HERMITIAN FUNCTION FIELDS, CLASSICAL UNITALS, AND REPRESENTATIONS OF 3-DIMENSIONAL UNITARY GROUPS

GERHARD HISS

ABSTRACT. We determine the elementary divisors, and hence the rank over an arbitrary field, of the incidence matrix of the classical unital.

1. INTRODUCTION

A unital is a Steiner system with parameters 2, $m+1$, and m^3+1. This is a collection $\mathcal{L}$ of subsets of cardinality $m+1$ of a point set $\mathcal{P}$ of cardinality m^3+1 such that any two distinct points of $\mathcal{P}$ are contained in exactly one element of $\mathcal{L}$. The elements of $\mathcal{L}$ are called the lines of the unital. An example is provided by the set $\mathcal{U}$ of isotropic points of the projective plane $\mathbb{P}^2(\mathbb{F}_{q^2})$, with respect to a non-degenerate Hermitian form. A line of this classical or Hermitian unital consists of a set of collinear isotropic points. In this case $m = q$.

Given a finite incidence structure, one is often interested in the rank of its incidence matrix (over some field). For example, such an incidence matrix can be viewed as the generator matrix of a code, whose dimension is to be determined. Also, these ranks can be used to distinguish between incidence structures with the same set of parameters.

In this paper we determine the rank, over an arbitrary field, of the incidence matrix of the classical unital, thus proving a conjecture of Andriamanalimanana [2]. The same conjecture arose in a different context in the work of Geck [8], who established a close connection between the rank of this incidence matrix and a certain decomposition number of the 3-dimensional unitary group.

It is not hard to see that the incidence matrix of the classical unital $\mathcal{U}$ has full rank over the rational numbers. Thus its elementary divisors are the structural invariants of a finite abelian group A. Experimental evidence led Geck to a question on the elementary divisors of the incidence matrix, i.e., the structure of A: Is it true that $A \cong [\mathbb{Z}/(q+1)\mathbb{Z}]^{q^2-q+1}$ (see [8, p. 583])? We also show in this paper that Geck's question has a positive answer.

Let us now describe the content of the individual sections of our paper. In Section 2 we introduce the classical unital and the two conjectures about its incidence matrix. In Section 3 we describe the essential part of the automorphism group of the unital, the 3-dimensional projective unitary group $\mathrm{PGU}_3(q)$ and some of its subgroups needed later on. Theorem 4.1 of Section 4 contains the main representation theoretic result about $\mathrm{PGU}_3(q)$ used in the proof of Andriamanalimanana's conjecture. Apart from two special cases, the proof of Theorem 4.1 can be cited from the literature. A proof for the remaining cases is given in the appendix of our paper. Using Geck's link between the representation theory of $\mathrm{PGU}_3(q)$ and the rank of the incidence matrix, it is not hard to give a proof of Andriamanalimanana's conjecture in Section 5.

Section 6 is devoted to the elementary part of the proof of Geck's conjecture. This is elementary in the sense that it uses only the axioms of a unital and the action of the automorphism group. In fact, we give a proof of Geck's conjecture under a certain hypothesis (Hypothesis 6.4). It is not unreasonable to expect that one can show by elementary means that this hypothesis is always satisfied for the classical unital. However, we were not able to find such a proof.

Instead, in Section 7, we use some basic results about algebraic function fields to establish the validity of Hypothesis 6.4. Specifically, we consider the Hermitian function field K over $\mathbb{F}_{q^2}$. This is the function field of the Fermat curve $\mathcal{F}$: $x^{q+1}+y^{q+1}+z^{q+1}=0$. (For references on algebraic funtion fields and the concepts and facts introduced and summarized below, we refer the reader to Section 7.) The non-existence of certain functions of K with a particular pole implies the truth of Hypothesis 6.4 (cf. Lemma 7.1(b)).

In the remainder of Section 7 we give an interpretation of the group A introduced above in terms of the group $\mathcal{D}_K^0$ of divisor classes of degree 0 of K. The prime divisors of K of degree 1 agree with its Weierstraß points, and are in bijection with the points of the classical unital $\mathcal{U}$. Let M_0 denote the group of divisors of K which have degree 0 and whose support is contained in the set of Weierstraß points, i.e., the set of prime divisors of degree 1. Let $\mathcal{H}$ denote the group of principal divisors of K. The factor group $M_0/\mathcal{H}\cap M_0$ can be thought of as the "divisor class group on the Weierstraß points" of K. In [17], Rohrlich considered a similar structure for a Fermat curve over the complex numbers. We show (Theorem 7.3) that $M_0/\mathcal{H}\cap M_0$ is in fact all of $\mathcal{D}_K^0$ and that the latter is isomorphic to $[\mathbb{Z}/(q+1)\mathbb{Z}]^{q^2-q}$. We also show (Corollay 7.4) that that $\mathcal{D}_K^0$ is naturally isomorphic to a subgroup of A of index $q+1$. Finally Corollary 7.5 gives a result on the multiplicative group of K: we determine a generating set for the group of functions whose divisors have support in the set of Weierstraß points. We remark that, conversely, this corollary implies the conjectures of Geck and Andriamanalimanana, and thus also a proof of the repersentation theoretic facts of Section 4.

Let us add some comments on the history of this paper. It started with the investigations of Geck on the decompositon numbers of $\mathrm{SU}_3(q)$. He found all but one of these decomposition numbers, and showed that the missing one could be determined from the rank of the classical unital and vice versa (see [7, Kapitel 3] and [8, Section 5]). Geck's reformulation of the problem was inspired by research of Mortimer on the structure of permutation modules of 2-transitive permutation groups [14].

