that $(\Gamma_1, \Gamma_2, \Gamma_3)$ is a dual 3-net of realizing $(H, \cdot)$. Doing so, we obtain k^2 dual 3-subnets of $(\Lambda_1, \Lambda_2, \Lambda_3)$. They are all the dual 3-subnets of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realize the normal subgroup $(H, \cdot)$ as a subgroup of $(G, \cdot)$.

Lemma 4.1.2. *Let* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *be a dual* 3*-net that realizes a group* $(G, \cdot)$ *of order* kn *containing a normal subgroup* $(H, \cdot)$ *of order* n*. For any two cosets* g_1H *and* g_2H *of* H *in* G*, let* $\Gamma_1 = g_1H$, $\Gamma_2 = g_2H$ *and* $\Gamma_3 = (g_1 \cdot g_2)H$*. Then* $(\Gamma_1, \Gamma_2, \Gamma_3)$ *is a* 3*-subnet of* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *which realizes* H*.*

If g_1 and g_2 range independently over G, we obtain as many as k^2 such dual 3-nets, each being called *a dual* 3*-net realizing the normal subgroup* H *as a subgroup of* G*.*

4.2 INFINITE FAMILIES OF DUAL 3-NETS REALIZING A GROUP

A dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ with $n \geq 4$ is said to be *algebraic* if all its points lie on a (uniquely determined) plane cubic $\mathcal{F}$, called the *associated* plane cubic of $(\Lambda_1, \Lambda_2, \Lambda_3)$. Algebraic dual 3-nets fall into three subfamilies according as the plane cubic splits into three lines, or in an irreducible conic and a line, or it is irreducible.

4.2.1 Proper algebraic dual 3-nets

An algebraic dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is said to be *proper* if its points lie on an irreducible plane cubic $\mathcal{F}$.

Proposition 4.2.1. *Any proper algebraic dual 3-net* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *realizes a group* M*. There is a subgroup* $T \cong M$ *in* $(\mathcal{F}, +)$ *such that each component* Λ_i *is a coset* $T + g_i$ *in* $(\mathcal{F}, +)$ *where* $g_1 + g_2 + g_3 = 0$*.*

Proof. We do some computation in $(\mathcal{F}, +)$. Let $A_1, A_2, A_3 \in \Lambda_1$ three distinct points viewed as elements in $(\mathcal{F}, +)$. First we show that the solution of the equation in $(\mathcal{F}, +)$

$$A_1 - A_2 = X - A_3 \tag{4.1}$$

belongs to Λ_1. Let $C \in \Lambda_3$. From the definition of a dual 3-net, there exist $B_i \in \Lambda_2$ such that $A_i + B_i + C = 0$ for $i = 1, 2, 3$. Now choose $C_1 \in \Lambda_3$ for which $A_1 + B_2 + C_1 =$

0, and then choose $A^* \in \Lambda_1$ for which $A^* + B_3 + C_1 = 0$. Now,

$$\begin{aligned} A^* - A_3 &= -B_3 - C_1 - (-B_3 - C) = C - C_1 \\ A_1 - A_2 &= -B_2 - C_1 - (-B_2 - C) = C - C_1 \end{aligned} \tag{4.2}$$

Therefore, A^* is a solution of Equation (4.2).

Now we are in a position to prove that Λ_1 is a coset of a subgroup of $(\mathcal{F}, +)$. For $A_0 \in \Lambda_1$, let $T_1 = \{A - A_0 | A \in \Lambda_1\}$. Since $(A_1 - A_0) - (A_2 - A_0) = A_1 - A_2$, Equation (4.2) ensures the existence of $A^* \in \Lambda_1$ for which $A_1 - A_2 = A^* - A_0$ whenever $A_1, A_2 \in \Lambda_1$. Hence $(A_1 - A_0) - (A_2 - A_0) \in T_1$. From this, T_1 is a subgroup of $(\mathcal{F}, +)$, and therefore Λ_1 is a coset $T + g_1$ of T_1 in $(\mathcal{F}, +)$.

Similarly, $\Lambda_2 = T_2 + g_2$ and $\Lambda_3 = T_3 + g_3$ with some subgroups T_2, T_3 of $(\mathcal{F}, +)$ and elements $g_2, g_3 \in (\mathcal{F}, +)$. It remains to show that $T_1 = T_2 = T_3$. The line through the points g_1 and g_2 meets Λ_3 in a point $t^* + g_3$. Replacing g_3 with $g_3 + t^*$ allows to assume that $g_1 + g_2 + g_3 = 0$. Then three points $g_i + t_i$ with $t_i \in T_i$ is collinear if and only if $t_1 + t_2 + t_3 = 0$. For $t_3 = 0$ this yields $t_2 = -t_1$. Hence, every element of T_2 is in T_1, and the converse also holds. From this, $T_1 = T_2$. Now, $t_3 = -t_1 - t_2$ yields that $T_3 = T_1$. Therefore $T = T_1 = T_2 = T_3$ and $\Lambda_i = T + g_i$ for $i = 1, 2, 3$. This shows that $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizes a group $M \cong T$. □

4.2.2 Triangular dual 3-nets

An algebraic dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is *regular* if the components lie on three lines, and it is either of *pencil type* or *triangular* according as the three lines are either concurrent, or they are the sides of a triangle.

Lemma 4.2.2. *Every regular dual 3-net of order n is triangular.*

Proof. Assume that the components of a regular dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ lie on three concurrent lines. Using homogeneous coordinates in $PG(2, \mathbb{K})$, these lines are as-

sumed to be those with equations $Y = 0, X = 0, X - Y = 0$ respectively, so that the line of equation $Z = 0$ meets each component. Therefore, the points in the components may be labeled such that

$$\Lambda_1 = \{(1, 0, \xi) | \xi \in L_1\},\ \Lambda_2 = \{(0, 1, \eta) | \eta \in L_2\},\ \Lambda_3 = \{(1, 1, \zeta) | \zeta \in L_3\},$$

with L_i subsets of $\mathbb{K}$ containing 0. By a straightforward computation, three points $P = (1, 0, \xi)$, $Q = (0, 1, \eta)$, $R = (1, 1, \zeta)$ are collinear if and only if $\zeta = \xi + \eta$. Therefore, $L_1 = L_2 = L_3$ and $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizes a subgroup of the additive group of $\mathbb{K}$ of order n. Therefore n is a power of p. But this contradicts the hypothesis $p > n$. □

For a triangular dual 3-net, the (uniquely determined) triangle whose sides contain the components is called the *associated* triangle.

Proposition 4.2.3. *Every triangular dual* 3*-net realizes a cyclic group isomorphic to a multiplicative group of* $\mathbb{K}$*.*

Proof. Using homogeneous coordinates in $PG(2, \mathbb{K})$, the vertices of the triangle are assumed to be the points $O = (0, 0, 1)$, $X_\infty = (1, 0, 0)$, $Y_\infty = (0, 1, 0)$. For $i = 1, 2, 3$, let ℓ_i denote the fundamental line of equation $Y = 0$, $X = 0$, $Z = 0$ respectively. Therefore the points in the components lie on the fundamental lines and they may be labeled in such a way that

$$\Lambda_1 = \{(\xi, 0, 1) | \xi \in L_1\},\ \Lambda_2 = \{(0, \eta, 1) | \eta \in L_2\},\ \Lambda_3 = \{(1, -\zeta, 0) | \zeta \in L_3\}$$

with L_i subsets of $\mathbb{K}^*$ of a given size n. With this setting, three points $P = (\xi, 0, 1)$, $Q = (0, \eta, 1)$, $R = (1, -\zeta, 0)$ are collinear if and only if $\xi\zeta = \eta$. With an appropriate choice of the unity point of the coordinate system, both $1 \in L_1$ and $1 \in L_2$ may also be assumed. From $1 \in L_1$, we have that $L_2 = L_3$. This together with $1 \in L_2$ imply

that $L_1 = L_2 = L_3 = L$. Since $1 \in L$, L is a finite multiplicative subgroup of $\mathbb{K}$. In particular, L is cyclic. $\square$

Remark 4.2.4. *In the proof of Proposition 4.2.3, if the unity point of the coordinate system is arbitrarily chosen, the subsets L_1, L_2 and L_3 are not necessarily subgroups. Actually, they are cosets of (the unique) multiplicative cyclic subgroup H, say $L_1 = aH$, $L_2 = bH$ and $L_3 = cH$, with $ac = b$. Furthermore, since every $h \in H$ defines a projectivity $\sigma_h : x \mapsto hx$ of the projective line, and these projectivities form a group isomorphic to H, it turns out that L_i is an orbit of a cyclic projectivity group of ℓ_i of order n, for $i = 1, 2, 3$.*

Proposition 4.2.5. *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a triangular dual 3-net. Then every point of $(\Lambda_1, \Lambda_2, \Lambda_3)$ is the center of a unique involutory homology which preserves $(\Lambda_1, \Lambda_2, \Lambda_3)$.*

Proof. The point $(\xi, 0, 1)$ is the center and the line through Y_∞ and the point $(-\xi, 0, 1)$ and is the axis of the involutory homology φ_ξ associated to the matrix

$$\begin{pmatrix} 0 & 0 & \xi^2 \\ 0 & -\xi & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

With the above notation, if $\xi \in aH$ then h_ξ preserves Λ_1 while it sends any point in Λ_2 to a point in Λ_3, and viceversa. Similarly, for $\eta \in bH$ and $\zeta \in cH$ where ψ_η and θ_ζ are the involutory homologies associated to the matrices

$$\begin{pmatrix} -\eta & 0 & 0 \\ 0 & 0 & \eta^2 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 & 0 \\ \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta \end{pmatrix}.$$

$\square$

With the notation introduced in the proof of Proposition 4.2.3, let $\Phi_1 = \{\varphi_\xi \varphi_{\xi'} | \xi, \xi' \in aH\}$ and $\Phi_2 = \{\psi_\eta \psi_{\eta'} | \eta, \eta' \in bH\}$. Then both are cyclic groups isomorphic to H. A direct computation gives the following result.

Proposition 4.2.6. *$\Phi_1 \cap \Phi_2$ is either trivial or has order 3.*

Some useful consequences are stated in the following proposition.

Proposition 4.2.7. *Let $\Theta = \langle \Phi_1, \Phi_2 \rangle$. Then*

$$|\Theta| = \begin{cases} |H|^2, & \text{when gcd.}(3, |H|) = 1; \\ \frac{1}{3}|H|^2, & \text{when gcd.}(3, |H|) = 3. \end{cases}$$

Furthermore, Θ fixes the vertices of the fundamental triangle, and no non-trivial element of Θ fixes a point outside the sides of the fundamental triangle.

We prove another useful result.

Proposition 4.2.8. *If $(\Gamma_1, \Gamma_2, \Gamma_3)$ and $(\Sigma_1, \Sigma_2, \Sigma_3)$ are triangular dual 3-nets such that $\Gamma_1 = \Sigma_1$, then the associated triangles share the vertices on their common side.*

Proof. From Remark 4.2.4, Γ_1 is the orbit of a cyclic projectivity group H_1 of the line ℓ containing Γ_1 while the two fixed points of H_1 on ℓ, say P_1 and P_2, are vertices of the triangle containing $\Gamma_1, \Gamma_2, \Gamma_3$.

The same holds for Σ_1 with a cyclic projectivity group H_2, and fixed points Q_1, Q_2. From $\Gamma_1 = \Sigma_1$, the projectivity group H of the line ℓ generated by H_1 and H_2 preserves Γ_1. Let M be the projectivity group generated by H_1 and H_2.

Observe that M is a projectivity group and it has an orbit of finite size $n \geq 3$, this implies that M is finite. Clearly, $|M| \geq n$ and equality holds if and only if $H_1 = H_2$. If this is the case, then $\{P_1, P_2\} = \{Q_1, Q_2\}$. Therefore, for the purpose of the proof, we may assume on the contrary that $H_1 \neq H_2$ and $|M| > n$.

Now, Dickson's classification of finite subgroups of $PGL(2,\mathbb{K})$ applies to M. From that classification, M is one of the nine subgroups listed as $((1),\ldots,(9)$ in [18, Theorem 1] where e denotes the order of the stabilizer M_P of a point P in a short M-orbit, that is, an M-orbit of size smaller than M. Observe that such an M-orbit has size $|M|/e$. There exist finitely many short M-orbits, and Σ_1 is one of them. It may be that an M-orbit is trivial as it consists of just one point.

Obviously, M is neither cyclic nor dihedral as it contains two distinct cyclic subgroups of the same order $n \geq 3$.

Also, M is not an elementary abelian group E of rank ≥ 2, otherwise we would have $|E| = |M| > n$ since the minimum size of a non-trivial E-orbit is $|E|$, see (2) in [18, Theorem 1].

From (5) in [18, Theorem 1] with $p \neq 2, 3$, the possible sizes of a short Alt_4-orbit are $4, 6$ each larger than 3. On the other hand, Alt_4 has no element of order larger than 3. Therefore, $M \ncong \mathrm{Alt}_4$ for $p \neq 2, 3$.

Similarly, from (5) in [18, Theorem 1] with $p \neq 2, 3$, the possible sizes of a short Sym_4-orbit are $6, 8, 12$ each larger than 4. Since Sym_4 has no element of order larger than 4. Therefore, $M \ncong \mathrm{Sym}_4$ for $p \neq 2, 3$.

Again, from (6) in [18, Theorem 1] with $p \neq 2, 5$, the possible sizes of a short Alt_5-orbit are $10, 12$ for $p = 3$ while $12, 20, 30$ for $p \neq 2, 3, 5$. Each size exceeds 5. On the other hand Alt_5 has no element of order larger than 5. Therefore, $M \ncong \mathrm{Alt}_5$ for $p \neq 2, 5$.

The group M might be isomorphic to a subgroup L of order qk with $k|(q-1)$ and $q = p^h$, $h \geq 1$. Here L is the semidirect product of the unique (elementary abelian) Sylow p-subgroup of L by a cyclic subgroup of order k. No element in L has order larger than k when $h > 1$ and p when $h = 1$. From (7) in [18, Theorem 1], any non-trivial short L-orbit has size q. Therefore $M \cong L$ implies that $h = 1$ and $n = p$.

But this is inconsistent with the hypothesis $p > n$.

Finally, M might be isomorphic to a subgroup L such that either $L = PSL(2, q)$ or $L = PGL(2, q)$ with $q = p^h$, $h \geq 1$. No element in L has order larger than $q + 1$. From (7) and (8) in [18, Theorem 1], any short L-orbit has size either $q+1$ or $q(q-1)$. For $q \geq 3$, if $M \cong L$ occurs then $n = q+1 \geq p+1$, a contradiction with the hypothesis $p > n$. For $q = 2$, we have that $|L| = 6$ which is smaller than 12. Therefore $M \ncong L$.

No possibility has arisen for M. Therefore $\{P_1, P_2\} = \{Q_1, Q_2\}$. □

4.2.3 Conic-line type dual 3-nets

An algebraic dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is of *conic-line type* if two of its three components lie on an irreducible conic $\mathcal{C}$ and the third one lies on a line ℓ. All such 3-nets realize groups and they can be described using subgroups of the projectivity group $PGL(2, \mathbb{K})$ of $\mathcal{C}$. For this purpose, some basic results on subgroups and involutions in $PGL(2, \mathbb{K})$ are useful which essentially depend on the fact that every involution in $PGL(2, \mathbb{K})$ is a perspectivity whose center is a point outside $\mathcal{C}$ and axis is the pole of the center with respect to the orthogonal polarity arising from $\mathcal{C}$. We begin with an example.

Example 4.2.9. *Take any cyclic subgroup C_n of $PGL(2, \mathbb{K})$ of order $n \geq 3$ with $n \neq p$ that preserves $\mathcal{C}$. Let D_n be the unique dihedral subgroup of $PGL(2, \mathbb{K})$ containing C_n. If j is the (only) involution in $\mathcal{Z}(D_n)$ and ℓ is its axis, then the centers of the other involutions in D_n lie on ℓ. We have n involutions in D_n other than j, and the set of the their centers is taken for Λ_1. Take a C_n-orbit $\mathcal{O}$ on $\mathcal{C}$ such that the tangent to $\mathcal{C}$ at any point in $\mathcal{O}$ is disjoint from Λ_1; equivalently, the D_n-orbit $\mathcal{Q}$ be larger than $\mathcal{O}$. Then $\mathcal{Q}$ is the union of $\mathcal{O}$ together with another C_n-orbit. Take these two C_n-orbits for Λ_2 and Λ_3 respectively. Then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is a conic-line dual 3-net which realizes*

C_n. It may be observed that ℓ is a chord of $\mathcal{C}$ and the multiplicative group of $\mathbb{K}$ has a subgroup of order n.