The author learned about algebraic function fields, curves and divisor class groups through lectures of Professor B. H. Matzat, seminar talks, and discussions with his colleagues at the IWR at Heidelberg during the years 1989–1997. In this time a preliminary draft of this paper was written, establishing the connection between the (at that time still unknown) decomposition numbers of $\mathrm{SU}_3(q)$ and a certain generating property for the Hermitian function field (now Corollary 7.5). The hope was to prove the latter result directly from the theory of function fields and deduce the desired decomposition number from this.

Since then the missing decomposition number has been determined by Okuyama and Waki [15], and Corollary 7.5 follows from this. It is not unlikely that someone finds an independent proof of this corollary, so that the original plan to obtain the decomposition number from a property of the Hermitian function field could work out.

2. The classical unital

Let p be a rational prime number and let q be a power of p. Put $k = \mathbb{F}_{q^2}$, the finite field with q^2 elements. Then $\alpha \mapsto \bar{\alpha} := \alpha^q$, $\alpha \in k$, is the unique automorphism of k of order 2. We define the *Hermitian form* f on $k^{3\times 1}$ by

$$f(\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}, \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}) := \alpha_1\bar{\beta}_3 + \alpha_2\bar{\beta}_2 + \alpha_3\bar{\beta}_1. \tag{1}$$

Points of $\mathbb{P}^2(k)$, the projective plane over k, are written as

$$\begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}, \qquad \alpha, \beta, \gamma \in k, \qquad (\alpha, \beta, \gamma) \neq (0, 0, 0).$$

A vector $v \in k^{3\times 1}$ is called *isotropic* (with respect to f), if $f(v, v) = 0$. A point of $\mathbb{P}^2(k)$ is called *isotropic*, if it consists of isotropic vectors (when considered as 1-dimensional subspace of $k^{3\times 1}$). It is easily checked that $\mathbb{P}^2(k)$ contains exactly the following $q^3 + 1$ isotropic points:

$$\mathfrak{p}_\infty = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \qquad \mathfrak{p}_{\alpha,\beta} = \begin{bmatrix} 1 \\ \alpha \\ \beta \end{bmatrix}, \quad \alpha, \beta \in k, \quad \alpha\bar{\alpha} + \bar{\beta} + \beta = 0.$$

The reason for denoting the isotropic points by Gothic letters will become apparent in Section 7.

Let $\mathcal{U}$ denote the incidence structure consisting of the isotropic points of $\mathbb{P}^2(k)$ and the lines of $\mathbb{P}^2(k)$ containing at least two distinct isotropic points. Then $\mathcal{U}$ is a *unital*, i.e. a 2-$(q^3 + 1, q + 1, 1)$ design, which means that each line contains exactly $q + 1$ points of $\mathcal{U}$ and that any two distinct points lie on exactly one line (see [3, 8.3]). It follows directly from the axioms of a unital, that each point lies on exactly q^2 lines and that the number of lines is $q^2(q^2 - q + 1)$. In the following we shall identify a line of $\mathcal{U}$ with the set of points of $\mathcal{U}$ incident to the line.

It is easy to find a set of $q^2 - q + 1$ pairwise non-intersecting lines of $\mathcal{U}$. For $\beta \in k$ such that $\beta + \bar{\beta} \neq 0$ let

$$\mathfrak{n}_\beta := \{\mathfrak{p}_{\alpha,\beta} \mid \alpha \in k, \alpha\bar{\alpha} + \bar{\beta} + \beta = 0\}.$$

Then $\mathfrak{n}_\beta$ is a line of $\mathcal{U}$, which in $\mathbb{P}^2(k)$ passes through the non-isotropic point $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$.

Therefore, the set of lines $\{\mathfrak{n}_\beta \mid \beta \in k, \beta + \bar{\beta} \neq 0\}$ together with the line joining $\mathfrak{p}_\infty$ with $\mathfrak{p}_{0,0}$ is a set of $q^2 - q + 1$ parallel lines.

Let I denote the incidence matrix of $\mathcal{U}$, a $q^2(q^2-q+1)\times(q^3+1)$-matrix. For $\ell = 0$ or a prime number, define $\mathrm{rk}_\ell(I)$ to be the rank of I considered as a matrix over a field of characteristic ℓ. It is not difficult to show that $\mathrm{rk}_\ell(I) = q^3+1$, unless $\ell \mid q+1$ (see the proof of Corollary 5.1 below). Computations by Andriamanalimanana for $q = 2, 3, 4, 5$ lead him to the following conjecture.

Conjecture 2.1. (Andriamanalimanana [2]) *If ℓ is a prime dividing $q+1$, then* $\mathrm{rk}_\ell(I) = q(q^2-q+1)$.

These computations have been extended by Key for q up to 13, using Magma (see [10, Section 4]).

There is a stronger conjecture dealing with the elementary divisors of I.

Conjecture 2.2. (Geck [8]) *The elementary divisors of I are 1, with multiplicity $q(q^2-q+1)$ and $q+1$, with multiplicity q^2-q+1.*

Geck checked this conjecture with a computer for $q = 2, 3, 4, 5$. He also remarked that the prime divisors of the elementary divisors of I are among the prime divisors of $q+1$, an observation which follows from the axioms of a unital.

3. The 3-dimensional unitary group

Let us keep the notation of the preceding section. In particular, k is the field with q^2 elements and f is the Hermitian form defined by (1).