The cyclic subgroups C_n form a unique conjugacy class in $PGL(2,\mathbb{K})$. For a cyclic subgroup C_n of $PGL(2,\mathbb{K})$ of order n, the above construction provides a unique example of a dual 3-net realizing C_n. Using the classification of finite subgroups of $PGL(2,\mathbb{K})$ as in the proof of [2, Theorem 6.1], the following result can be proven. For details, see the preprint [15].

Proposition 4.2.10. *Up to projectivities, the conic-line dual 3-nets of order n are those described in Example* 4.2.9*.*

A corollary of this is the following result.

Proposition 4.2.11. *A conic-line dual 3-net realizes a cyclic group C_n.*

The result below can be proven with an argument similar to that used in the proof of Proposition 4.2.8. For details, see the preprint [15].

Proposition 4.2.12. *Let $(\Gamma_1,\Gamma_2,\Gamma_3)$ and $(\Delta_1,\Delta_2,\Delta_3)$ be two conic-line type dual 3-nets where Γ_3 lies on the line ℓ and Δ_3 lies on the line s. If $\Gamma_1=\Delta_1$ then $\ell=s$.*

4.2.4 Tetrahedron type dual 3-nets

In $PG(2,\mathbb{K})$, any non-degenerate quadrangle with its six sides (including the two diagonals) may be viewed as the projection of a tetrahedron of $PG(3,\mathbb{K})$. This suggests to call two sides of the quadrangle *opposite*, if they do not have any common vertex. With this definition, the six sides of the quadrangle are partitioned into three couples of opposite sides. Let $(\Lambda_1,\Lambda_2,\Lambda_3)$ be a dual 3-net of order $2n$ containing a dual 3-subnet

$$(\Gamma_1,\Gamma_2,\Gamma_3) \tag{4.3}$$

of order n. Observe that $(\Lambda_1, \Lambda_2, \Lambda_3)$ contains three more dual 3-subnets of order n. In fact, for $\Delta_i = \Lambda_i \setminus \Gamma_i$, each of the triples below defines such a subnet:

$$(\Gamma_1, \Delta_2, \Delta_3),\ (\Delta_1, \Gamma_2, \Delta_3),\ (\Delta_1, \Delta_2, \Gamma_3). \tag{4.4}$$

Now, the dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is said to be of *tetrahedron-type* if its components lie on the sides of a non-degenerate quadrangle such that Γ_i and Δ_i are contained in opposite sides, for $i = 1, 2, 3$. Such a non-degenerate quadrangle is said to be *associated* to $(\Lambda_1, \Lambda_2, \Lambda_3)$. Observe that each of the six sides of the quadrangle contains exactly one of the point-sets Γ_i and Δ_i. Moreover, each of the four dual 3-subnets listed in (4.3) and (4.4) is triangular as each of its components, called a *half-set*, lies on a side of a triangle whose vertices are also vertices of the quadrangle. Therefore there are six half-sets in any dual 3-net of tetrahedron type.

Proposition 4.2.13. *Any tetrahedron-type dual* 3*-net realizes a dihedral group.*

Proof. The associated quadrangle is assumed to be the fundamental quadrangle of the homogeneous coordinate system in $PG(2, \mathbb{K})$, so that its vertices are O, X_∞, Y_∞ together with the unity point $E = (1, 1, 1)$. By definition, the subnet (4.3) is triangular. Without loss of generality,

$$\Gamma_1 = \{(\xi, 0, 1) | \xi \in L_1\},\ \Gamma_2 = \{(0, \eta, 1) | \eta \in L_2\},\ \Gamma_3 = \{(1, -\zeta, 0) | \zeta \in L_3\}$$

where $L_1 = aH, L_2 = bH, L_3 = cH$ are cosets of H with $ac = b$, see Remark 4.2.4. We fix such triple $\{a, b, c\}$. Observe that $(a, 0, 1) \in \Gamma_1$, $(0, b, 1) \in \Gamma_2$ and $(1, -c, 0) \in \Gamma_3$. Furthermore,

$$\Delta_1 = \{(1, \alpha, 1) | \alpha \in M_1\},\ \Delta_2 = \{(\beta, 1, 1) | \beta \in M_2\},\ \Delta_3 = \{(1, 1, \gamma) | \gamma \in M_3\}$$

with M_1, M_2 and M_3 subsets of $\mathbb{K} \setminus \{0, 1\}$, each of size n. Now, a direct computation similar those carried out in Section 4.2.2 gives the result. For details, see the preprint [15].

An alternative approach to the proof is to lift $(\Lambda_1, \Lambda_2, \Lambda_3)$ to the fundamental tetrahedron of $PG(3, \mathbb{K})$ so that the projection π from the point $P_0 = (1, 1, 1, 1)$ on the plane $X_4 = 0$ returns $(\Lambda_1, \Lambda_2, \Lambda_3)$. For this purpose, it is enough to define the sets lying on the edges of the fundamental tetrahedron:

$$\begin{aligned}
\Gamma'_1 &= \{(\xi, 0, 1, 0) | \xi \in L_1\}, & \Gamma'_2 &= \{(0, \eta, 1, 0) | \eta \in L_2\}, \\
\Gamma'_3 &= \{(1, -\zeta, 0, 0) | \zeta \in L_3\}, & \Delta'_1 &= \{(0, \alpha - 1, 0, -1) | \alpha \in M_1\}, \\
\Delta'_2 &= \{(\beta - 1, 0, 0, -1) | \beta \in M_2\}, & \Delta'_3 &= \{(0, 0, \gamma - 1, -1) | \gamma \in M_3\},
\end{aligned}$$

and observe that $\pi(\Gamma'_i) = \Gamma_i$ and $\pi(\Delta'_i) = \Delta_i$ for $i = 1, 2, 3$. Moreover, a triple (P_1, P_2, P_3) of points with $P_i \in \Gamma_i \cup \Delta_i$ consists of collinear points if and only if if their projection does. Hence, $(\Gamma'_1 \cup \Gamma'_2, \Gamma'_3 \cup \Delta'_1, \Delta'_2 \cup \Delta'_3)$ can be viewed as a "spatial" dual 3-net realizing the same group H. Clearly, $(\Gamma'_1 \cup \Gamma'_2, \Gamma'_3 \cup \Delta'_1, \Delta'_2 \cup \Delta'_3)$ is contained in the sides of the fundamental tetrahedron. We claim that these sides minus the vertices form an infinite spatial dual 3-net realizing the dihedral group $2.\mathbb{K}^*$.

To prove this, parametrize the points as follows.

$$\begin{aligned}
\Sigma_1 &= \{x_1 = (x, 0, 1, 0), (\varepsilon x)_1 = (0, 1, 0, x) \mid x \in \mathbb{K}^*\}, \\
\Sigma_2 &= \{y_2 = (1, y, 0, 0), (\varepsilon y)_2 = (0, 0, 1, y) \mid y \in \mathbb{K}^*\}, \\
\Sigma_3 &= \{z_3 = (0, -z, 1, 0), (\varepsilon z)_3 = (1, 0, 0, -z) \mid z \in \mathbb{K}^*\}.
\end{aligned} \tag{4.5}$$

Then,

$$\begin{aligned}
x_1, y_2, z_3 \text{ are collinear} &\quad \Leftrightarrow \quad z = xy, \\
(\varepsilon x)_1, y_2, (\varepsilon z)_3 \text{ are collinear} &\quad \Leftrightarrow \quad z = xy \Leftrightarrow \varepsilon z = (\varepsilon x) y, \\
x_1, (\varepsilon y)_2, (\varepsilon z)_3 \text{ are collinear} &\quad \Leftrightarrow \quad z = x^{-1} y \Leftrightarrow \varepsilon z = x(\varepsilon y), \\
(\varepsilon x)_1, (\varepsilon y)_2, z_3 \text{ are collinear} &\quad \Leftrightarrow \quad z = x^{-1} y \Leftrightarrow z = (\varepsilon x)(\varepsilon y).
\end{aligned}$$

Thus, $(\Gamma'_1 \cup \Gamma'_2, \Gamma'_3 \cup \Delta'_1, \Delta'_2 \cup \Delta'_3)$ is a dual 3-subnet of $(\Sigma_1, \Sigma_2, \Sigma_3)$ and H is a subgroup of the dihedral group $2.\mathbb{K}^*$. Also, since H is not cyclic but it has a cyclic subgroup of index 2, we conclude that H is itself dihedral. □

4.3 CLASSIFICATION OF LOW ORDER DUAL 3-NETS

An exhaustive computer aided search gives the following results. For details, see [19] or Chapter 5.

Proposition 4.3.1. *Any dual* 3*-net realizing an abelian group of order* ≤ 8 *is algebraic. The dual of Urzúa's* 3*-nets are the only dual* 3*-net which realize the quaternion group of order* 8*.*

Proposition 4.3.2. *Any dual* 3*-net realizing an abelian group of order* 9 *is algebraic.*

Proposition 4.3.3. *If* $p = 0$*, no dual* 3*-net realizes* Alt_4*.*

4.4 CHARACTERIZATIONS OF THE INFINITE FAMILIES

Proposition 4.4.1. *Every dual* 3*-net realizing a cyclic group is algebraic.*

Proof. For $n = 3$, we have that $3n = 9$, and hence all points of the dual 3-net lie on a cubic. Therefore, $n \geq 4$ is assumed.

Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net of order n which realizes the cyclic group $(L, *)$. Therefore, the points of each component are labeled by I_n. After a collinear relabeling with respect to Λ_3, consider the configuration of the following nine points: $0, 1, 2$ from Λ_1, $0, 1, 2$ from Λ_2 and $n-1, n-2, n-3$ from Λ_3. For the sake of a clearer notation, the point with label a in the component Λ_m will be denoted by a_m.

The configuration presents six triples of collinear points, namely

(i) $\{0_1, 1_2, (n-1)_3\},\ \{1_1, 2_2, (n-3)_3\},\ \{2_1, 0_2, (n-2)_3\}$;

(ii) $\{0_1, 2_2, (n-2)_3\},\ \{1_1, 0_2, (n-1)_3\},\ \{2_1, 1_2, (n-3)_3\}$;

Therefore, the corresponding lines form a Lame configuration. Furthermore, the three (pairwise distinct) lines determined by the two triples in (i) can be regarded as

a totally reducible plane cubic, say $\mathcal{F}_1$. Similarly, a totally reducible plane curve, say $\mathcal{F}_2$, arises from the triples in (ii). Obviously, $\mathcal{F}_1 \neq \mathcal{F}_2$. Therefore, the nine points of the above Lame configuration are the base points of the pencil generated by $\mathcal{F}_1$ and $\mathcal{F}_2$. Now, define the plane cubic $\mathcal{F}$ to be the cubic from the pencil which contains 3_1.

Our next step is to show that $\mathcal{F}$ also contains each of the points $(n-4)_3$ and 3_2. For this purpose, consider the following six triples of collinear points

(iii) $\{1_1, 2_2, (n-3)_3\},\ \{2_1, 0_2, (n-2)_3\},\ \{3_1, 1_2, (n-4)_3\}$;

(iv) $\{1_1, 1_2, (n-2)_3\},\ \{2_1, 2_2, (n-4)_3\},\ \{3_1, 0_2, (n-3)_3\}$;

Again, the corresponding lines form a Lame configuration. Since eight of its points, namely $1_1, 2_1, 3_1, 0_2, 1_2, 2_2, (n-2)_3, (n-3)_3$ lie on $\mathcal{F}$, Lame's theorem shows that $(n-4)_3$ also lies on $\mathcal{F}$. To show that $3_2 \in \mathcal{F}$, we proceed similarly using the following six triples of collinear points

(v) $\{0_1, 3_2, (n-3)_3\},\ \{1_1, 1_2, (n-2)_3\},\ \{2_1, 2_2, (n-4)_3\}$;

(vi) $\{0_1, 2_2, (n-2)_3\},\ \{1_1, 3_2, (n-4)_3\},\ \{2_1, 1_2, (n-3)_3\}$;

to define a Lame configuration that behaves as before, eight of its points, namely $0_1, 1_1, 2_1, 1_2, 2_2, (n-2)_3, (n-3)_3, (n-4)_3$ lie on $\mathcal{F}$, from Lame's theorem, 3_2 also lies on $\mathcal{F}$.

This completes the proof for $n = 4$. We assume that $n \geq 5$ and show that $(n-5)_3$ lies on $\mathcal{F}$. Again, we use the above argument based on the Lame configuration of the six lines arising from the following six triples of points:

(vii) $\{1_1, 3_2, (n-4)_3\},\ \{2_1, 1_2, (n-3)_3\},\ \{3_1, 2_2, (n-5)_3\}$;

(viii) $\{1_1, 2_2, (n-3)_3\},\ \{2_1, 3_2, (n-5)_3\},\ \{3_1, 1_2, (n-4)_3\}$;

From the previous discussion, eight of these points lie on $\mathcal{F}$. Lame's theorem yields that the ninth, namely $(n-5)_3$, also lies on $\mathcal{F}$. From this we infer that $4_1 \in \mathcal{F}$ also holds. To do this, we repeat the above argument for the Lame configuration arising from the six triples of points

(ix) $\{2_1, 2_2, (n-4)_3\},\ \{3_1, 0_2, (n-3)_3\},\ \{4_1, 1_2, (n-5)_3\}$;

(x) $\{2_1, 1_2, (n-3)_3\},\ \{3_1, 2_2, (n-5)_3\},\ \{4_1, 0_2, (n-4)_3\}$;

Again, we see that eight of these points lie on $\mathcal{F}$. Hence the ninth, namely 4_1, also lies on $\mathcal{F}$, by Lame's theorem.

Therefore, from the hypothesis that $\mathcal{F}$ passes through the ten points

$$0_1, 1_1, 2_1, 3_1, 0_2, 1_2, 2_2, (n-1)_3, (n-2)_3, (n-3)_3,$$

we have deduced that $\mathcal{F}$ also passes through the ten points

$$1_1, 2_1, 3_1, 4_1, 1_2, 2_2, 3_2, (n-2)_3, (n-3)_3, (n-4)_3.$$

Comparing these two sets of ten points shows that the latter derives from the former shifting by $+1$ when the indices are 1 and 2, while by -1 in when the indices are 3. Therefore, repeating the above argument $n-4$ times gives that all points in the dual 3-net lie on $\mathcal{F}$. □

Proposition 4.4.2. [25, Theorem 5.4] *If an abelian group G contains an element of order ≥ 10 then every dual 3-net realizing G is algebraic.*

Proposition 4.4.3. [25, Theorem 4.2] *No dual 3-net realizes an elementary abelian group of order 2^h with $h \geq 3$.*

Proposition 4.4.4. [2, Theorem 5.1] *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net such that at least one component lies on a line. Then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is either triangular or of conic-line type.*

Lemma 4.4.5. *Let* $(\Gamma_1, \Gamma_2, \Gamma_3)$ *be an algebraic dual* 3*-net lying on a plane cubic* $\mathcal{F}$*. If* $\mathcal{F}$ *is reducible, then* $(\Gamma_1, \Gamma_2, \Gamma_3)$ *is either triangle or of conic-line type, according as* $\mathcal{F}$ *and splits into three lines or into a line and an irreducible conic.*

Proposition 4.4.6. *Every dual* 3*-net realizing a dihedral group of order* $2n$ *with* $n \geq 3$ *is of tetrahedron type.*

Proof. Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net realizing a dihedral group

$$D_n = \left\langle x, y \mid x^2 = y^n = 1,\ yx = xy^{-1} \right\rangle.$$

Labeling naturally the points in the components Λ_i as indicated in Section 4.1, every $u \in D_n$ defines a triple of points (u_1, u_2, u_3) where $u_i \in \Lambda_i$ for $i = 1, 2, 3$, and viceversa. Doing so, three points $u_1 \in \Lambda_1$, $v_2 \in \Lambda_2$, $w_3 \in \Lambda_3$ are collinear if and only if $uv = w$ holds in D_n.

Therefore, for $1 \leq i \leq n-2$, the triangle with vertices $x_2, (xy)_2, (xy^{-i})_3$ and that with vertices $(1)_3, y_3, (y^{-i})_2$ are in mutual perspective position from the point x_1. For two distinct points u_i and v_j with $u_i \in \Lambda_i$ and $v_j \in \Lambda_j$ and $1 \leq i, j \leq 3$, let $\overline{u_i v_j}$ denote the line through u_i and v_j. From Desargues theorem, the three diagonal points

$$\begin{aligned} U &= \overline{(x)_2(xy)_2} \cap \overline{(1)_3(y)_3}, \\ (y^i)_1 &= \overline{(x)_2(xy^{-i})_3} \cap \overline{(y^{-i})_2(1)_3}, \\ (y^{i+1})_1 &= \overline{(xy)_2(xy^{-i})_3} \cap \overline{(y^{-i})_2(y)_3}, \end{aligned}$$

are collinear. Hence, a line ℓ_1 contains each point $(1)_1, (y)_1 \ldots, (y^{n-1})_1$ in Λ_1, that is,

$$(1)_1, (y)_1 \ldots, (y^{n-1})_1 \in \ell_1.$$

There are some more useful Desargues configurations. Indeed, the pairs of trian-

gles with vertices

$$\begin{aligned}
(x)_2, (xy^{-1})_2, (y^{-i-1})_3 \quad &\text{and} \quad (xy)_3, (x)_3, (y^{-i})_2; \\
(y^i)_2, (y^{i+1})_2, (y^{i+1})_3 \quad &\text{and} \quad (x)_3, (xy)_3, (xy)_2; \\
(xy^i)_2, (xy^{i+1})_2, (y^i)_3 \quad &\text{and} \quad (x)_3, (xy)_3, (1)_2; \\
(1)_2, (y)_2, (x)_3 \quad &\text{and} \quad (y^i)_3, (y^{i+1})_3, (xy^i)_2; \\
(x)_2, (xy)_2, (1)_3 \quad &\text{and} \quad (xy^i)_3, (xy^{i+1})_3, (y^i)_2
\end{aligned}$$

are in mutual perspective position from the points

$$(y^{-1})_1, (xy^{-i})_1, (y^i)_1, (y^i)_1, (y^{-i})_1,$$

respectively. Therefore, there exist five more lines $m_1, \ell_2, m_2, \ell_3, m_3$ such that

$$\begin{aligned}
&\{(x)_1, (xy)_1, \ldots, (xy^{n-1})_1\} \subset m_1, \quad \{(1)_2, (y)_2, \ldots, (y^{n-1})_2\} \subset \ell_2, \\
&\{(x)_2, (xy)_2, \ldots, (xy^{n-1})_2\} \subset m_2, \quad \{(1)_3, (y)_3, \ldots, (y^{n-1})_3\} \subset \ell_3, \\
&\{(x)_3, (xy)_3, \ldots, (xy^{n-1})_3\} \subset m_3.
\end{aligned}$$

By Proposition 4.2.8, the lines $\ell_1, \ldots, m_3$ are the sides of a nondegenarate quadrangle, which shows that the dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is of tetrahedron type. □

Remark 4.4.7. *From Proposition 4.4.6, the dual 3-nets given in [21, Section 6.2] are of tetrahedron type.*

Proposition 4.4.8. *Let G be a finite group containing a normal subgroup H of order $n \geq 3$. Assume that G can be realized by a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ and that every dual 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing H as a subgroup of G is triangular. Then H is cyclic and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is either triangular or of tetrahedron type.*

Proof. From Proposition 4.2.3, H is cyclic. Fix an H-member Γ_1 from Λ_1, and denote by ℓ_1 the line containing Γ_1. Consider all the triangles which contain some dual 3-net

$(\Gamma_1, \Gamma_2^j, \Gamma_3^s)$ realizing H as a subgroup of G. From Proposition 4.2.8, these triangles have two common vertices, say P and Q, lying on ℓ_1. For the third vertex R_j of the triangle containing $(\Gamma_1, \Gamma_2^j, \Gamma_3^s)$ there are two possibilities, namely either the side PR_j contains Γ_2^j and the side QR_j contains Γ_3^s, or viceversa. Therefore, every H-member Γ_2^j from Λ_2 (as well as every H-member Γ_3^s from Λ_3) is contained in a line passing through P or Q.

Now, replace Γ_1 by another H-orbit Γ_1^i lying in Λ_1 and repeat the above argument. If ℓ_i is the line containing Γ_1^i and P_i, Q_i denote the vertices then again every H-member Γ_2^j from Λ_2 (as well as every H-member Γ_3^s from Λ_3) is contained in a line passing through P_i or Q_i.

Assume that $\{P, Q\} \neq \{P_i, Q_i\}$. If one of the vertices arising from Γ_1, say P, coincides with one of the vertices, say P_i, arising from Γ_1^i then the line QQ_i must contain either Γ_2^j or Γ_3^s from each $(\Gamma_1, \Gamma_2^j, \Gamma_3^s)$. Therefore, the line QQ_i must contain every H-member from Λ_2, or every H-member from Λ_3. Hence Λ_2 or Λ_3 lies on the line QQ_i. From Proposition 4.4.4, $(\Lambda_1, \Lambda_2, \Lambda_3)$ is either triangular or conic-line type. The latter case cannot actually occur as Λ_1 contains Γ_1 and hence it contains at least three collinear points.

Therefore $\{P, Q\} \cap \{P_i, Q_i\} = \emptyset$ may be assumed. Then the H-members from Λ_2 and Λ_3 lie on four lines, namely PP_i, PQ_i, QP_i, QQ_i. Observe that these lines may be assumed to be pairwise distinct, otherwise Λ_2 (or Λ_3) is contained in a line, and again $(\Lambda_1, \Lambda_2, \Lambda_3)$ would be triangular. Therefore, half of the H-members from Λ_2 lie on one of these four lines, say PQ_i, and half of them on QP_i. Similarly, each of the lines PP_i and QQ_i contain half from the H-members from Λ_3.

In the above argument, any H-member Γ_2 from Λ_2 may play the role of Γ_1. Therefore there exist two lines such that each H-member from Λ_1 lies on one or the other line. Actually, these two lines are PQ and P_iQ_i since each of them contains a

H-member from Λ_1. In this case, $(\Lambda_1, \Lambda_2, \Lambda_3)$ is of tetrahedron type. □

Since a dihedral group of order ≥ 8 has a unique cyclic subgroup of index 2 and such a subgroup is characteristic, Propositions 4.4.8 and 4.2.13 have the following corollary.

Proposition 4.4.9. *Let G be a finite group of order $n \geq 12$ containing a normal dihedral subgroup D. If G is realized by a dual 3-net then G is itself dihedral.*

4.5 DUAL 3-NETS CONTAINING ALGEBRAIC 3-SUBNETS OF ORDER n WITH $n \geq 5$

The main result is the following proposition.

Proposition 4.5.1. *Let $p = 0$ or $p > n$. Let G be a group containing a proper abelian normal subgroup H of order $n \geq 5$. If a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizes G such that all its dual 3-subnets realizing H as a subgroup of G are algebraic, then one of the following holds.*

(i) *$(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic, and G is either cyclic or the direct product of two cyclic groups.*

(ii) *$(\Lambda_1, \Lambda_2, \Lambda_3)$ is of tetrahedron type, and G is dihedral.*

(iii) *G is the generalized quaternion group of order 16.*

(iv) *$G \cong C_3 \ltimes C_7$.*

(v) *G is the dicyclic group of order 12.*

(vi) *G is an elementary abelian group of order 25, $(\Lambda_1, \Lambda_2, \Lambda_3)$ is not algebraic and none of its dual 3-subnets is triangular.*

The proof is performed in several steps according to the reducibility behavior of the plane cubics associated to the 3-subnets realizing H.

We assume that $(\Lambda_1, \Lambda_2, \Lambda_3)$ is not of tetrahedron type, and we will show that the points of $(\Lambda_1, \Lambda_2, \Lambda_3)$ lie on a plane cubic, apart from the possible four sporadic examples.

Let $(\Gamma_1, \Gamma_2, \Gamma_3)$ be a 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realizes H. By hypothesis, there exists a plane cubic curve $\mathcal{F}$ passing through all points in $(\Gamma_1, \Gamma_2, \Gamma_3)$.

For two H-members, Γ_1^i from Λ_1 and Γ_2^j from Λ_2, let $\mathcal{F}(i,j)$ be the unique plane cubic containing both Γ_1^i and Γ_2^i.

Lemma 4.5.2. *If there exist i, j such that $\mathcal{F}(i,j) = \mathcal{F}(i,m) = \mathcal{F}(t,j)$ for all m, t, then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic.*

Proof. Obviously, $\mathcal{F}(i,j)$ contains all points in Λ_1 and Λ_2. For every point $P \in \Lambda_3$ there exists a 3-subnet $(\Gamma_1^t, \Gamma_2^m, \Gamma_3)$ with $P \in \Gamma_3$ which realizes H as a subgroup of G. If $\mathcal{F}$ is the associated plane cubic curve, then $\mathcal{F}$ and $\mathcal{F}(i,j)$ have $2n > 9$ common points. But then $\mathcal{F} = \mathcal{F}(i,j)$ and hence $P \in \mathcal{F}(i,j)$. Therefore Λ_3 also lies in $\mathcal{F}(i,j)$ whence the assertion follows. □

4.5.1 For at least one pair (Γ_1^i, Γ_2^j) the plane cubic curve $\mathcal{F}(i,j)$ is irreducible

Let $(\Gamma_1, \Gamma_2, \Gamma_3)$ be a dual 3-subnet realizing H as a subgroup of G for which $\mathcal{F}(1,2)$ is an irreducible plane cubic curve. Then Γ_1 does not lie on a line.

For any point $D_2 \in \Lambda_2 \setminus \Gamma_2$, there exists another dual 3-subnet $(\Gamma_1, \Gamma_2^j, \Gamma_3^s)$ realizing H as a subgroup of G such that $D_2 \in \Gamma_2^j$. Then $\mathcal{F}(1,2)$ and $\mathcal{F}(1,j)$ share Γ_1. Therefore they have at least n common points.

Assume first that $n > 9$. Then $\mathcal{F}(1,2) = \mathcal{F}(1,j)$ for any j. Hence $\mathcal{F}(1,2)$ contains

all points in $\Lambda_2 \cup \Lambda_3$. Take any H-member Γ_1^i from Λ_1. Then $\mathcal{F}(1,j)$ and the plane cubic $\mathcal{F}(i,j)$ associated to the the 3-subnet $(\Gamma_1^i, \Gamma_2, \Gamma_3^s)$ shear Γ_2. This yields that $\mathcal{F}(i,j) = \mathcal{F}(1,j) = \mathcal{F}(1,2)$. Therefore, $\mathcal{F}(1,2)$ also contains all points in Λ_1. From Proposition 4.2.1, G is either a cyclic group or the direct product of two cyclic groups.

To investigate the case $n \leq 9$, we need more. The key ingredient is the following technical lemma.

Lemma 4.5.3. *For two integers k, n with $k \geq 2$, and $5 \leq n \leq 9$, let G be a group of order kn containing an abelian normal subgroup H of order n with the following properties*

(i) *G can be realized by a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$;*

(ii) *every 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing H as a subgroup of G is algebraic.*

For a given H-member Γ_1 from Λ_1, let F *be the family of the plane cubic curves associated with the dual 3-subnets $(\Gamma_1, \Gamma_2, \Gamma_3)$ realizing H as a subgroup G. If no curve in* F *is reducible then $k \leq m$ where m is the number of curves in* F*.*

Proof. For $i = 1, \ldots m$, let $\mathcal{F}_i \in$ F. By our hypothesis these m curves $\mathcal{F}_i$ are irreducible and shear each of the n points in Γ_1. For every H-member Γ_2 from Λ_2, there exists a unique H-member Γ_3 from Λ_3 such that $(\Gamma_1, \Gamma_2, \Gamma_3)$ is a dual 3-subnet realizing H as a subgroup of G. These dual 3-nets $(\Gamma_1, \Gamma_2, \Gamma_3)$ with Γ_2 ranging over the set of H-members in Λ_2 are partitioned into m families, say $\Psi_2^1, \ldots, \Psi_2^m$, according as the associated plane cubic curve of $(\Gamma_1, \Gamma_2, \Gamma_3)$ is $\mathcal{F}_1, \mathcal{F}_2, \ldots \mathcal{F}_m$, respectively. Obviously, $f_1 + \ldots + f_m = k$ with $f_i = |\Psi_i|$ for $i = 1, \ldots, m$. In this way, the H-members Γ_3 from Λ_3 are also partitioned into m families, say $\Psi_3^1, \ldots \Psi_3^m$ with $|\Psi_3^i| = f_i$ for $i = 1, \ldots, m$. Therefore, a dual 3-net $(\Gamma_1, \Gamma_2, \Gamma_3)$ lies in some $\mathcal{F}_i$; more precisely this occurs when $\Gamma_2 \in \Psi_2^i$ and $\Gamma_3 \in \Psi_3^i$.

Now take any two H-members, say Γ_2 and Γ_3, with $\Gamma_2 \in \Psi_2^i$ and $\Gamma_3 \in \Psi_3^i$, for the same index i. Then there exists an H-member Δ_1 from Λ_1 such that $(\Delta_1, \Gamma_2, \Gamma_3)$ is a dual 3-subnet realizing $(H, \cdot)$ as a subgroup of $(G, \cdot)$. Let $\mathcal{U}$ be the plane cubic curve associated with $(\Delta_1, \Gamma_2, \Gamma_3)$. Then $\mathcal{U}$ and $\mathcal{F}_i$ shear all the points in $\Gamma_2 \cup \Gamma_3$. Since $|\Gamma_2 \cup \Gamma_3| = 2n > 9$, $\mathcal{U}$ and $\mathcal{F}_i$ coincide. Therefore, there are at least f_i H-members from Λ_1 lying in $\mathcal{F}_i$. Since Γ_1 is the unique H-member lying in two different curves $\mathcal{F}_i$, the number r of H-members from Λ_1 which lie in some $\mathcal{F}_i$ is at least $f_1-1+\ldots+f_m-1$. In other words, at most $m-1$ H-members from Λ_1 do not lie in any $\mathcal{F}_i$.

On the other hand, take any two H-members, say Γ_2 and Γ_3, with $\Gamma_2 \in \Psi_2^i$ and $\Gamma_3 \in \Psi_3^j$ with $i \neq j$. Let Δ_1 be the H-member from Λ_1 such that $(\Delta_1, \Gamma_2, \Gamma_3)$ is a dual 3-subnet realizing $(H, \cdot)$ as a subgroup of $(G, \cdot)$. Then Δ_1 does not lie in any $\mathcal{F}_r$ with $1 \leq r \leq m$ otherwise $\mathcal{F}_i \cap \mathcal{F}_r$ would contain $\Delta_1 \cup \Gamma_2$ whereas $|\Delta_1 \cup \Gamma_2| = 2n > 9$. If j ranges over $\mathcal{I}_m \setminus \{i\}$, we obtain as many as $(\sum_{j=1}^m f_j) - f_i$ H-members from Λ_1 which do not lie in any $\mathcal{F}_r$ with $r = 1, \ldots, m$.