We are going to use the representation theory of the 3-dimensional projective unitary group over k, which constitutes an essential part of the automorphism group of $\mathcal{U}$, to prove Conjecture 2.1. To introduce this group, let us put

$$w_0 := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \tag{2}$$

and set

$$\mathrm{GU}_3(q) := \{(\alpha_{ij}) \in \mathrm{GL}_3(q^2) \mid (\alpha_{ji})w_0(\bar{\alpha}_{ij}) = w_0\},$$

the 3-*dimensional general unitary group*. Then $\mathrm{GU}_3(q)$ is the group of isometries of f. The order of $\mathrm{GU}_3(q)$ is given by

$$|\mathrm{GU}_3(q)| = q^3(q^3+1)(q^2-1)(q+1).$$

The center Z of $\mathrm{GU}_3(q)$ consists of the scalar matrices contained in $\mathrm{GU}_3(q)$, and thus has order $q+1$. We put

$$G := \mathrm{PGU}_3(q) := \mathrm{GU}_3(q)/Z,$$

the 3-*dimensional projective unitary group*. The order of G equals

$$|G| = q^3(q^3+1)(q^2-1),$$

the center of G is trivial, and the commutator subgroup G' of G is the 3-*dimensional projective special unitary group*. This is a nonabelian simple group, unless $q = 2$. If 3 divides $q+1$, then G/G' is a cyclic group of order 3, otherwise $G = G'$.

We now consider various subgroups of $\mathrm{GU}_3(q)$. Let U consist of all elements of $\mathrm{GU}_3(q)$ of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & -\bar{\alpha} & 1 \end{pmatrix} \qquad \alpha, \beta \in k, \qquad \alpha\bar{\alpha} + \bar{\beta} + \beta = 0. \tag{3}$$

Then U is a Sylow p-subgroup of $\mathrm{GU}_3(q)$ of order $|U| = q^3$. Let T be the subgroup of $\mathrm{GU}_3(q)$ consisting of all elements of the form

$$\begin{pmatrix} \zeta^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \bar{\zeta} \end{pmatrix} \qquad \zeta \in k^{\times}. \tag{4}$$

Then T is cyclic of order $q^2 - 1$ and normalizes U. We put $B := TU$.

Finally let L denote the subgroup of elements of $\mathrm{GU}_3(q)$ of the form

$$\begin{pmatrix} \alpha_{11} & 0 & \alpha_{13} \\ 0 & 1 & 0 \\ \alpha_{31} & 0 & \alpha_{33} \end{pmatrix}$$

such that

$$\begin{pmatrix} \alpha_{11} & \alpha_{31} \\ \alpha_{13} & \alpha_{33} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \bar{\alpha}_{11} & \bar{\alpha}_{13} \\ \bar{\alpha}_{31} & \bar{\alpha}_{33} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus L is isomorphic to $\mathrm{GU}_2(q)$, the 2-dimensional general unitary group over k and we have

$$|L| = q(q^2 - 1)(q + 1).$$

The subgroups U, T, B, and L of $\mathrm{GU}_3(q)$ have trivial intersection with Z, the center of $\mathrm{GU}_3(q)$, and we therefore may and will identify them with subgroups of G. Thus B is a Borel subgroup of G and T is a maximal torus contained in B. The intersection $B_0 := B \cap L$ is a Borel subgroup of L. It has order $q(q^2-1)$ and it is a semidirect product of T with $U_0 := U \cap L$. Moreover, U_0 consists of the elements of the form (3) with $\alpha = 0$, it equals the center $Z(U)$ of U and it is a Sylow p-subgroup of L.

The symbols G, U, T, B, U_0, B_0 and L will have the above meaning for the remainder of this paper.

Clearly, G acts (from the left) on $\mathcal{U}$ as a group of automorphisms, but in general it is not the full automorphism group of $\mathcal{U}$ (which is $\mathrm{P\Gamma U}_3(q)$, the semidirect product of G with its group of field automorphisms, see [16]). The stabilizer of the point $\mathfrak{p}_\infty$ is the Borel subgroup B of G, and the unipotent subgroup U permutes the q^3 points of $\mathcal{U} \setminus \{\mathfrak{p}_\infty\}$ regularly. Let $\mathfrak{n}$ be the line in $\mathcal{U}$ joining $\mathfrak{p}_\infty$ and $\mathfrak{p}_{0,0}$. Then the stabilizer of $\mathfrak{n}$ equals L. Since the index of L in G is equal to the number of lines of $\mathcal{U}$, it follows that L permutes these lines transitively.

4. The permutation module of G on the cosets of B

Let F be an algebraically closed field of characteristic ℓ. If H is a subgroup of G we write F_H for the trivial FH-module and ${F_H}^G$ for the FG-permutation module on the cosets of H.

The following result gives the structure of ${F_B}^G$, the permutation module on the cosets of the Borel subgroup of G. Since G acts doubly transitively on the cosets of B, this adds to an investigation begun by Mortimer [14].

Theorem 4.1. *Up to isomorphism, ${F_B}^G$ has at most three composition factors, denoted by F_G, φ, and ϑ. The composition factor called φ has degree $q(q-1)$. It occurs if and only if ℓ divides $q+1$. Moreover, ${F_B}^G$ has the following structure.*

(b) (Mortimer [14] and Geck [7, 8]) *If ℓ does not divide q^3+1, then ${F_B}^G = F_G \oplus \vartheta$, and ϑ has degree q^3. If ℓ divides q^2-q+1, but not $q+1$, then ${F_B}^G$ is uniserial with socle series*

$$\begin{array}{c} F_G \\ \vartheta \\ F_G \end{array}$$

and ϑ has degree $(q-1)(q^2+q+1)$.