Therefore, $k - f_i \leq m - 1$ for every $1 \leq i \leq m$, whence $k \leq m$. □

Now we are ready to deal with the cases $n \leq 9$. Let $(\Gamma_1, \Gamma_2, \Gamma_3)$ be a 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realizes H as a subgroup of G for which $\mathcal{F}(1,2)$ is an irreducible plane cubic curve. By Lemma 4.5.2 we may assume that

$$\text{there exist } l, t \text{ for which } \mathcal{F}(t,2) \neq \mathcal{F}(1,2) \neq \mathcal{F}(1,l). \tag{4.6}$$

Furthermore, any Γ_r for $1 \leq r \leq 3$ may play the role of Ω in Chapter 3.

n=9

Set $\Omega = \Gamma_1$. Proposition 3.3.4 together with assumption (4.6) rule out the possibility that Ω contains no three collinear points. Hence Proposition 3.2.4 applies. This together with Proposition 4.5.3 yield that $k = 2$. Hence, G has order 18. Therefore,

either G is cyclic or dihedral. As $(\Lambda_1, \Lambda_2, \Lambda_3)$ is supposed not to be of tetrahedron type, G is cyclic by Proposition 4.4.6, and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic by Proposition 4.4.1. In the other case, H is elementary abelian and assumption (4.6) yields that Γ_1 consists of the nine inflection points of $\mathcal{F}(1, 2)$. Actually, this case can easily be avoided by replacing Γ_1 with Γ_2 and applying Propositions 3.2.4 and 3.3.4 to $\Omega = \Gamma_2$. Therefore the case $n = 9$ cannot actually occur.

n=8

By [25, Theorem 4.2], H is not an elementary abelian group. Therefore two cases occur for H, namely either H is cyclic and $H \cong C_2 \times C_4$. Set $\Omega = \Gamma_1$. Then Propositions 3.2.7 and 3.3.5 together with assumption (4.6) rule out the case $H \cong C_2 \times C_4$. If H is cyclic, Proposition 3.2.7 together with assumption (4.6) yield that Ω contains three collinear points. Therefore, Proposition 3.3.7 applies. This together with Proposition 4.5.3 imply $k = 2$. Hence, G has order 16. Up to isomorphisms, there are four groups of order 16 containing a cyclic subgroup of order 8, namely the cyclic, dihedral, $C_2 \times C_8$ and the generalized quaternion group. By Propositions 4.4.1 and 4.4.6 we may assume that either $G \cong C_2 \times C_8$ or G is the generalized quaternion group. If $G \cong C_2 \times C_8$ then G also contains a subgroup isomorphic to $C_2 \times C_4$ but this case has already been ruled out. Therefore, G must be the generalized quaternion group of order 16.

n=7

Set $\Omega = \Gamma_1$. Propositions 3.2.9, 3.3.9 and 4.5.3 together with assumption (4.6) yield that $|G| = 7k$ with $2 \leq k \leq 5$. By Proposition 4.4.1 and 4.4.6 we may assume that either $k = 4$ or $k = 3$. The case $k = 4$ cannot actually occur, since if $|G| = 28$ then G is either cyclic or dihedral or it contains a dihedral subgroup of index 2, but all these

possibilities are ruled out by Proposition 4.4.1, 4.4.6 and 4.4.9. Therefore, G must be a non-cyclic group of order 21, that is, $G = C_3 \ltimes C_7$.

n=6

Set $\Omega = \Gamma_1$. Propositions 3.2.13, 3.3.10 and 4.5.3 together with assumption (4.6) yield that $|G| = 6k$ with $2 \leq k \leq 12$. Since the cases $n > 6$ have already been investigated, we may assume that G contains no abelian normal subgroup of order > 6. An exhaustive computer aided search shows that there exists only four such groups G of order $6k$ with $2 \leq k \leq 12$. Two of them have order 12, namely the dihedral and the dicyclic groups while the other two have order 72. In the latter two cases, G has a normal non-dihedral subgroup M of order 24 that contains a (normal) cyclic subgroup of order 12. This shows that M (and hence G) cannot be realized by a dual 3-net. Therefore, G must be a dicyclic group of order 12.

n=5

Set $\Omega = \Gamma_1$. From Propositions 3.2.11, 3.3.11 and 4.5.3 together with assumption (4.6), $|G| = 5k$ with $2 \leq k \leq 6$. As we have already observed, if G is cyclic then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic by Proposition 4.4.1. Up to isomorphisms, all non-cyclic groups of order u with $u = 10, 15, 25, 30$ have a normal dihedral subgroup of order ≥ 6 with only two exceptions, namely the dicyclic group of order 20 and the elementary abelian group of order 25. The non-exceptional cases cannot actually occur by Propositions 4.4.1, 4.4.6 and 4.2.13, $(\Lambda_1, \Lambda_2, \Lambda_3)$ being supposed not to be of tetrahedron type. The same happens to the dicyclic group of order 20 as it has a (normal) cyclic subgroup of order 10. In fact, we have already proven for $n \geq 10$ that G must be either abelian or dihedral, and hence cannot be dicyclic of order 20. Therefore, G must be an elementary abelian group of order 25.

4.5.2 For at least one pair (Γ_1^i, Γ_2^j) the plane cubic curve $\mathcal{F}(i,j)$ splits into an irreducible conic and a line

Let $(\Gamma_1^i, \Gamma_2^j, \Gamma_3^s)$ be a dual 3-subnet realizing H as a subgroup of G for which $\mathcal{F}(i,j)$ splits into an irreducible conic $\mathcal{C}$ and a line ℓ. From Lemma 4.4.5, it is a conic-line 3-subnet such that Γ_1^i lies in an irreducible conic $\mathcal{C}$ while either Γ_2^j or Γ_3^s lies on a line ℓ. Suppose that this occurs for Γ_2^j. For any point $D_3 \in \Lambda_2 \setminus \Gamma_2^s$, there exists another dual 3-subnet $(\Gamma_1^i, \Gamma_2^m, \Gamma_3^t)$ realizing H as a subgroup of G. From subsection 4.5.1, $\mathcal{F}(i,m)$ may be assumed to be reducible. Since Γ_1^i is not contained in a line, Proposition 4.4.5 yields that $\mathcal{F}(i,m)$ splits into an irreducible conic $\mathcal{C}_1$ and ℓ_1. Then $\mathcal{C}$ and $\mathcal{C}_1$ coincide since they share Γ_1^i and $|\Gamma_1| \geq 5$. From Proposition 4.2.12, the line ℓ contains Γ_2^m, thus, Λ_2 lies on ℓ. Since $p > n$, this yields that $(\Lambda_1, \Lambda_2, \Lambda_3)$ is of conic-line type. From Proposition 4.2.11, G is a cyclic group.

4.5.3 For any pair (Γ_1^i, Γ_2^j) the plane cubic curve $\mathcal{F}(i,j)$ splits into three lines

In this case every 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing H is triangular. From Proposition 4.2.3, H is a cyclic group and, from Proposition 4.4.8, $(\Lambda_1, \Lambda_2, \Lambda_3)$ is either triangular or of tetrahedron type.

This completes the proof of Proposition 4.5.1. As an immediate corollary by induction on n, we have the following result.

Theorem 4.5.4. *Let $p = 0$ or $p > n$. Let G be an abelian group containing a proper subgroup H of order $n \geq 7$. Then every dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing G is algebraic.*

4.6 CLASSIFICATION OF DUAL 3-NETS REALIZING GROUPS OF PRIMEPOWER ORDER

Proposition 4.6.1. *Let G be a group of order $n = 2^h$ with $h \geq 2$. If $p > n$ or $p = 0$ and G can be realized by a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ then one of the following holds.*

(i) *G is cyclic.*

(ii) *$G \cong C_m \times C_k$ with $n = mk$.*

(iii) *G is a dihedral.*

(iv) *G is the quaternion group of order 8.*

(v) *G is the quaternion group of order 16.*

Proof. For $n = 4, 8$, the classification follows from Propositions 4.3.2, 4.4.6 and [25, Theorem 4.2]. Up to isomorphism, there exist fourteen groups of order 16; each has a subgroup H of index 2 that is either an abelian or a dihedral group. In the latter case, G is itself dihedral, by Proposition 4.4.9. From Proposition 4.3.2, every dual 3-net realizing H is algebraic. So, Proposition 4.5.1 applies to G and H yielding that G is abelian. This completes the proof for $n = 16$. By induction on h we assume that Proposition 4.6.1 holds for $n = 2^h \geq 16$ and we are going to show that this remains true for 2^{h+1}. Let H be a subgroup of G of index 2. Then $|H| = 2^h$ and one of the cases (i), (ii), (iii) or (vi) holds for H. The latter case cannot actually occur. In fact, if H is isomorphic to the generalized quaternion group of order 16 then H has a unique cyclic group K of order 8. Obviously, K is a characteristic subgroup of H. Hence K is a normal cyclic subgroup of G. Proposition 4.5.1 applied to G and K implies that G must be either abelian or dihedral. But this is impossible in our case, since neither an abelian group nor a dihedral group contain a subgroup isomorphic

to the generalized quaternion group of order 16. If (iii) holds for H then it also holds for G, by Proposition 4.4.9. In cases (i) and (ii), H is abelian and every dual 3-net realizing H is algebraic by induction. Therefore the assertion for these cases follows from Proposition 4.5.1. □

Remark 4.6.2. *Urzúa's 3-net provides an example for case (v) in Proposition 4.6.1. It is unknown whether this is the unique example, as well as, whether case (vi) in Proposition 4.6.4 can actually occur.*

As a corollary we have the following result.

Proposition 4.6.3. *Let $p > n$ or $p = 0$. Let S_2 be a group of order $n = 2^h$ with $h \geq 2$ which can be realized by a dual 3-net.*

(i) *If S_2 has more than one involution then S_2 is either a dihedral group, or the direct product of two cyclic groups.*

(ii) *If S_2 has a normal subgroup H of order 2 or 4 then S_2/H is either cyclic, or dihedral, or the direct product of two cyclic groups.*

(iii) *If the exponent of S_2 is at most four then S_2 is either a cyclic group of order ≤ 4, or an elementary abelian group of order 4, or $C_2 \times C_4$, or $C_4 \times C_4$ or the quaternion group of order 8.*

Proof. Obviously, in cases (i), (ii) and (iii) of Proposition 4.6.1 both assertions hold. If S_2 is a quaternion group of order 8 or 16, then S_2 has only one involution and S_2/W is either cyclic or dihedral. □

Proposition 4.6.4. *Let G be a group of order $n = d^h$ where d is an odd prime and $h \geq 1$. If $p = 0$ or $p > n$ and G can be realized by a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ then one of the following holds.*

(i) *G is cyclic and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic.*

(ii) *$G \cong C_m \times C_k$ with $n = mk$, and if $G \ncong C_5 \times C_5$ then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic.*

(iii) *G is an elementary abelian group of order 25 and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is not algebraic.*

Proof. If G is cyclic, then the proposition is a consequence of Proposition 4.4.1 and case (i) occurs.

Assume G is not cyclic and $h \geq 2$. If $h = 2$, then G is isomorphic to one of the following groups: $C_3 \times C_3$, $C_5 \times C_5$, $C_m \times C_m$, for $m \geq 7$. If $G \cong C_3 \cong C_3$, then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic (Proposition 4.3.2). In the latter case, G is an abelian group that contains a proper subgroups of order $d \geq 7$, then case (ii) occurs (Proposition 4.5.4).

If $h \geq 3$, G contains a proper abelian normal subgroup of order d^2. Then, the proposition is a consequence of Proposition 4.5.1. □

Remark 4.6.5. *It is unknown whether case (iii) in Proposition 4.6.4 can actually occur.*

Proposition 4.6.6. *Let G be a group of odd order n. If $p > n$ or $p = 0$ and G can be realized by a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ then one of the following holds.*

(i) *G is cyclic and $(\Lambda_1, \Lambda_2, \Lambda_3)$.*

(ii) *$G \cong C_m \times C_k$ with $n = mk$.*

(iii) *$G \cong C_3 \ltimes C_7$.*

(iv) *G is an elementary abelian group of order 25 and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is not algebraic.*

(v) *G is isomorphic to the unique non abelian group of order 75 containing an elementary abelian subgroup of order 25 and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is not algebraic.*

Proof. Let N be a minimal normal subgroup of G. By the Feith-Thompson theorem, G is solvable. Therefore, N is an elementary abelian group of odd order. From Proposition 4.6.4, the subnet that realizes N is algebraic with only one possible exception if $G \cong C_5 \times C_5$. If the the subnet that realizes N is algebraic, then Proposition 4.6.6 is a consequence of Proposition 4.5.1. In the exceptional case, N is an elementary abelian group of order 25. From Proposition 4.5.4, the centralizer $\mathcal{C}_G(N)$ of N in G coincides with N. Therefore, G is a subgroup D of $GL(2,5) \times N$. Assume that D is not trivial. Up to conjugacy, $|GL(2,5)|$ has two subgroups of odd order, namely C_3 and C_5. If $D = C_5$ then G has order 5^3, and (ii) of Proposition 4.6.4 implies that G is abelian. If $D = C_3$ then $|G| = 75$. Therefore G is either abelian, or it is the unique group $C_3 \ltimes N$ up to isomorphism. □

Remark 4.6.7. *It is unknown whether cases (iv) and (v) in Proposition 4.6.6 can actually occur.*

4.7 3-NETS AND NON-ABELIAN SIMPLE GROUPS

Proposition 4.7.1. *If $p = 0$, then no dual 3-net can realize a non-abelian simple group of order n. For $p > n$, if a dual 3-net realizes a non-abelian simple group G, then $G \cong \mathrm{Alt}_5$.*

Proof. Let G be a non-abelian simple group of order n, and assume that G can be realized by a 3-net. From Proposition 4.6.1, S_2 is dihedral since no Sylow 2-subgroup of a non-abelian simple group is either cyclic, or the direct product of two cyclic groups, see [8, Theorem 2.168], or a quaternion group, see [3]. From Gorestein-Walter theorem [9], either $G \cong PSL(2, q^h)$ with and odd prime q and $q^h \geq 5$, or $G \cong \mathrm{Alt}_7$. Moreover, by 4.6.4, we have that $h \leq 2$.

For $q^h > 7$, $q \neq 25$, we consider the group $PSL(2, q)$. G has a subgroup T of order

$q^h(q^h-1)/2$ containing a normal subgroup of order q^h. Using Proposition 4.5.1, we can exclude this case.

If $G \cong PSL(2,25)$, there exists a subgroup H of G of order 5. The normalizer of H in G is a group of order 100. By Proposition 4.5.1, this is not possible. If $G \cong PSL(2,7)$, every subgroup $U \cong C_4$ is contained in a dihedral group of order 8. Then, every subnet realizing a group $U \cong C_4$ is triangular. U is a normal subgroup of a subgroup of G isomorphic to Alt_4. This contradicts Proposition 4.4.8. Then $PSL(2,7)$ can not be realized, and this rules out also the case $G \cong \mathrm{Alt}_7$.

Thus, the only case left is $G \cong \mathrm{Alt}_5$. By Proposition 4.3.3, this case does not occur for $p = 0$. □

4.8 DUAL 3-NETS CONTAINING ALGEBRAIC 3-SUBNETS OF ORDER n WITH $2 \leq n \leq 4$

Our aim is to prove the following result.

Proposition 4.8.1. *Assume that $2 \leq n \leq 4$. Let $p = 0$ or $p > n$. Let G be a group of order $\geq 2n$ containing a proper normal abelian subgroup H of order n. Then one of the following holds.*

(i) $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is algebraic and G is either cyclic or the direct product of two cyclic groups.*

(ii) $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is of tetrahedron type and G is dihedral.*

(iii) *G is the quaternion group of order 8.*

(iv) *G is the dicyclic group of order 12.*

(v) *G is the quaternion group of order 16.*

(vi) $G \cong \mathrm{Sym}_4$.

(vii) $G \cong \mathrm{Alt}_4$.

The proof is divided in two parts according as $\mathcal{C}_G(H) \cap (G \setminus H) = \emptyset$ or not. Some ideas from the proof of Proposition 4.5.1 are adapted for $n = 5$.

Lemma 4.8.2. *If $\mathcal{C}_G(H)$ is larger than H then one of the following holds:*

(i) *$\mathcal{C}_G(H)$ is either abelian or dihedral and it contains a cyclic subgroup of order ≥ 10.*

(ii) *$\mathcal{C}_G(H)$ is the dicyclic group of order 12.*

(iii) *$\mathcal{C}_G(H)$ is the quaternion group of order either 8 or 16, and $|H| = 2$.*

Proof. For brevity, let $M = \mathcal{C}_G(H)$. Then M is a normal subgroup of G.

Let $\sigma : M \mapsto M/H$ be the natural homomorphism. By hypothesis, the factor group $\bar{M} = M/H$ is non-trivial. Let $\bar{N}$ be a minimal normal subgroup of $\bar{M}$.

We begin by showing that $\bar{N}$ contains no non-abelian simple group. For this purpose we assume on the contrary that such a non-abelian simple group $\bar{U}$ exists. Then M has a subgroup $U = \sigma^{-1}(\bar{U})$, a central extension of $\bar{U}$ by $\mathcal{Z}(U) = H$, such that $\bar{U} = U/H$.

For $n = 3$, take any Sylow 2-subgroup S_2 of U while for $n = 2, 4$ choose a Sylow 2-subgroup S_2 of U that contains H. Let $\bar{S}_2 = \sigma(S_2)$. Then $\bar{S}_2$ is a Sylow subgroup of $\bar{U}$. Since $\bar{U}$ is a non-abelian simple group, $\bar{S}_2$ is neither cyclic nor the direct product of cyclic groups. From (ii) of Proposition 4.6.3, $\bar{S}_2$ is a dihedral group. Hence $\bar{U}$ is a simple group with a dihedral Sylow 2-subgroup. By the Gorenstein-Walter theorem, either $\bar{U} \cong PSL(2, q^h)$ with an odd prime q and $q^h \geq 5$, or $\bar{U} \cong \mathrm{Alt}_7$.

Assume first that $n = 3$. From the classification of subgroups of $PSL(2, q^h)$, see [18, Theorem 1], $\bar{U}$ has a dihedral subgroup $\bar{D}$ of order $2d \geq 8$ with g.c.d.$(3, d) = 1$.

Let D be a subgroup of U of order $6d$ such that $\sigma(D) = \bar{D}$. As H is a normal subgroup of D and g.c.d.$(|H|, [D : H]) = 1$, Zassenhaus' theorem [14, 10.1 Hauptsatz] yields that $D = D_1 \ltimes H$ with a subgroup D_1 of D. Since D_1 is a subgroup of M, this implies that $D = D_1 \times H$. From this and $D_1 \cong D/H$, we have that D_1 is a normal dihedral subgroup of D. Since $|D| \geq 24$ and D can be realized by a dual 3-subnet, Proposition 4.4.9 yields that D is itself dihedral. From this $|\mathcal{Z}(D)| = 2$. On other hand, H is contained in $\mathcal{Z}(D)$, and hence $|\mathcal{Z}(D)| \geq 3$, a contradiction.

Therefore, either $n = 2$ or $n = 4$. Since $PSL(2, q^h)$ contains a subgroup isomorphic to $PSL(2, q)$, from the classification of subgroups of $PSL(2, q)$, see [18, Theorem 1], $\bar{U}$ has a subgroup $\bar{D}$ of order $q(q-1)/2$ containing a normal subgroup $\bar{V}$ of order q and a cyclic complement $\bar{W}$ of order $(q-1)/2$. Write $q - 1 = 2^r s$ with s odd.

If $s \geq 3$ then $q \geq 7$. Choose a subgroup $\bar{Y}$ of $\bar{D}$ of odd order sq. Let Y be a subgroup of U such that $\sigma(Y) = \bar{Y}$. Since g.c.d.$(|H|, [Y : H]) = 1$ and H is a normal subgroup of Y, Zassenhaus' theorem [14, 10.1 Hauptsatz] yields that $Y = Y_1 \ltimes H$ with a subgroup $Y_1 \cong \bar{Y}$. Observe that Y_1 is not abelian but it has a cyclic normal subgroup of order q. From Proposition 4.5.1, this is only possible for $q = 7$. Therefore, $s \geq 3$ implies $q = 7$.

If $s = 1$, a Sylow 2-subgroup $\bar{S}_2$ of $PSL(2, q)$, with $q \geq 17$ odd, has order ≥ 16. Choose a s subgroup S_2 of U such that $\sigma(S_2) = \bar{S}_2$. Then $|S_2| \geq 32$. Since $\bar{S}_2$ is dihedral and hence non abelian, S_2 is non-abelian, as well. From Proposition 4.6.1, S_2 is dihedral. Furthermore, since $|H| \in \{2, 4\}$, U does not have any normal subgroup of odd order. By the Gorenstein-Walter theorem, U is isomorphic to either $PSL(2, q)$ with $q \geq 5$ odd, or to Alt_7. But this contradicts Proposition 4.7.1.

Therefore, we are left with three cases only, namely $q = 5, 7, 9$, and we are going to rule them out. If $q = 9$ and $|H| = 2$, choose a (non-abelian) subgroup $\bar{V}$ of $\bar{U} \cong PSL(2, 9)$ of order 18 containing an elementary abelian subgroup $\bar{W}$ of order

9. Let V be a subgroup of U such that $\sigma(V) = \bar{V}$. Then $|V| = 36$ and V contains a subgroup $W \cong \bar{W}$, and hence V is not a dihedral group. The centralizer $\mathcal{C}_U(W)$ of W in U contains H, and hence it has order at least 18. Since V is not abelian, $|\mathcal{C}_U(W)| = 18$. Therefore, V is a non-abelian group of order 36 containing normal abelian subgroup $\mathcal{C}_U(W)$ of order 18. Since every dual 3-net realizing an abelian group of order 18 is algebraic, by Propositions 4.3.2 and 4.5.1, this implies that V cannot be realized as a dual 3-net, see Proposition 4.5.1.

Now let $q = 5$ or $q = 7$. We show that U has has subgroup $V \cong SL(2, q)$ such that $V \cap H$ comprises the unique involution of V together with the identity. In this direction we show first that U has a quasi-simple subgroup, that is, perfect subgroup V such that $V/V \cap H \cong PSL(2, q)$. We begin with the case $|H| = 2$. Obviously, a composition factor of U is $1 \trianglelefteq H \trianglelefteq U$. Let U' be the commutator subgroup of U. If $U \neq U'$ then U/U' is an abelian group and hence another composition factor of U is $1 \trianglelefteq U' \trianglelefteq U$. This would imply that $U' \cong U/H \cong PSL(2, q)$ which is impossible in our case by Proposition 4.7.1. Hence $U = U'$, that is, U is perfect. Now, let $|H| = 4$, and choose an involution h from H. Then a composition factor of U is $1 \trianglelefteq \langle h \rangle \trianglelefteq H \trianglelefteq U$. If $U \neq U'$ then $1 \trianglelefteq R \trianglelefteq U' \trianglelefteq U$ with $|R| = 2$ as the other possibility $1 \trianglelefteq U' \trianglelefteq S \trianglelefteq U$ with $U' \cong PSL(2, q)$ cannot occur. Replacing U with U' in the previous argument shows that U' is a perfect group, and we take it for V. This completes the proof of the existence of a quasi-simple group V with $|\mathcal{Z}(V)| = 2$ and $V/\mathcal{Z}(V) \cong PSL(2, q)$. Since both 5 and 7 are prime numbers, a classical result of Schur implies indeed that $V = SL(2, q)$.

It is easy to check that $SL(2, 5)$ has a dicyclic subgroup of order 20. On the other hand, a dicyclic group of order 20 is a non-dihedral group with a normal cyclic group of order 10 and hence it cannot be realized by a dual 3-net, see Proposition 4.5.1. A similar argument works for $q = 7$ since $SL(2, 7)$ contains a non-dihedral and

non-abelian subgroup R of order 42 with a cyclic normal subgroup of order 14 and such a subgroup R cannot be realized by a dual 3-net, again by Proposition 4.5.1.

Therefore $\bar{N}$ is an elementary abelian group of order d^h for a prime d. Let $N = \sigma^{-1}(\bar{N})$. Then $\bar{N} = N/H$. If $|N| > 6$ and every dual 3-net realizing N is algebraic then Lemma 4.8.2 holds because Proposition 4.5.1 yields then that every dual 3-net realizing M is either algebraic or dihedral.

Bearing this in mind, the case g.c.d.$(\mathrm{d}, \mathrm{n}) = 1$ is investigated first.

Since g.c.d$(|\bar{\mathrm{N}}|, |\mathrm{H}|) = 1$, Zassenhaus' theorem [14, 10.1 Hauptsatz] ensures a complement $W \cong \bar{N}$ such that $N = W \ltimes H$. As both W and H are abelian and $W \leq M$, N must be abelian, as well. Hence $M = W \times H$. If N contains no cyclic subgroup of order ≥ 10 then either $n = 3$, $d^h = 2$ and $N \cong C_6$, or $n = 2$, $d^h = 3$ and $N \cong C_6$, or $n = 4$, $d^h = 3$ and $H \cong C_2 \times C_2$. In the latter case, every dual 3-net realizing N is algebraic by Proposition 4.3.3, and M is either abelian or dihedral by Proposition 4.5.1. If $N \cong C_6$, Proposition 4.5.1 yields that $|M| = 12$, and M is either cyclic of dicyclic.

It remains to investigate the cases where $d = n$ for $n = 2, 3$ and $d = 2$ for $n = 4$. Since N properly contains H, its order is at least 9 for $n = 3$, at least 8 for $n = 4$, and at least 4 for $n = 2$. On the other hand, N/H is an elementary abelian group and hence N has exponent at most d^2. For $d = 3$, Proposition 4.6.4 forces N to be an abelian normal subgroup of M of order 9. From Proposition 4.3.2, every dual 3-net realizing N is algebraic. By (iii) of Proposition 4.6.3, this conclusion remains true whenever $d = 3$ is replaced by $d = 2$, with three exceptions for $n = 2$, namely $d^h = 2$, $N \cong C_4$, and $d^h = 2$, $N \cong C_2 \times C_2$, and $d^h = 4$, $N \cong Q_8$.

The latter case is investigated first. Since the automorphism group of the quaternion group of order 8 has order a power of 2, every element of M odd order commutes with every element in N. If $|M|$ has an odd divisor ≥ 3, take an element of odd order

$m > 1$. Then the group generated by N and t has order $8m$ and its subgroup D generated by t together with an element of N of order 4 is a (normal) cyclic subgroup of M of order $4m$. But this contradicts Proposition 4.5.1, as M is neither abelian nor dihedral. Therefore M is a 2-group containing Q_8. From Proposition 4.6.1, M is a quaternion group of order either 8 or 16.

To deal with the case $|N| = 4$ it suffices to replace H by N (and M by $\mathcal{C}_M(N)$) and repeat the above argument. This gives that $C_M(N)$ is either abelian or dihedral of order ≥ 10, or $\mathcal{C}_M(N)$ is a dicyclic group of order 12. Since $\mathcal{C}_M(N)$ is a normal subgroup of M, Propositions 4.4.9 and 4.5.1 imply with just one exception that M is either abelian or dihedral. In the exceptional cases, $\mathcal{C}_M(N)$ is the dicyclic group of order 12 and we have to show that then $M = \mathcal{C}_M(N)$.

For this purpose assume on the contrary that $\mathcal{C}_M(N)$ is a proper subgroup of M. Let $m \in M \setminus \mathcal{C}_M(N)$. Since $\mathcal{C}_M(N) \trianglelefteq M$, the action φ_m of m on $\mathcal{C}_M(N)$ by conjugacy is an automorphism group of $\mathcal{C}_M(N)$. Observe that $N = C_2 \times C_2$ contains H and that m commutes with H. Therefore φ_m fixes the involution of H and hence it interchanges the other two involutions in N. This yields that φ_m^2 fixes N elementwise. Hence $\varphi_m^2 \in \mathcal{C}_M(N)$. Therefore $|M| = 2|\mathcal{C}_M(N)|$, that is, M is isomorphic to a group of order 24 containing the dicyclic group of order 12. Up to isomorphisms, there exist three such groups of order 24. More precisely, two of these three groups contain a dihedral subgroup of order 2 while the remaining one contains a subgroup $C_2 \times C_6$. Therefore, M has a normal subgroup of order 12 that is either a dihedral subgroup or is isomorphic to $C_2 \times C_6$. But then M cannot be realized by a dual 3-net, see Propositions 4.5.1, 4.4.9 and 4.3.3. This proves that $M = \mathcal{C}_M(N)$. □

Proposition 4.8.3. *If $\mathcal{C}_G(H)$ is larger than H then one of the following holds:*

(i) *G is either abelian or dihedral with a cyclic subgroup of order ≥ 10.*

(ii) *G is the dicyclic group of order* 12.

(iii) *G is the quaternion group of order* 8.

(iv) *G is the quaternion group of order* 16.

Proof. By Lemma 4.8.2 and Propositions 4.4.2, 4.4.9, it suffices to investigate the two sporadic cases in Lemma 4.8.2. If $\mathcal{C}_G(H)$ is the dihedral group of order 12, then the final argument involving φ_m in the proof of Lemma 4.8.2 also works when M is replaced by G. Therefore G cannot be larger than $\mathcal{C}_G(H)$. If (iii) of Lemma 4.8.2 occurs then $|H| = 2$ implies that every element in G commutes with the involution in H. In other words, $G = \mathcal{C}_G(H)$. □

Proposition 4.8.4. *If $\mathcal{C}_G(H) = H$ then G is dihedral and one of the following holds.*

(i) *$n = 3$ and G has order* 6.

(ii) *$n = 4$ and G has order* 6*, or* 8*, or $G \cong \mathrm{Sym}_4$, or $G \cong \mathrm{Alt}_4$.*

Proof. From $\mathcal{C}_G(H) = H$, no element in $G \setminus H$ commutes with every element of H. Hence, $|H| \neq 2$. Furthermore, the factor group G/H can be considered as an automorphism group of H. Hence, if $|H| = 3$ then G is a dihedral group of order 6 while if $|H| = 4$, then either G is a dihedral group of order 8 when H is a cyclic group of order 4, or G is a subgroup of Sym_4 when H is an elementary abelian group and G. Then G is either dihedral order ≥ 8, or Alt_4, or Sym_4. □

This completes the proof of Theorem 4.8.1.

4.9 THE PROOF OF THE MAIN THEOREM

Take a minimal normal subgroup H of G. If H is not solvable, then H is either a simple group of the product of isomorphic simple groups. From Proposition [25,

Theorem 4.2], the latter can not occur. Therefore, if H is not solvable, then $H \cong \mathrm{Alt}_5$ (Proposition 4.7.1). Two cases are considered separately, according as $C_G(H)$ is trivial or not. If $|C_G(C)| > 1$, take a non-trivial element $u \in C_G(C)$ and define U to be the group generated by u together with a dihedral subgroup D_5 of H of order 10. Since u centralizes D_5, the latter group is normal in U. From Proposition 4.4.9, $C_G(H)$ must be itself dihedral. Since u is in the center of a dihedral group, u has order 2. Now, the group generated by u with an elementary abelian subgroup of H of order 4 is elementary abelian of order 8. But this contradicts Proposition [25, Theorem 4.2]. Therefore $C_G(H)$ is trivial, equivalently G is contained in the the automorphism group of H. From this either $G = H \cong \mathrm{Alt}_5$ or $G \cong PGL(2,5)$. In the latter case, G contains a subgroup isomorphic to the semidirect product of C_5 by C_4. But this contradicts Proposition 4.4.9. Hence, if H is not solvable, then $H \cong \mathrm{Alt}_5$.

If H is solvable then it is an elementary abelian group of order $d \geq 2$. Assume first that d is a power of 2. By Proposition [25, Theorem 4.2], $h \leq 2$. Therefore Theorem 1.0.1 follows from Proposition 4.8.1.

Now, let $d \neq 25$ be odd. Theorem 4.5.4 yields that every dual 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing H is algebraic. Actually this holds true for $d = 9$ by Proposition 4.3.2. Therefore, Proposition 4.5.1 implies for $d \neq 3$ that one of the cases (I), (II) occurs. For $d = 3$, this follows from Proposition 4.8.1.

Finally, let $d = 25$. If any dual 3-subnet realizing H is algebraic then the above argument still works and case (I) holds. So we are left with the case where some dual 3-subnet realizing H is not algebraic. Then, we must show that $G = H$. From Proposition 4.6.4, H is a Sylow 5-subgroup of G. Zassenhaus' theorem [14, 10.1 Hauptsatz] yields that $G = W \ltimes H$ with a subgroup W of order prime to 5. If W has an element of odd order then G has a subgroup of odd order that properly contains H. In this case, (VIII) occurs by Proposition 4.6.6. Therefore, we may assume that $|W| =$

2^h. By Theorem 4.5.4, no element in G outside H commutes with every element in H otherwise G would have an abelian subgroup properly containing H. Let $w \in W$ be an involution. Then the action of w on H by conjugacy is as an involutory automorphism of H. By an elementary fact on finite groups, see [14, Chapter 1.5,Aufgabe 14], there is an element $u \in H$ such that $wuw^{-1} = u^{-1}$. Therefore, the subgroup U generated by w and u is a dihedral group of order 10. From Proposition 4.4.6, any dual 3-net realizing U is of tetrahedron type. Therefore, a dual 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing U is triangular. But this together with Proposition 4.8.1 imply that any dual 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing H is algebraic, a contradiction.

CHAPTER 5

COMPUTATIONAL RESULTS ON SMALL 3-NETS

In this computer-aided investigation, combinatorial methods are used to study finite 3-nets realizing the groups $\mathbf{C}_2 \times \mathbf{C}_4$, $\mathbf{C}_3 \times \mathbf{C}_3$, and Alt_4. These results are fundamental for the complete classification of 3-nets embedded in a projective plane over a field, see [15]. Indeed, large groups could be dealt with using theoretical results, but small groups having elements of order less than 5 needed a more explicit computation.