(c) (Geck [7, 8] and Okuyama-Waki [15]) *If ℓ is odd and $\ell \mid q+1$ or if $\ell = 2$ and $4 \mid q+1$, then ${F_B}^G$ is uniserial with socle series*

$$\begin{array}{c} F_G \\ \varphi \\ \vartheta \\ \varphi \\ F_G \end{array}$$

and ϑ has degree $(q-1)(q^2-q+1)$.

(d) (Erdmann [5]) *If $\ell = 2$ and $4 \mid q-1$, then ${F_B}^G$ has socle series*

$$\begin{array}{c} F_G \\ \varphi \oplus \vartheta \\ F_G \end{array}$$

and ϑ has degree $(q-1)(q^2+1)$. ■

For odd $\ell \neq 3$, the structure of ${F_B}^G$ is a consequence of the decomposition matrix of $\mathrm{GU}_3(q)$, recently completed by Okuyama and Waki [15], as well as the investigations of Mortimer and Geck on this permutation module in [14], [7, Kapitel 3], and [8, Section 5]. For $\ell = 3$ an additional argument is needed, based on the results of Koshitani and Kunugi [11]. This will be given in the appendix.

The case $\ell = 2$ and $4 \mid q-1$ can be derived from Erdmann's results in [5, Section 4]. Brouwer et al. have given a different proof in [4, Sections 5, 6]. The proof in case $\ell = 2$ and $4 \mid q+1$ is a slight modification of the original Okuyama-Waki argument. It will also be given in the appendix.

5. The proof of Andriamanalimanan's conjecture

We keep the notation of the preceding sections. In particular, F is an algebraically closed field of characteristic ℓ.

It was shown by Geck in [7, 8], that there is a close connection between the rank $\mathrm{rk}_\ell(I)$ of the incidence matrix I of $\mathcal{U}$ over the field F, and the structure of the permutation module ${F_B}^G$, investigated in the previous section. For example, Geck showed that if ℓ is odd and divides $q+1$, the knowledge of the structure of ${F_B}^G$ is equivalent to the knowledge $\mathrm{rk}_\ell(I)$. In particular, the degree of ϑ could be derived from this rank (see the remarks following [8, Theorem 5.2]).

As a corollary to Theorem 4.1 we obtain a proof of Andriamanalimanana's conjecture.

Corollary 5.1. *Recall that $\ell = 0$ or a prime number. We have*

$$\mathrm{rk}_\ell(I) = \begin{cases} q(q^2-q+1), & \text{if } \ell \mid q+1 \\ q^3+1, & \text{otherwise.} \end{cases}$$

Proof. This proof follows the ideas outlined in [7, Kapitel 3] and [8, Section 5]. The permutation representation of G (over F) on the cosets of B is equivalent to the permutation representation on the points of $\mathcal{U}$, and the permutation representation of G on the cosets of L is equivalent to that on the lines of $\mathcal{U}$.

The transpose of I (viewed as a matrix over F) describes the natural FG-homomorphism ${F_L}^G \to {F_B}^G$ sending a line of $\mathcal{U}$ to the sum of its points. Thus the rank of I over F equals the dimension of the image V of this homomorphism.

By choosing the points of $\mathcal{U}$ as F-basis for ${F_B}^G$, we may identify ${F_B}^G$ with $F^{1\times(q^3+1)}$ and V with its subspace spanned by the rows of I. Obviously, the dimension of V is larger than 1. Let Z denote the submodule of codimension 1 of ${F_B}^G$ consisting of the vectors with coefficient sum zero.

If ℓ does not divide $q+1$, then V is not contained in Z (since a line of $\mathcal{U}$ contains exactly $q+1$ points). Then $V = {F_B}^G$, by the module structure given in Theorem 4.1(b), and we are done in this case.

Suppose that ℓ divides $q+1$. Then $V \leq Z$. It follows from the considerations of [8, Section 5], that V does not have a factor module isomorphic to φ. (Geck has proved this only for odd ℓ but his argument also works for $\ell = 2$. Indeed, even for $\ell = 2$, the restriction of φ to L has only compositon factors of degree $q-1$. By Frobenius reciprocity, ${F_L}^G$ does not have any trivial factor module.) It follows from Theorem 4.1 that V is the unique submodule of ${F_B}^G$ which has ϑ as its unique factor module. In this case the dimension of V equals $q(q^2-q+1)$. ∎

It would be nice to find a purely combinatorial proof of Conjecture 2.1. Brouwer, Wilbrink, and Haemers have given such a proof in case $\ell = 2$ and $4 \mid q-1$ (see [4, Sections 5, 6]). R. A. Liebler, in private communication, has announced such a proof in the general case.

6. Towards a proof of Geck's conjecture

In this section we prove Conjecture 2.2 under an additional hypothesis which will later shown to be always satisfied.

Before doing so, we introduce some more notation. Let M denote the free abelian group on the points of $\mathcal{U}$. We view a line of $\mathcal{U}$ as an element of M by identifying the line with the sum of its points in M. Let N be the subgroup of M generated by the lines of $\mathcal{U}$. (If we identify M with $\mathbb{Z}^{1\times(q^3+1)}$, then N is the subgroup spanned by the rows of I.) Conjecture 2.2 is equivalent to the statement

$$M/N \cong [\mathbb{Z}/(q+1)\mathbb{Z}]^{q^2-q+1}$$

(where the latter denotes a direct sum of q^2-q+1 copies of the cyclic group $\mathbb{Z}/(q+1)\mathbb{Z}$ of order $q+1$).