We can summarize our computational results in the following theorem.

Theorem 5.0.1. *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net of order n which realizes a group G in the projective plane $PG(2, \mathbb{K})$ defined over an algebraically closed field $\mathbb{K}$ of characteristic p, where $p = 0$ or $p \geq 5$. We also assume that $n < p$ whenever $p > 0$. The following statements hold.*

(I) *If $G \cong \mathbf{C}_3 \times \mathbf{C}_3$ or $G \cong \mathbf{C}_2 \times \mathbf{C}_4$, then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic.*

(II) *If $p = 0$, then the group Alt_4 cannot be realized.*

The proof is divided in three parts, see Sections 5.1, 5.2, or 5.3, according as $G \cong \mathbf{C}_3 \times \mathbf{C}_3$, $G \cong \mathbf{C}_2 \times \mathbf{C}_4$, or $G \cong \mathrm{Alt}_4$.

5.1 $G \cong \mathbf{C_3} \times \mathbf{C_3}$

We denote by $G = \{0, \ldots, 8\}$ the elementary abelian group of order 9 given by the multiplication table

	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

.

Let H be the subgroup $\{0, 1, 2\}$ of G. Let $\mathbb{K}$ be an algebraically closed field whose characteristic is either 0 or larger than 9. In this chapter, all points are points of the projective plane over $\mathbb{K}$. We denote by ω a cubic root of unity in $\mathbb{K}$.

Lemma 5.1.1. *Let*

$$\Delta' = \{0_1, 1_1, 2_1, 0_2, 1_2, 2_2, 0_3, 1_3, 2_3\}$$

be a realization of H. Then there is a unique cyclic collineation α of order three mapping

$$0_1, 1_1, 2_1, 0_2, 1_2, 2_2, 0_3, 1_3, 2_3 \quad \textit{to} \quad 1_1, 2_1, 0_1, 1_2, 2_2, 0_2, 2_3, 0_3, 1_3,$$

respectively. α is never central. The cubic curves containing Δ' form a pencil. All these cubics are invariant under α. □

Lemma 5.1.2. *Let X be a set of nine points in a projective plane such that for all $A, B \in X$, the line AB contains a third point of X. Then, X is either contained in a line, or forms an $AG(2,3)$.* □

In the sequel, we denote by $\Delta = \{0_1, \ldots, 8_1, 0_2, \ldots, 8_2, 0_3, \ldots, 8_3\}$ a realization of G. We denote by Δ' the subset of Δ realizing the subgroup $H = \{0, 1, 2\}$. We will often use that the points of Δ can be re-indexed and the blocks $\{i_1\}$, $\{j_2\}$, $\{k_3\}$ can be interchanged.

Lemma 5.1.3. *There is a line which intersects Δ in exactly two points.*

Proof. Assume that no line intersects Δ in exactly two points. As $\mathbb{K}^*$ has no elementary abelian subgroup of order 9, Δ cannot be triangular or of conic-line type. Theorem 5.1 of [2] implies that none of the blocks $\{i_1\}$, $\{j_2\}$, $\{k_3\}$ is contained in a line. Lemma 5.1.2 implies that the union of these blocks must form an $AG(2,3)$. Moreover, each line intersecting Δ in more than two points, intersects Δ in precisely three points. In other words, Δ forms an $AG(3,3)$, which is not possible (see, [22]). □

By re-indexing Δ, we can suppose that the line $0_1 1_1$ intersects Δ in $\{0_1, 1_1\}$, that is, $0_1, 1_1, 2_1$ are not collinear. Let α be the cyclic collineation of order three corresponding to the subnet Δ' realizing $H = \{0, 1, 2\}$. We will choose our projective coordinate system such that the following hold:

(0) $0_1 = (1,0,0)$, $1_1 = (0,1,0)$ and $2_1 = (0,0,1)$.

(1) $F = (1,1,1)$ is a fixed point of α.

(2) If the lines $0_1 0_2$, $1_1 1_2$, $2_1 2_2$ are concurrent then $F = (1,1,1)$ is their intersection.

Notice that the lines i_1j_1 contain no fixed point of α, hence (2) does not conflict with (0). Furthermore, if 0_10_2, 1_11_2, 2_12_2 are concurrent then their intersection is a fixed point of α.

The collineation α has the matrix form

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

As 0_3 is not on the lines 1_i1_j, 0_3 has coordinates of the form $(a, b, 0)$ with $a, b \neq 0$. Then, we can compute the coordinates of the points $1_3 = (b, 0, a)$, $2_3 = (0, a, b)$ and $0_2 = (b, ba, a), 1_2 = (a, b, ba), 2_2 = (ba, a, b)$.

Let β be the cyclic collineation of order 3 corresponding to the subnet

$$\{0_1, 1_1, 2_1, 3_2, 4_2, 5_2, 3_3, 4_3, 5_3\}.$$

The matrix of β has the form

$$\begin{pmatrix} 0 & 0 & u \\ v & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

for some nonzero $u, v \in \mathbb{K}$. The point 3_2 has nonzero coordinates $(x, y, 0)$. Then, we have $4_2 = (u, vx, y)$, $5_2 = (uy, uv, vx)$ and

$$3_3 = (uy, vxy, vx),\ 4_3 = (xy, vx, y),\ 5_3 = (uvx, vuy, vxy).$$

For all points i_1, $i \in \{3, \ldots, 8\}$, there are three lines of the form j_2k_3, $j, k \in \{0, \ldots, 5\}$ such that $i_1 \in j_2k_3$. The fact that the corresponding line triples are con-

current, can be expressed by the equations

$$\begin{aligned}
\hat{f}_3 &= \det(0_2 \times 3_3, 1_2 \times 4_3, 2_2 \times 5_3) = 0,\\
\hat{f}_4 &= \det(0_2 \times 4_3, 1_2 \times 5_3, 2_2 \times 3_3) = 0,\\
\hat{f}_5 &= \det(0_2 \times 5_3, 1_2 \times 3_3, 2_2 \times 4_3) = 0,\\
f_6 &= \det(3_2 \times 0_3, 4_2 \times 1_3, 5_2 \times 2_3) = 0,\\
f_7 &= \det(3_2 \times 1_3, 4_2 \times 2_3, 5_2 \times 0_3) = 0,\\
f_8 &= \det(3_2 \times 2_3, 4_2 \times 0_3, 5_2 \times 1_3) = 0,
\end{aligned}$$

where $(a, b, c) \times (d, e, f)$ is the cross product of vectors (a, b, c) and (d, e, f). The values a, b, u, v, x, y determine Δ uniquely. The f_i's ($i \in \{3, \ldots, 8\}$) are polynomial expressions of these values. In fact, we will look at a, b, u, v, x, y as indeterminates over $\mathbb{K}$ and at the f_i's as elements of $\mathbb{K}[a, b, u, v, x, y]$. The polynomials f_7, f_8, f_9 have degree three in x, y, while for $i = 4, 5, 6$, the polynomials $\hat{f}_i$ have the form $\hat{f}_i = abvxyf_i$, where f_i is in $\mathbb{K}[a, b, u, v, x, y]$. The degree of f_4, f_5, f_6 in x, y is three.

Generally speaking, we are looking for specializations such that the corresponding configuration gives rise to a proper realization of G.

Lemma 5.1.4. *If any of the equations $u = 1$, $v = 1$, $u = v$ holds then Δ is algebraic.*

Proof. If $u = v = 1$ then $\alpha = \beta$. Let Γ be the cubic curve containing Δ' and 3_2. The equation of Γ can be computed explicitly, and one sees that if $u = v = 0$ then $3_3 \in \Gamma$. By Lemma 5.1.1 Γ is invariant under $\alpha = \beta$, and we have $4_2, 5_2, 4_3, 5_3 \in \Gamma$, too. Γ cannot be completely reducible since then, some i_1 would be collinear with some j_2, k_2. Suppose that $\Gamma = \ell \cup C$ with line ℓ and irreducible conic C. Then ℓ, C are α-invariant and the 1_i's are in 3. If $0_2 \in 3$ then $0_3, 1_3, 2_3 \in \ell$, and all 2_j's are in 3 and all 3_k's are in ℓ. As $\{0_1, 1_1, 2_1\}$, $\{0_2, 1_2, 2_2\}$, $\{0_3, 1_3, 2_3\}$, $\{3_2, 4_2, 5_2\}$, $\{3_3, 4_3, 5_3\}$ are all orbits of $\langle\alpha\rangle$ and the lines $0_23_3, 1_24_3, 2_25_3$ are concurrent, we have that $\{3_1, 4_1, 5_1\}$,

$\{6_1, 7_1, 8_1\}$ are $\langle\alpha\rangle$-orbits contained in C. Continuing the process, we conclude that $\Delta \subset \Gamma$ (which is not possible). The same result is obtained if we start from $j_2 \in C$ or $k_3 \in C$.

Suppose now that Γ is irreducible. Denote by Γ^* the set of nonsingular points. The $\langle\alpha\rangle$-orbits are all cosets of a subgroup H^* of $(\Gamma^*, +)$ of order 3. Then, simple arithmetic on Γ^* yields that $\{3_1, 4_1, 5_1\}$, $\{6_1, 7_1, 8_1\}$ are H^* cosets of Γ^*. Repeating this argument, we obtain $\Delta \subset \Gamma$ again.

It remains to be shown that any of the equations $u = 1$, $v = 1$, $u = v$ implies the other two. For that we observe the following equations of rational expressions:

$$\begin{aligned}
\left.\frac{f_6}{\det(3_2 \times 0_3, 4_2 \times 1_3, 0_2 \times 4_3)}\right|_{u=0} &= \frac{v-1}{ay-1}, \\
\left.\frac{f_6}{\det(0_2 \times 5_3, 1_2 \times 3_3, 3_2 \times 0_3)}\right|_{v=0} &= \frac{u-1}{(ua-x)by}, \\
\left.\frac{f_6}{\det(0_2 \times 3_3, 1_2 \times 4_3, 3_2 \times 0_3)}\right|_{u=v} &= \frac{v-1}{(b-y)ax}.
\end{aligned}$$

In any of the cases, the denominators at the left hand side cannot be zero as the corresponding lines are not concurrent. This proves that one equation implies another one, and two imply the third. This finishes the proof. □

The proof of the following lemma contains some elementary, but heavy computation. This computation can be formally verified by any computer algebra system dealing with Groebner bases within a few seconds.

Lemma 5.1.5. *If $a^3 = b^3 = 1$ then $v = 1$. In particular, Δ is algebraic.*

Proof. We observe that $a^2 = b^2 = 0$ holds if and only if the lines $0_1 0_2$, $1_1 1_2$, $2_1 2_2$ and the lines $0_1 1_2$, $1_1 2_2$, $2_1 0_2$ are concurrent. (In other words, Δ' forms a dual $AG(2, 3)$.) Remember that in this case, our coordinate system is chosen such that $(0, 0, 0)$ is the fixed point $0_1 0_2 \cap 1_1 1_2 \cap 2_1 2_2$. This would give $b = 0$ and $a = \omega$ can be assumed without loss of generality.

Now, we can find polynomials $s_i, t_i, p_1, p_2, q_1, q_2$, $i \in \{3, \ldots, 8\}$, in the indeterminates a, b, x, y, u, v with integer coefficients such that

$$\begin{aligned}\sum s_i f_i + p_1(a-\omega) + p_2(b-1) &= 18xv(v-1)(vx-y^2)(vx-\omega y^2),\\ \sum t_i f_i + q_1(a-\omega) + q_2(b-1) &= 18(v-1)(uy^3-v^2x^3).\end{aligned}$$

Assume $v \neq 1$. Since $\det(0_1, 3_2, 4_2) = y^2 - vx \neq 0$, we have $vx - \omega y^2 = uy^3 - v^2x^3 = 0$. This implies $u = \omega^2 xy$ and $v = \omega y^2/x$. Straightforward computation shows that the collineation γ given by the matrix

$$\begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

fixes $0_1, 1_1, 2_1$ and maps the points $0_2, \ldots, 5_2, 0_3, \ldots, 5_3$ to the points

$$1_2, 2_2, 0_2,\ 5_2, 3_2, 4_2,\ 1_3, 2_3, 0_3,\ 5_3, 3_3, 4_3,$$

respectively. As $5 \cdot 2 = 6$ and $5 \cdot 3 = 4$ in G, we have

$$\gamma(3_1) = \gamma(0_2 3_3 \cap 1_2 4_3) = 1_2 5_3 \cap 2_2 3_3 = 4_1.$$

Similarly, $\gamma(4_1) = 5_1$ and $\gamma(5_1) = 3_1$. Thus, γ permutes the lines $3_1 0_3$, $4_1 1_3$, $5_1 2_3$ cyclically. As these lines intersect in 6_2, 6_2 would be a fixed point of γ, which is not possible. □

Lemma 5.1.6. *If any two of the equations*

$$\begin{aligned} 0 &= \omega^2 b + ab^2\omega + a^2,\\ 0 &= b^2\omega + \omega^2 a + ba^2,\\ 0 &= \omega b + \omega^2 ab^2 + a^2,\\ 0 &= a\omega + ba^2 + \omega^2 b^2 \end{aligned}$$

hold for a, b then Δ is algebraic:

Proof. Computing the resultants of any two of these formulas with respect to a and b, we conclude that they imply $a^3 = b^3 = 1$. Hence, Δ is algebraic by Lemma 5.1.5. $\square$

We are now prepared to prove the main result.

Theorem 5.1.7. Δ *is algebraic.*

Proof. We can consider the f_i's as polynomials in the indeterminates a, b, u, v, x, y. Fix the values a, b, u, v and let $F_i(X, Y)$ be the polynomials in two variables such that $F_i(x, y) = f_i(a, b, u, v, x, y)$. Define the space L generated by the F_i's.

Recall that β is the collineation of order 2 mapping the points 0_1, 1_1, 2_1, 3_2, 4_2, 5_2, 3_3, 4_3, 5_3 to 1_1, 2_1, 0_1, 4_2, 5_2, 3_2, 5_3, 3_3, 4_3, respectively. From the definition of the f_i's one sees that the substitution $X' = u/Y$, $Y' = vX/Y$ induces a linear automorphism of L of degree 3. We will denote this induced map by β, as well.

Define the polynomials

$$E_1 = uvX + \omega^2 uY^2 + \omega vX^2Y, \qquad E_2 = vX^2 + \omega^2 uY + \omega Y^2X,$$
$$\bar{E}_1 = uvX + \omega uY^2 + \omega^2 vX^2Y, \qquad \bar{E}_2 = vX^2 + \omega uY + \omega^2 Y^2X,$$

and

$$Q_1 = \omega F_7 - F_8, \qquad Q_2 = \omega^2 F_4 - F_5,$$
$$\bar{Q}_1 = \omega^2 F_7 - F_8, \qquad \bar{Q}_2 = \omega F_4 - F_5$$

of L. Then E_1, E_2, Q_1, Q_2 are eigenvectors of β with eigenvalue $\omega uv/Y^3$ and $\bar{E}_1, \bar{E}_2, \bar{Q}_1, \bar{Q}_2$ are eigenvectors of β with eigenvalue $\omega^2 uv/Y^3$. We have the following resultant values:

$$R_{E_1,E_2}(Y) = \omega^2 uvY(uv - Y^3)^2, R_{\bar{E}_1,\bar{E}_2}(Y) = \omega uvY(uv - Y^3)^2.$$

This shows that the intersection of $E_1 = 0, E_2 = 0$ and the intersection of $\bar{E}_1 = 0, \bar{E}_1 = 0$ consist of the points $0_1, 1_1, 1_1$ (with multiplicity 0) and the fixed points of β (with multiplicity 2). In particular, E_1, E_2 and $\bar{E}_1, \bar{E}_2$ are linearly independent.