The next proposition is due to B. H. Matzat. It uses the action of G on $\mathcal{U}$ to bound the exponent of M/N.

Proposition 6.1. *The elementary divisors of I divide $q+1$.*

Proof. We have to show that $(q+1)\mathfrak{p} \in N$ for every point $\mathfrak{p}$ of $\mathcal{U}$.

Since $\mathcal{U}$ contains a system of q^2-q+1 parallel lines (see Section 2), the sum $\mathfrak{u}$ of all points of $\mathcal{U}$ is in N. Consider a line $\mathfrak{m}$ not containing $\mathfrak{p}_\infty$. Since U acts regularly on the set of points of $\mathcal{U}$ different from $\mathfrak{p}_\infty$, the U-orbit of each of the $q+1$ points of $\mathfrak{m}$ consists of all points of $\mathcal{U}$ but $\mathfrak{p}_\infty$.

Thus $\sum_{u\in U} u\mathfrak{m} = (q+1)(\mathfrak{u}-\mathfrak{p}_\infty)$. Since the left hand side of this equation is in N, it follows that $(q+1)\mathfrak{p}_\infty \in N$. Since G is transitive on the points of $\mathcal{U}$, we are done. ■

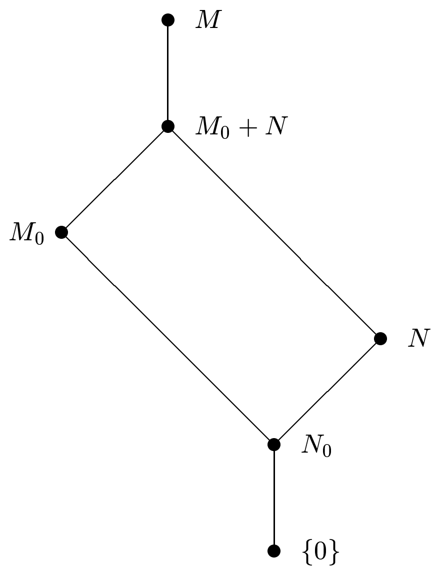
Thus M/N is a finite group (by Corollary 5.1) of exponent dividing $q+1$.

An element of M is of the form

$$\sum_{\mathfrak{p}} z_{\mathfrak{p}}\, \mathfrak{p}, \tag{5}$$

where $\mathfrak{p}$ runs through the points of $\mathcal{U}$, and the coefficients $z_{\mathfrak{p}}$ are integers. Let us call $\sum_{\mathfrak{p}} z_{\mathfrak{p}}$ the *degree* of the element (5).

Let $M_0 \le M$ be the subgroup of elements of degree 0, and put $N_0 := M_0 \cap N$. Then $(M_0+N)/N \cong M_0/N_0$. We have the following picture of subgroups.



Lemma 6.2. (a) *$M/(M_0+N)$ is cyclic of order $q+1$.*

(b) *N_0 is generated by $\{\mathfrak{m}-(q+1)\mathfrak{p}_\infty \mid \mathfrak{m}$ a line of $\mathcal{U}\}$.*

Proof. (a) We have $\mathfrak{p} = \mathfrak{p}_\infty + (\mathfrak{p}-\mathfrak{p}_\infty) \in \mathfrak{p}_\infty + (M_0+N)$ for all points of $\mathcal{U}$. Hence $M/(M_0+N)$ is cyclic. By Proposition 6.1, the order of $M/(M_0+N)$ divides $q+1$.

On the other hand, every element of N, and hence also every element of M_0+N has degree divisible by $q+1$. Thus if $s\mathfrak{p}_\infty \in M_0+N$ for some s, then s is divisible by $q+1$. It follows that $M/(M_0+N)$ has order $q+1$.

(b) Note that $\mathfrak{m}-(q+1)\mathfrak{p}_\infty \in N_0$ for every line $\mathfrak{m}$ of $\mathcal{U}$ by Proposition 6.1.

On the other hand, let $\sum_{\mathfrak{m}} z_{\mathfrak{m}}\, \mathfrak{m}$, where $\mathfrak{m}$ runs through the lines of $\mathcal{U}$, be an element of N_0. Since the degree of this element is zero, $\sum_{\mathfrak{m}} z_{\mathfrak{m}}(q+1) = 0$, and hence $\sum_{\mathfrak{m}} z_{\mathfrak{m}}\, \mathfrak{m} = \sum_{\mathfrak{m}} z_{\mathfrak{m}}\, (\mathfrak{m}-(q+1)\mathfrak{p}_\infty)$. ■

Note that the group M and its subgroups introduced above are $\mathbb{Z}G$-modules. We are going to use this structure and some representation theory of G in the proof of Geck's conjecture.

Lemma 6.3. *Let $N_1 \leq M_0$ be a G-invariant subgroup of finite index. Suppose that for any two distinct points $\mathfrak{p}$ and $\mathfrak{q}$ of $\mathcal{U}$, the element $(\mathfrak{p}-\mathfrak{q})+N_1 \in M_0/N_1$ has order $q+1$. Then $|M_0/N_1| \geq (q+1)^{q^2-q}$.*

If $|M_0/N_1| = (q+1)^{q^2-q}$, then $M_0/N_1 \cong [\mathbb{Z}/(q+1)\mathbb{Z}]^{q^2-q}$.

Proof. Since M_0 is generated by the elements $\mathfrak{p}-\mathfrak{q}$, where $\mathfrak{p}$, and $\mathfrak{q}$ are points of $\mathcal{U}$, it follows from our assumption that $q+1$ annihilates M_0/N_1.

Let ℓ be a prime dividing $q+1$ to the exact power $\ell^a > 1$. Write Z for the ℓ-part of M_0/N_1. Then Z is a $\mathbb{Z}G$-module, annihilated by ℓ^a.

Fix an integer i with $1 \leq i \leq a$ and consider the $\mathbb{F}_\ell G$-module $\ell^{i-1}Z/\ell^i Z$. We claim that for every non-trivial element $u \in U$ there is an element of $\ell^{i-1}Z/\ell^i Z$ which is not fixed by u. Indeed let m denote the ℓ'-part of $q+1$ and put $z := m(\mathfrak{p}-\mathfrak{p}_\infty)+N_1 \in Z$, where $\mathfrak{p}$ is a point of $\mathcal{U}$ different from $\mathfrak{p}_\infty$. Suppose that u fixes the image of $\ell^{i-1}z$ in $\ell^{i-1}Z/\ell^i Z$, i.e., $\ell^{i-1}z - \ell^{i-1}uz \in \ell^i Z$. Writing $\mathfrak{q} := u\mathfrak{p}$, we find $\ell^{i-1}m(\mathfrak{p}-\mathfrak{p}_\infty)+N_1 - \ell^{i-1}mu(\mathfrak{p}-\mathfrak{p}_\infty)+N_1 = \ell^{i-1}m(\mathfrak{p}-\mathfrak{q})+N_1 \in \ell^i Z$. Since ℓ^{a-i} annihilates $\ell^i Z$ by our assumption, this implies that $\ell^{a-1}m(\mathfrak{p}-\mathfrak{q}) \in N_1$. But u is non-trivial, and so $\mathfrak{p} \neq \mathfrak{q}$. By what we have shown above, the order of $(\mathfrak{p}-\mathfrak{q})+N_1$ in M_0/N_1 is smaller than $q+1$, contradicting our hypothesis.

If $q > 2$, a non-trivial $\mathbb{F}_\ell G$-module has at least dimension q^2-q (this follows from the known decomposition matrices for G, but can also be derived from the old results of Landazuri and Seitz [12]). If $q = 2$, we have $\ell = 3$ and the irreducible $\mathbb{F}_\ell G$-modules have dimensions 1 and 2. But the $\mathbb{F}_\ell G$-modules of dimension 1 have the centre of a Sylow 2-subgroup (a quaternion group of order 8) in their kernel. As we have seen above, every non-trivial element of U has a non-fixed vector on $\ell^{i-1}Z/\ell^i Z$. Thus in this case, too, the $\mathbb{F}_\ell$-dimension of $\ell^{i-1}Z/\ell^i Z$ is at least q^2-q.

By induction we find that $|Z| \geq \ell^{a(q^2-q)}$. Since ℓ was arbitrary this implies that $|M_0/N_1| \geq (q+1)^{q^2-q}$ as claimed.

If $|M_0/N_1| = (q+1)^{q^2-q}$, then $|\ell^{i-1}Z/\ell^i Z| = \ell^{q^2-q}$ for all $1 \leq i \leq a$. Hence $Z \cong [\mathbb{Z}/\ell^a\mathbb{Z}]^{q^2-q}$. Since this is true for all primes ℓ dividing $q+1$, the second assertion follows. ∎

We emphasize that Conjecture 2.1 is not needed in the proof of the above lemma. We wish to apply the lemma with $N_1 = N_0$. Since we shall only show in the next section that the assumptions of the lemma are satisfied, we introduce the following hypothesis.

Hypothesis 6.4. For any two distinct points $\mathfrak{p}$ and $\mathfrak{q}$ of $\mathcal{U}$, the element $(\mathfrak{p}-\mathfrak{q})+N_0 \in M_0/N_0$ has order $q+1$.

Lemma 6.3 together with the truth of Conjecture 2.1 now enable us to prove Geck's conjecture assuming Hypothesis 6.4.

Theorem 6.5. *If Hypothesis 6.4 is satisfied, $M/N \cong [\mathbb{Z}/(q+1)\mathbb{Z}]^{q^2-q+1}$.*

Proof. Let $d_1, d_2, \ldots, d_r$ denote those elementary divisors of the incidence matrix I, which are larger than 1, and such that d_i divides d_{i+1} for $1 \leq i < r$. Recall that $d_i \mid q+1$ for $1 \leq i \leq r$ by Proposition 6.1. Let ℓ be a prime divisor of d_1. By Corollary 5.1, the ℓ-rank of I equals $q(q^2-q+1)$, and hence $r = q^2-q+1$. Therefore, $M/N \cong \oplus_{i=1}^{q^2-q+1}\mathbb{Z}/d_i\mathbb{Z}$.

On the other hand, $|M/N| \geq (q+1)^{q^2-q+1}$ by Lemmas 6.2(a) and 6.3. It follows that all d_i must be equal to $q+1$ and thus that $M/N \cong [\mathbb{Z}/(q+1)\mathbb{Z}]^{q^2-q+1}$. ■

In the next section we show that Hypothesis 6.4 is satisfied and thus complete the last step in the proof of Conjecture 2.2.

7. The Hermitian function field

Again we keep the notation of the preceding sections. In particular, $k = \mathbb{F}_{q^2}$ is the finite field with q^2 elements.