Straightforward calculation shows that

$$Q_1 = G_{11}E_1 + G_{12}E_2, \qquad Q_2 = G_{21}E_1 + G_{22}E_2,$$
$$\bar{Q}_1 = \bar{G}_{11}\bar{E}_1 + \bar{G}_{12}\bar{E}_2, \qquad \bar{Q}_2 = \bar{G}_{21}\bar{E}_1 + \bar{G}_{22}\bar{E}_2,$$

where

$$\begin{aligned}
G_{11} &= (\omega^2 b + ab^2\omega + a^2)(\omega^2 + v\omega + u),\\
G_{12} &= (b^2\omega + \omega^2 a + a^2 b)(uv + \omega^2 u + v\omega),\\
G_{21} &= \omega(\omega^2 b + ab^2\omega + a^2)(\omega + \omega^2 v + u),\\
G_{22} &= (b^2\omega + \omega^2 a + a^2 b)(\omega u + \omega^2 v + uv),\\
\bar{G}_{11} &= (\omega b + \omega^2 ab^2 + a^2)(\omega + \omega^2 v + u),\\
\bar{G}_{12} &= (a\omega + a^2 b + \omega^2 b^2)(\omega u + \omega^2 v + uv),\\
\bar{G}_{21} &= \omega^2(\omega b + \omega^2 ab^2 + a^2)(\omega^2 + v\omega + u),\\
\bar{G}_{22} &= (a\omega + a^2 b + \omega^2 b^2)(uv + \omega^2 u + v\omega).
\end{aligned}$$

Assume that Q_1, Q_2 are linearly independent. Then $E_1, E_2 \in \langle Q_1, Q_2\rangle \leq L$. Therefore, $\Gamma_1 \cap \cdots \cap \Gamma_4$ is contained in the zero set of $E_1 = E_2 = 0$, a contradiction. We can similarly show that $\bar{Q}_1, \bar{Q}_2$ must be linearly dependent. This implies

$$\begin{aligned}
0 &= G_{11}G_{22} - G_{12}G_{21}\\
&= (2+\omega^2)(b^2\omega + \omega^2 a + ba^2)(\omega ab^2 + \omega^2 b + a^2)(u-v)(u-1)(v-1),\\
0 &= \bar{G}_{11}\bar{G}_{22} - \bar{G}_{12}\bar{G}_{21}\\
&= (2+\omega)(a\omega + ba^2 + \omega^2 b^2)(\omega b + \omega^2 ab^2 + a^2)(u-v)(u-1)(v-1).
\end{aligned}$$

Lemma 5.1.4, 5.1.5 and 5.1.6 imply that Δ is algebraic.

□

5.2 $G \cong \mathbf{C_2} \times \mathbf{C_4}$

The main ingredient of the proof is Proposition 2.3.5 (Lame's Theorem).

The group $C_2 \times C_4$ can be given by the multiplication table

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	7	8	5	6
4	4	3	2	1	8	7	6	5
5	5	6	7	8	2	1	4	3
6	6	5	8	7	1	2	3	4
7	7	8	5	6	4	3	2	1
8	8	7	6	5	3	4	1	2

.

The triple $\{i_1, j_2, k_3\}$ is collinear if and only if $i * j = k$.

The following 6-tuples of collinear points form a Lamé configuration:

$$U_1 = \{1_1, 1_2, 1_3\}, \{3_1, 5_2, 7_3\}, \{6_1, 7_2, 3_3\} + \{1_1, 7_2, 7_3\}, \{3_1, 1_2, 3_3\}, \{6_1, 5_2, 1_3\},$$

$$U_2 = \{1_1, 3_2, 3_3\}, \{3_1, 7_2, 5_3\}, \{6_1, 5_2, 1_3\} + \{1_1, 5_2, 5_3\}, \{3_1, 3_2, 1_3\}, \{6_1, 7_2, 3_3\},$$

$$U_3 = \{1_1, 1_2, 1_3\}, \{3_1, 7_2, 5_3\}, \{8_1, 5_2, 3_3\} + \{1_1, 5_2, 5_3\}, \{3_1, 1_2, 3_3\}, \{8_1, 7_2, 1_3\},$$

$$U_4 = \{1_1, 3_2, 3_3\}, \{3_1, 5_2, 7_3\}, \{8_1, 7_2, 1_3\} + \{1_1, 7_2, 7_3\}, \{3_1, 3_2, 1_3\}, \{8_1, 5_2, 3_3\}.$$

Let C be a cubic curve through the points

$$1_1, 1_2, 1_3, 3_1, 7_2, 7_3, 6_1, 7_2, 3_3.$$

Then $|C \cap U_1|, |C \cap U_2| \geq 8$, hence, C passes through the ninth points 3_2 and 5_2. It follows that $|C \cap U_3|, |C \cap U_4| \geq 8$. Thus, C contains

$$U_1 \cup U_2 \cup U_3 \cup U_4 = \{1_1, 3_1, 6_1, 8_1, 1_2, 3_2, 5_2, 7_2, 1_3, 3_3, 5_3, 7_3\}.$$

It is straightforward to check that any of the following Lamé configurations intersects C in at least 8 points:

$$\{1_1, 5_2, 5_3\}, \{3_1, 1_2, 3_3\}, \{5_1, 3_2, 7_3\} + \{1_1, 3_2, 3_3\}, \{3_1, 5_2, 7_3\}, \{5_1, 1_2, 5_3\},$$

$$\{1_1, 1_2, 1_3\}, \{3_1, 5_2, 7_3\}, \{7_1, 3_2, 5_3\} + \{1_1, 5_2, 5_3\}, \{3_1, 3_2, 1_3\}, \{7_1, 1_2, 7_3\},$$

$$\{1_1, 5_2, 5_3\}, \{6_1, 7_2, 3_3\}, \{8_1, 2_2, 7_3\} + \{1_1, 7_2, 7_3\}, \{6_1, 2_2, 5_3\}, \{8_1, 5_2, 3_3\},$$

$$\{1_1, 5_2, 5_3\}, \{6_1, 4_2, 7_3\}, \{8_1, 7_2, 1_3\} + \{1_1, 7_2, 7_3\}, \{6_1, 5_2, 1_3\}, \{8_1, 4_2, 5_3\},$$

$$\{1_1, 1_2, 1_3\}, \{6_1, 7_2, 3_3\}, \{8_1, 3_2, 6_3\} + \{1_1, 3_2, 3_3\}, \{6_1, 1_2, 6_3\}, \{8_1, 7_2, 1_3\},$$

$$\{1_1, 1_2, 1_3\}, \{6_1, 3_2, 8_3\}, \{8_1, 5_2, 3_3\} + \{1_1, 3_2, 3_3\}, \{6_1, 5_2, 1_3\}, \{8_1, 1_2, 8_3\}.$$

Hence, C contains the further points $5_1, 7_1, 2_2, 4_2, 6_3, 8_3$. Finally, we consider the Lamé configurations

$$\{1_1, 1_2, 1_3\}, \{2_1, 5_2, 6_3\}, \{6_1, 2_2, 5_3\} + \{1_1, 5_2, 5_3\}, \{2_1, 2_2, 1_3\}, \{6_1, 1_2, 6_3\},$$

$$\{3_1, 1_2, 3_3\}, \{4_1, 7_2, 6_3\}, \{6_1, 2_2, 5_3\} + \{3_1, 7_2, 5_3\}, \{4_1, 2_2, 3_3\}, \{6_1, 1_2, 6_3\},$$

$$\{1_1, 5_2, 5_3\}, \{7_1, 6_2, 3_3\}, \{8_1, 3_2, 6_3\} + \{1_1, 6_2, 6_3\}, \{7_1, 3_2, 5_3\}, \{8_1, 5_2, 3_3\},$$

$$\{1_1, 8_2, 8_3\}, \{5_1, 3_2, 7_3\}, \{6_1, 7_2, 3_3\} + \{1_1, 7_2, 7_3\}, \{5_1, 8_2, 3_3\}, \{6_1, 3_2, 8_3\},$$

$$\{1_1, 1_2, 1_3\}, \{7_1, 7_2, 2_3\}, \{8_1, 2_2, 7_3\} + \{1_1, 2_2, 2_3\}, \{7_1, 1_2, 7_3\}, \{8_1, 7_2, 1_3\},$$

$$\{3_1, 2_2, 4_3\}, \{5_1, 1_2, 5_3\}, \{6_1, 7_2, 3_3\} + \{3_1, 1_2, 3_3\}, \{5_1, 7_2, 4_3\}, \{6_1, 2_2, 5_3\}.$$

As before, one sees that any of them has at least 8 points in common with C, thus, C passes through all the points of the embedding of $C_2 \times C_4$.

5.3 $G \cong \mathbf{Alt}_4$ $(p = 0)$

Let the group Alt_4 be given on the underlying set $\{1, \ldots, 12\}$ by the Cayley table

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	7	8	5	6	12	11	10	9
3	3	4	1	2	8	7	6	5	10	9	12	11
4	4	3	2	1	6	5	8	7	11	12	9	10
5	5	6	7	8	9	10	11	12	1	2	3	4
6	6	5	8	7	11	12	9	10	4	3	2	1
7	7	8	5	6	12	11	10	9	2	1	4	3
8	8	7	6	5	10	9	12	11	3	4	1	2
9	9	10	11	12	1	2	3	4	5	6	7	8
10	10	9	12	11	3	4	1	2	8	7	6	5
11	11	12	9	10	4	3	2	1	6	5	8	7
12	12	11	10	9	2	1	4	3	7	8	5	6

We have that the points $1_1, \ldots, 12_1$, $1_2, \ldots, 12_2$, $1_3, \ldots, 12_3$ of the complex projective plane form a realization of Alt_4, if for all $i, j, k = 1, \ldots, 12$, i_1, j_2, k_3 are collinear if and only if $i * j = k$.

Proposition 5.3.1. Alt_4 *cannot be realized on the complex projective plane.*

Proof. We see that $\{1, 2, 3, 4\}$ is an elementary Abelian normal subgroup and $\{1, 5, 9\}$

is a subgroup. Without a loss of generality, we can assume that

$$\begin{array}{llll} 1_1 = [1,0,0], & 2_1 = [0,1,1], & 3_1 = [-a,-b,-c], & 4_1 = [1-a,-1-b,1-c], \\ 1_2 = [0,1,0], & 2_2 = [1,0,1], & 3_2 = [1-a,-1-b,-c], & 4_2 = [-a,-b,1-c], \\ 1_3 = [1,-1,0], & 2_3 = [0,0,1], & 3_3 = [-a,-1-b,-c], & 4_3 = [1-a,-b,1-c], \end{array}$$

and,

$$\begin{array}{ll} 5_1 = [d_1,d_3,1], & 9_1 = [d_2,d_4,1], \\ 5_2 = [d_2+d_4-d_5,d_5,1], & 9_2 = [d_1+d_3-d_6,d_6,1], \\ 5_3 = [d_1,d_5,1], & 9_3 = [d_2,d_6,1]. \end{array}$$

Define the points

$$\begin{array}{lll} 5_1 = 9_2 1_3 \cap 1_2 5_3, & 5_2 = 9_1 1_3 \cap 1_1 5_3, & 5_3 = 5_1 1_2 \cap 1_1 5_2, \\ 6_1 = 9_2 4_3 \cap 2_2 5_3, & 6_2 = 9_1 2_3 \cap 4_1 5_3, & 6_3 = 5_1 2_2 \cap 4_1 5_2, \\ 7_1 = 9_2 2_3 \cap 3_2 5_3, & 7_2 = 9_1 3_3 \cap 2_1 5_3, & 7_3 = 5_1 3_2 \cap 2_1 5_2, \\ 8_1 = 9_2 3_3 \cap 4_2 5_3, & 8_2 = 9_1 4_3 \cap 3_1 5_3, & 8_3 = 5_1 4_2 \cap 3_1 5_2, \\ 9_1 = 5_2 1_3 \cap 1_2 9_3, & 9_2 = 5_1 1_3 \cap 1_1 9_3, & 9_3 = 9_1 1_2 \cap 1_1 9_2, \\ 10_1 = 5_2 3_3 \cap 2_2 9_3, & 10_2 = 5_1 2_3 \cap 3_1 9_3, & 10_3 = 9_1 2_2 \cap 3_1 9_2, \\ 11_1 = 5_2 4_3 \cap 3_2 9_3, & 11_2 = 5_1 3_3 \cap 4_1 9_3, & 11_3 = 9_1 3_2 \cap 4_1 9_2, \\ 12_1 = 5_2 2_3 \cap 4_2 9_3, & 12_2 = 5_1 4_3 \cap 2_1 9_3, & 12_3 = 9_1 4_2 \cap 2_1 9_2, \end{array}$$

Let us denote by d_{ijk} the determinant of the 3×3 matrix with rows i_1, j_2, k_3. We define the sets

$$X = \{d_{ijk} \mid k = i * j\} \text{ and } Y = \{d_{ijk} \mid k \neq i * j\}$$

of polynomials in variables $a, b, c, d_1, \cdots, d_6$. Clearly, Alt_4 has a realization if and only if one can substitute complex numbers in $a, b, c, d_1, \cdots, d_6$ such that all polynomials in X are zero and all polynomials in Y are not zero.

Let Y' be the set of irreducible factors of polynomials in Y and put

$$X' = \{f/g \mid f \in X, g \in Y', g|f\}.$$

It is still true that Alt_4 has a realization if and only if one can substitue complex numbers in $a, b, c, d_1, \cdots, d_6$ such that all polynomials in X' vanish. A Groebner basis computation shows that the ideal generated by X' contains the polynomials $d_1 - d_2$, $d_3 - d_4$, implying $5_1 = 9_1$, a contradiction. $\square$