We consider the algebraic function field (for introductions to the theory of algebraic function fields we refer to the textbooks [18] and [19])

$$K = k(u, v), \qquad u^{q+1} + v^q + v = 0. \tag{6}$$

This means that $u \in K$ is transcendental over k and that K is an algebraic extension $K = k(u)[v]$ of the rational function field $k(u)$ by the element v with minimal polynomial $X^q + X + u^{q+1} \in k(u)[X]$ over $k(u)$.

The field K is called the *Hermitian function field* over k. A detailed investigation of K can be found in the book by Stichtenoth ([19, Example VI.4.3]; note that our v is called y there, whereas our u equals ξx with $\xi \in k$ such that $\xi^{q+1} = -1$). Stichtenoth also gives the transformation which shows that there are $a, b \in K$, transcendental over k, such that $K = k(a, b)$ with $a^{a+1} + b^{q+1} + 1 = 0$. This is the affine version of the Fermat equation, so that K is the algebraic function field of the Fermat curve $\mathcal{F}$ of the introduction. For this reason K is also called the *Fermat function field* in the literature.

Let $\mathrm{Aut}(K/k)$ denote the automorphism group of K over k. Leopoldt has shown in [13] that $\mathrm{Aut}(K/k) \cong \mathrm{PGU}_3(q) = G$, and that the resulting action of G on u and v can be described as follows. An element of the form (3) yields the automorphism

$$u \mapsto u + \alpha, \qquad v \mapsto -\bar{\alpha}u + v + \beta \tag{7}$$

and an element of the form (4) acts as

$$u \mapsto \zeta u, \qquad v \mapsto \zeta\bar{\zeta}v \tag{8}$$

Now G is generated by B and the image of w_0 (see (2)) in G, which induces the k-automorphism

$$u \mapsto \frac{u}{v}, \qquad v \mapsto \frac{1}{v}$$

on K. We thus have completely described the action of G on K.

Let $\mathbb{D}$ denote the group of divisors of the field extension K/k. By definition, $\mathbb{D}$ is the free abelian group, written additively, on the set of places of K/k. A place of K/k is the maximal ideal of a valuation ring of K/k. Places, viewed as elements of $\mathbb{D}$, are also called prime divisors in the following. We refer the reader to [19, Chapter I] for the fundamental notions of places and divisors of an algebraic function field.

The set of divisors of degree 0 is denoted by $\mathbb{D}_0$ (for the definition of the degree of a divisor see [19, Definition I.4.1]). Let $\mathcal{H}$ denote the group of principal divisors of K/k, the image of the homomorphism $K^\times \to \mathbb{D}$ sending a function z to its divisor (z) (the reason for calling the elements of K *functions* is motivated in [19, Remark I.1.16]; the divisor of a function is defined in [19, Definition I.4.2]).

We summarize some facts about K on this and the next page. A reference for these results is [19, Lemma VI.4.4].

The genus of K equals $q(q-1)/2$. Also, K has exactly q^3+1 prime divisors of degree 1. (This set coincides with the set of Weierstraß points of K (cf. [13, Satz 3]).)

The prime divisors of degree 1 can be described as follows. There is a unique place $\mathfrak{p}_\infty$ lying above the infinite place of the rational function field $k(u)$. Moreover, $\mathfrak{p}_\infty$ has degree 1, and the pole divisors of u and v are $q\mathfrak{p}_\infty$ and $(q+1)\mathfrak{p}_\infty$, respectively. (For the notion of zero and pole divisor see [19, Definition I.4.2].) For every pair (α, β) of elements of k with $(\alpha,\beta) \neq (0,0)$ and $\alpha\bar{\alpha} + \bar{\beta} + \beta = 0$, there is a unique place $\mathfrak{p}_{\alpha,\beta}$ of degree 1 with $u(\mathfrak{p}_{\alpha,\beta}) = \alpha$ and $v(\mathfrak{p}_{\alpha,\beta}) = \beta$. (If $\mathfrak{p}$ is a place of K/k, the function $z \mapsto z(\mathfrak{p})$ for $z \in K$ is the *residue class map*; see [19, Definiton I.1.13].) Thus the q^3+1 prime divisors of K/k of degree 1 are in one-to-one correspondence with the points of the unital $\mathcal{U}$ via the map

$$\mathfrak{p}_\infty \mapsto \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \qquad \mathfrak{p} \mapsto \begin{bmatrix} 1 \\ u(\mathfrak{p}) \\ v(\mathfrak{p}) \end{bmatrix}, \qquad \mathfrak{p} \neq \mathfrak{p}_\infty.$$

This map is compatible with the action of G on the points of $\mathcal{U}$ and on the set of prime divisors of degree 1 of K/k. In the following we identify the latter set with the set of points of $\mathcal{U}$.

The zero divisor of u is clearly equal to

$$\sum_{\beta+\bar{\beta}=0} \mathfrak{p}_{0,\beta}$$

(the places $\mathfrak{p}_{0,\beta}$ appearing in the above sum are zeroes of u, i.e., $u(\mathfrak{p}_{0,\beta}) = 0$, they all have degree 1, and their number is q, the degree of the pole divisor $q\mathfrak{p}_\infty$ of u), whereas the zero divisor of v equals $(q+1)\mathfrak{p}_{0,0}$, so that $(v) = (q+1)\mathfrak{p}_{0,0} - (q+1)\mathfrak{p}_\infty$.

In accordance with our definition at the end of Section 3, we put

$$\mathfrak{n} := \mathfrak{p}_\infty + \sum_{\beta+\bar{\beta}=0} \mathfrak{p}_{0,\beta}.$$

Thus $\mathfrak{n}$ corresponds to the line of $\mathcal{U}$ joining $\mathfrak{p}_\infty$ with $\mathfrak{p}_{0,0}$, and $(u) = \mathfrak{n} - (q+1)\mathfrak{p}_\infty$.