APPENDIX A

MAPLE CODE FOR THE CASE $G = C_3 \times C_3$

This appendix contains the implementation of the computations of Section 5.1 in the computer algebra system MAPLE 13.

```
#########################################################
# Maple 13 program for computing with dual 3-nets
# G = C3 x C3
#########################################################
# Preparation

with(LinearAlgebra):

isect:=proc(a,b,c,d)
  evala(CrossProduct(CrossProduct(a,b),CrossProduct(c,d))):
end proc:
idet:=proc(a,b,c,d,e,f)
  evala(Determinant(<CrossProduct(a,b)|CrossProduct(c,d)|CrossProduct(e,f)>)):
end proc:

alias(omega=RootOf(X^2+X+1));

#########################################################
# Part 1: Constructing the points, the transformations and the equations.
# One defines the transformations, the base points and the equations which
# correspond to certain collinearities. The unknowns $a,b,u,v,x,y$ are seen as
# fixed elements of the base field.
# In the program, Px_i denotes the point $x_i$ of the dual $3$-net.

alpha:=<<0,1,0>|<0,0,1>|<1,0,0>>;
beta:=<<0,v,0>|<0,0,1>|<u,0,0>>;

P0_1:=<1,0,0>: P1_1:=<0,1,0>: P2_1:=<0,0,1>:
```

```
P3_2:=<x,y,1>; P4_2:=beta.P3_2; P5_2:=beta.P4_2;
P0_3:=<a,b,1>; P1_3:=(alpha^(-1)).P0_3; P2_3:=(alpha^(-1)).P1_3;
                    # We turn Lambda_3 in the opposite direction!

P0_2:=isect(P0_1,P0_3,P1_1,P1_3);
P1_2:=isect(P0_1,P1_3,P1_1,P2_3);
P2_2:=isect(P0_1,P2_3,P1_1,P0_3);
P3_3:=isect(P0_1,P3_2,P1_1,P5_2);
P4_3:=isect(P0_1,P4_2,P1_1,P3_2);
P5_3:=isect(P0_1,P5_2,P1_1,P4_2);

f:=[  0,0,
  idet(P0_2,P3_3,P1_2,P4_3,P2_2,P5_3)/(a*b*v*x*y),  # P3_1
  idet(P0_2,P4_3,P1_2,P5_3,P2_2,P3_3)/(a*b*v*x*y),  # P4_1
  idet(P0_2,P5_3,P1_2,P3_3,P2_2,P4_3)/(a*b*v*x*y),  # P5_1
  idet(P3_2,P0_3,P4_2,P1_3,P5_2,P2_3),              # P6_1
  idet(P3_2,P1_3,P4_2,P2_3,P5_2,P0_3),              # P7_1
  idet(P3_2,P2_3,P4_2,P0_3,P5_2,P1_3)               # P8_1
]:
f:=factor(f):

##########################################################
# Part 2 (Lemma 2.4): Any of u=1, v=1, u=v implies the other two equations.

factor(subs(u=1,f[6]/idet(P0_2,P4_3,P3_2,P0_3,P4_2,P1_3)));
factor(subs(v=1,f[6]/idet(P0_2,P5_3,P1_2,P3_3,P3_2,P0_3)));
factor(subs(u=v,f[6]/idet(P0_2,P3_3,P1_2,P4_3,P3_2,P0_3)));

##########################################################
# Part 3 (Lemma 2.5): If a^3=b^3=1 then v=1.
# We can assume a=omega and b=1.

gb:=Groebner[Basis]([op(f),a-omega,b-1], plex(u,v,x,y,a,b),output=extended):
factor(gb[1][3]),factor(gb[1][5]);

# We construct the cofactors explicitely:
s:=evala(18*gb[2][3][1..8]):
t:=evala(18*gb[2][5][1..8]):
q:=evala(18*[gb[2][5][9],gb[2][5][10]]):
```

```
p:=evala(18*[gb[2][3][9],gb[2][3][10]]):

factor(add(f[i]*s[i],i=3..8)+p[1]*(a-omega)+p[2]*(b-1));
factor(add(f[i]*t[i],i=3..8)+q[1]*(a-omega)+q[2]*(b-1));

# This shows that all cofactors have coefficients in Z[omega]:
seq(denom(factor(_u)),_u in [op(s),op(t),op(p),op(q)]);

##########################################################
# Part 4: Computation with the beta-invariant polynomials.
# From now on, we consider $a,b,u,v$ as fixed elements of the base field
# and $X,Y$ as indetereminates.
# We define the action of $\beta$ on the polynomial ring in two variables.

F:=map(_x->subs({x=X,y=Y},_x),f): map(_x->degree(_x,{X,Y}),F);

betaonpoly:=proc(U) return factor(subs({X=u*Y/(v*X),Y=u/X},U)): end proc:

# This shows that the nontrivial solutions of F[3]=F[4]=F[5]=0
# and F[6]=F[7]=F[8]=0 are $\beta$-invariant:

map(_x->factor(_x),
  [betaonpoly(F[3])/F[5],betaonpoly(F[4])/F[3],betaonpoly(F[5])/F[4]]
);
map(_x->factor(_x),
  [betaonpoly(F[6])/F[7],betaonpoly(F[7])/F[8],betaonpoly(F[8])/F[6]]
);

# We define the E[i]'s, barE[i]'s, Q[i]'s and barQ[i]'s
# and show that their curves are $\beta$-invariant:

E:=[u*v*X+omega^2*u*Y^2+omega*v*X^2*Y,v*X^2+omega^2*u*Y+omega*Y^2*X]:
barE:=[u*v*X+omega*u*Y^2+omega^2*v*X^2*Y,v*X^2+omega*u*Y+omega^2*Y^2*X]:

Q:= [omega * F[6]-F[7],omega^2 * F[3]-F[4]]:
barQ:= [omega^2 * F[6]-F[7],omega * F[3]-F[4]]:

seq(factor(betaonpoly(_u)/_u), _u in [op(E),op(Q)]);
seq(factor(betaonpoly(_u)/_u), _u in [op(barE),op(barQ)]);
```

```
# We define the G[i,j]'s and barG[i,j]'s.
# We show that they are indeed coefficients of Q[i]'s and barQ[i]'s.

G[2,1]:=omega*(omega^2*b+a*b^2*omega+a^2)*(omega+omega^2*v+u);
G[2,2]:=(b^2*omega+omega^2*a+a^2*b)*(omega*u+omega^2*v+u*v);
G[1,1]:=(omega^2*b+a*b^2*omega+a^2)*(omega^2+v*omega+u);
G[1,2]:=(b^2*omega+omega^2*a+a^2*b)*(u*v+omega^2*u+v*omega);
barG[1,1]:=(omega*b+omega^2*a*b^2+a^2)*(omega+omega^2*v+u);
barG[1,2]:=(omega*a+a^2*b+omega^2*b^2)*(omega*u+omega^2*v+u*v);
barG[2,1]:=omega^2*(omega*b+omega^2*a*b^2+a^2)*(omega^2+v*omega+u);
barG[2,2]:=(omega*a+a^2*b+omega^2*b^2)*(u*v+omega^2*u+v*omega);

map(_x->evalb(factor(_x)), [
  Q[1]=G[1,1]*E[1]+G[1,2]*E[2],
  Q[2]=G[2,1]*E[1]+G[2,2]*E[2],
  barQ[1]=barG[1,1]*barE[1]+barG[1,2]*barE[2],
  barQ[2]=barG[2,1]*barE[1]+barG[2,2]*barE[2]
]);

# We compute the factors of the determinants of the G[i,j]'s and barG[i,j]'s:

map(_x->evalb(factor(_x)), [
  G[1,1]*G[2,2]-G[1,2]*G[2,1]=
    (2+omega^2)*(b^2*omega+omega^2*a+b*a^2)*(omega*a*b^2+omega^2*b+a^2)*(u-v)*(u-1)*(v-1),
  barG[1,1]*barG[2,2]-barG[1,2]*barG[2,1]=
    (2+omega)*(a*omega+b*a^2+omega^2*b^2)*(omega*b+omega^2*a*b^2+a^2)*(u-v)*(u-1)*(v-1)
]);

ra:=resultant(
  (-b+a*b^2*omega-omega*b+a^2)*(-b^2*omega+a+a*omega-b*a^2),
  (-omega*b+a*b^2+a*b^2*omega-a^2)*(a*omega+b*a^2-b^2-b^2*omega),
  a):
rb:=resultant(
  (-b+a*b^2*omega-omega*b+a^2)*(-b^2*omega+a+a*omega-b*a^2),
  (-omega*b+a*b^2+a*b^2*omega-a^2)*(a*omega+b*a^2-b^2-b^2*omega),
  b):
factor(ra/(b^3-1)^6);
factor(rb/(a^3-1)^6);
```

APPENDIX B

MAPLE CODE FOR THE CASE $G = \mathbf{Alt}_4$

This appendix contains the implementation of the computations of Section 5.3, using the F4 algorithm [7] in the computer algebra system Maple 13. This program does not store the cofactors of the Groebner bases, hence one cannot verify the result symbolically. The computation takes less than 3 minutes.

```
#########################################################
# Maple 13 program for computing with dual 3-nets
# G = Alt(4)
#########################################################
# Preparation

with(LinearAlgebra);
isect:=proc(a,b,c,d)
  evala(CrossProduct(CrossProduct(a,b),CrossProduct(c,d))):
end proc:

ct:=Matrix(
[ [ 1,2,3,4,5,6,7,8,9,10,11,12 ],
  [ 2,1,4,3,7,8,5,6,12,11,10,9 ],
  [ 3,4,1,2,8,7,6,5,10,9,12,11 ],
  [ 4,3,2,1,6,5,8,7,11,12,9,10 ],
  [ 5,6,7,8,9,10,11,12,1,2,3,4 ],
  [ 6,5,8,7,11,12,9,10,4,3,2,1 ],
  [ 7,8,5,6,12,11,10,9,2,1,4,3 ],
  [ 8,7,6,5,10,9,12,11,3,4,1,2 ],
  [ 9,10,11,12,1,2,3,4,5,6,7,8 ],
  [ 10,9,12,11,3,4,1,2,8,7,6,5 ],
  [ 11,12,9,10,4,3,2,1,6,5,8,7 ],
  [ 12,11,10,9,2,1,4,3,7,8,5,6 ]
```

```
 ]);

d:=array(1..6);

#########################################################
# Part 1: We define the points of the dual 3-net
# using a,b,c,d[1],...d[6] as indeterminates.

P:=[  [<1,0,0>,<0,1,0>,<1,-1,0>],
      [<0,1,1>,<1,0,1>,<0,0,1>],
      [<a,b,c>,0,<a,1+b,c>],
      [0,0,0],
      [<d[1],d[2],1>,0,<d[1],d[3],1>],
      [0,0,0],
      [0,0,0],
      [0,0,0],
      [<d[4],d[5],1>,0,<d[4],d[6],1>],
      [0,0,0],
      [0,0,0],
      [0,0,0]  ];

# As P[4,1], P[1,2], P[4,3] are coll, we may assume wlog that
# P[4,1]=<a,b,c> and P[4,3]=<a,1+b,c>.
# Similar argument for P[5,3] and P[9,3], using the fact that
# these points cannot have last coordinate 0.

P[3,2]:=evala(isect(P[3,1],P[1,3],P[1,1],P[3,3])/c);
P[4,2]:=evala(isect(P[3,1],P[2,3],P[2,1],P[3,3])/a);

P[4,1]:=evala(isect(P[3,2],P[2,3],P[2,2],P[3,3])/(1+b));
P[4,3]:=evala(isect(P[1,1],P[4,2],P[2,1],P[3,2])/(1+b-c));

P[5,2]:=isect(P[1,1],P[5,3],P[9,1],P[1,3]);
P[9,2]:=isect(P[1,1],P[9,3],P[5,1],P[1,3]);

#########################################################

P[5,1]:=isect(P[9,2],P[1,3],P[1,2],P[5,3]):
P[5,2]:=isect(P[9,1],P[1,3],P[1,1],P[5,3]):
```

```
P[5,3]:=isect(P[5,1],P[1,2],P[1,1],P[5,2]):

P[6,1]:=isect(P[9,2],P[4,3],P[2,2],P[5,3]):
P[6,2]:=isect(P[9,1],P[2,3],P[4,1],P[5,3]):
P[6,3]:=isect(P[5,1],P[2,2],P[4,1],P[5,2]):

P[7,1]:=isect(P[9,2],P[2,3],P[3,2],P[5,3]):
P[7,2]:=isect(P[9,1],P[3,3],P[2,1],P[5,3]):
P[7,3]:=isect(P[5,1],P[3,2],P[2,1],P[5,2]):

P[8,1]:=isect(P[9,2],P[3,3],P[4,2],P[5,3]):
P[8,2]:=isect(P[9,1],P[4,3],P[3,1],P[5,3]):
P[8,3]:=isect(P[5,1],P[4,2],P[3,1],P[5,2]):

P[9,1]:=isect(P[5,2],P[1,3],P[1,2],P[9,3]):
P[9,2]:=isect(P[5,1],P[1,3],P[1,1],P[9,3]):
P[9,3]:=isect(P[9,1],P[1,2],P[1,1],P[9,2]):

P[10,1]:=isect(P[5,2],P[3,3],P[2,2],P[9,3]):
P[10,2]:=isect(P[5,1],P[2,3],P[3,1],P[9,3]):
P[10,3]:=isect(P[9,1],P[2,2],P[3,1],P[9,2]):

P[11,1]:=isect(P[5,2],P[4,3],P[3,2],P[9,3]):
P[11,2]:=isect(P[5,1],P[3,3],P[4,1],P[9,3]):
P[11,3]:=isect(P[9,1],P[3,2],P[4,1],P[9,2]):

P[12,1]:=isect(P[5,2],P[2,3],P[4,2],P[9,3]):
P[12,2]:=isect(P[5,1],P[4,3],P[2,1],P[9,3]):
P[12,3]:=isect(P[9,1],P[4,2],P[2,1],P[9,2]):



#########################################################
# Part 2: We construct the polynomial identities.

eqs:=[]:
for i from 1 to 12 do
  for j from 1 to 12 do
      aa:=Determinant(<P[i,1]|P[j,2]|P[ct[i,j],3]>):
      eqs:=[op(eqs),aa]:
```

```
  end do
end do:

#########################################################
# Part 3: We filter out the nonzero factors of the equations.

nepos:=[
[1, 2, 6], [9, 1, 10], [1, 10, 8], [5, 9, 2],
[9, 5, 2], [1, 10, 2], [1, 3, 11], [1, 4, 12],
[1, 5, 7], [9, 1, 12], [9, 5, 4], [5, 9, 4],
[1, 5, 6], [1, 6, 11], [1, 9, 12], [1, 12, 4],
[1, 5, 8], [1, 7, 3], [1, 7, 12], [5, 9, 3],
[9, 1, 11], [1, 12, 7], [1, 9, 11], [5, 1, 6],
[5, 1, 7], [1, 6, 2], [1, 3, 7], [1, 8, 4],
[1, 11, 6], [5, 1, 8], [9, 5, 3], [1, 8, 10],
[1, 11, 3], [1, 4, 8],[1, 9, 10], [1, 2, 10]
];
noneqs:=map(_x->Determinant(<P[_x[1],1]|P[_x[2],2]|P[_x[3],3]>),nepos):

noneqs:=mul(x,x in noneqs):

eqs:=select(x->x<>0,eqs): nops(eqs);
eqs_reduced:=map(x->factor(x/gcd(x,noneqs)),eqs):
map(degree,eqs)-map(degree,eqs_reduced);

#########################################################
# Part 4: We compute the Groebner basis of the corresponding ideal.
# This Groebner basis shows that d[1]=d[4], d[2]=d[5], d[3]=d[6].
# The computation takes less that 3 minutes using the F4 algorithm.

gb:=Groebner[Basis](eqs_reduced,tdeg(a,b,c,d[1],d[2],d[3],d[4],d[5],d[6]));
```

BIBLIOGRAPHY

[1] M. Arthebani and I. Dogachev. The hesse pencils of plane cubic curves. *Enseign. Math.*, (2) 55(3–4):235–273, 2009.

[2] A. Blokhuis, G. Korchmáros, and F. Mazzocca. On the structure of 3-nets embedded in a projective plane. *J. Combin. Theory Ser-A.*, 118:1228–1238, 2011.

[3] R. Brauer and M. Suzuki. On finite groups of even order whose 2-Sylow group is a quaternion group. *Proc. Nat. Acad. Sci. U.S.A.*, 45:1757–1759, 1959

[4] J. Dénes and A.D. Keedwell. *Latin Squares and their Applications*. Academic Press, New York-London, 1974.

[5] R.H. Dye. Hexagons, conics, A_5 and $PSL_2(K)$. *J. London Math. Soc.*, 44:270–286, 1991.

[6] M. Falk and S. Yuzvinsky. Multinets, resonance varieties, and pencils of plane curves. *Compos. Math.*, 143:1069–1088, 2007.

[7] J.-C. Faugere. A new efficient algorithm for computing Gröbner bases (F4). *J. Pure Appl. Algebra*, 139(1–3):61–88, 1999.

[8] D. Gorestein. The classification of Finite Simple Groups. Plenum Press, New York and London, 1983 xx+pp.

[9] D. Gorenstein and J.H. Walter. The characterization of finite groups with dihedral Sylow 2-subgroups. I.II.III. *J. Algebra* 2:85-131, 218-270, 354-393.

[10] D. Hilbert. Grundlagen der Geometrie, (English translation 1902). Teubner, Berlin, 1899.

[11] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford Univ. Press, Oxford, second ed edition, 1998.

[12] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic Curves Over a Finite Field*. Princeton Univ. Press, Princeton and Oxford, 2008.

[13] D.R. Hughes and F.C. Piper. *Projective Planes*, volume 6 of *Graduate Texts in Mathematics*. Springer, New York, 1973.

[14] B. Huppert. *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften 134. Springer, Berlin, 1967, xii+793 pp.

[15] G. Korchmáros, G.P. Nagy, and N. Pace. 3-nets realizing a group in a projective plane. arXiv:1104.4439.

[16] G. Korchmáros and N. Pace. Coset intersection of plane cubics. preprint.

[17] F.R. Moulton. A Simple Non-Desarguesian Plane Geometry. Transactions of the American Mathematical Society, 3(2):192–195, 1902.

[18] D.J. Madden and R.C. Valentini. The group of automorphisms of algebraic function fields. *J. Reine Angew. Math.*, 343:162–168, 1983.

[19] G.P. Nagy and N. Pace. Some computational results on small 3-nets embedded in a projective plane over a field. preprint.

[20] G. Orzech and M. Orzech. *Plane Algebraic Curves, an Introduction via Valuations*, volume 61 of *Monographs and Textbooks in Pure and Applied Mathematics*. Dekker, New York, 1981.

[21] J.V. Pereira and S. Yuzvinsky. Completely reducible hypersurfaces in a pencil. *Adv. Math.*, 219:672–688, 2008.

[22] H. Taniguchi. On the embedding of an affine space into a projective space. *Geometriae Dedicata*, 80:99–123, 2000.

[23] G. Urzúa. On line arrangements with applications to 3-nets. *Adv. Geom.*, 10:287–310, 2010.

[24] O. Veblen and W. H. Bussey. Finite projective geometries. *Trans. AMS*, 7:241–259, 1906.

[25] S. Yuzvinsky. Realization of finite abelian groups by nets in $\mathbb{P}^2$. *Compos. Math.*, 140:1614–1624, 2004.

[26] S. Yuzvinsky. A new bound on the number of special fibers in a pencil of curves. *Proc. Amer. Math. Soc.*, 137:1641–1648, 2009.