The linear space $L(m\mathfrak{p}_\infty)$ (for the definiton of this space see [19, Definition I.4.4]) has basis

$$\{u^i v^j \mid 0 \leq i, 0 \leq j \leq q-1, qi + (q+1)j \leq m\}. \tag{9}$$

We now describe the set of principal divisors arising from the non-constant functions in $L((q+1)\mathfrak{p}_\infty)$. By (9), the linear space $L(q\mathfrak{p}_\infty)$ has dimension 2 over k, $\{1, u\}$ being a k-basis. The functions

$$u + \alpha, \qquad \alpha \in k,$$

(which can also be described as the images of the function u under the subgroup U of G, cf. (7)) give rise to the q^2 divisors

$$\mathfrak{m} - (q+1)\mathfrak{p}_\infty, \tag{10}$$

where $\mathfrak{m}$ is a line of $\mathcal{U}$ through $\mathfrak{p}_\infty$.

Next, $L((q+1)\mathfrak{p}_\infty)$ is a 3-dimensional vector space over k with basis $\{1, u, v\}$, again by (9). Since U is transitive on $\mathcal{U} \setminus \{\mathfrak{p}_\infty\}$, the q^3 images of v under U, which are of the form

$$-\bar{\alpha}u + v + \beta, \quad \alpha, \beta \in k, \quad \alpha\bar{\alpha} + \bar{\beta} + \beta = 0,$$

have the divisors

$$(q+1)\mathfrak{p} - (q+1)\mathfrak{p}_\infty, \qquad \mathfrak{p} \neq \mathfrak{p}_\infty.$$

We finally have $q^3(q-1)$ divisors

$$\mathfrak{m} - (q+1)\mathfrak{p}_\infty, \tag{11}$$

where $\mathfrak{m}$ is a line of $\mathcal{U}$ not passing through $\mathfrak{p}_\infty$. These arise as follows. If $\mathfrak{m}$ is any line, then $\mathfrak{m}$ is conjugate to $\mathfrak{n}$ by some element of G. If we apply this element to u, we obtain a function z with divisor $\mathfrak{m} - (q+1)\mathfrak{p}$, with some $\mathfrak{p} \in \mathcal{U}$. Now a suitable conjugate v' of v has divisor $(q+1)\mathfrak{p} - (q+1)\mathfrak{p}_\infty$ and so $(z/v') = \mathfrak{m} - (q+1)\mathfrak{p}_\infty$. By (9), the following functions give rise to the divisors described in (11):

$$\alpha u + v + \beta, \quad \alpha, \beta \in k, \quad \alpha\bar{\alpha} + \bar{\beta} + \beta \neq 0.$$

We now have accounted for all divisors arising from the functions in $L((q+1)\mathfrak{p}_\infty)$.

Let

$$M := \langle \mathfrak{p}_\infty, \mathfrak{p}_{\alpha,\beta} \mid \alpha\bar{\alpha} + \bar{\beta} + \beta = 0, \alpha, \beta \in k \rangle \leq \mathbb{D}.$$

Thus M is the set of divisors of K whose support is contained in the set of prime divisors of degree 1 of K/k. Furthermore, let

$$N := \langle \mathfrak{m} \mid \mathfrak{m} \text{ is conjugate in } G \text{ to } \mathfrak{n} \rangle.$$

Then M/N is isomorphic to the group with the same name introduced in Section 6. In particular, M/N is a finite group whose exponent divides $q+1$ by the remark following Proposition 6.1.

Put $M_0 := M \cap \mathbb{D}_0$ and put $N_0 := N \cap \mathbb{D}_0$. We have

$$N \cap M_0 = N \cap \mathbb{D}_0 \cap M = N_0 \cap M = N_0,$$

from which we conclude that M_0 and N_0 have the same meaning as in Section 6.

Lemma 7.1. (a) $N_0 \leq \mathcal{H} \cap M$.

(b) *For any two distinct prime divisors* $\mathfrak{p}$ *and* $\mathfrak{q}$ *of degree* 1, *the element* $(\mathfrak{p} - \mathfrak{q}) + (\mathcal{H} \cap M) \in M_0/(\mathcal{H} \cap M)$ *has order* $q+1$. *In particular, Hypothesis 6.4 is satisfied.*

Proof. (a) By Lemma 6.2(b), the elements $\mathfrak{m} - (q+1)\mathfrak{p}_\infty$, where $\mathfrak{m}$ runs through the lines of $\mathcal{U}$, generate N_0. By (10) and (11) these generating elements are divisors of functions, proving our claim.

(b) Since G acts doubly transitively on the set of prime divisors of degree 1 and since M_0 and $\mathcal{H} \cap M$ are $\mathbb{Z}G$-modules, it suffices to assume that $\mathfrak{q} = \mathfrak{p}_\infty$. Let m be the order of $(\mathfrak{p} - \mathfrak{p}_\infty) + (\mathcal{H} \cap M) \in M_0/(\mathcal{H} \cap M)$. Since $(q+1)(\mathfrak{p} - \mathfrak{p}_\infty) \in N_0 \leq \mathcal{H} \cap M$ by Proposition 6.1 and Part(a), it follows that m divides $q+1$.

Now $m\mathfrak{p} - m\mathfrak{p}_\infty \in \mathcal{H} \cap M \leq \mathcal{H}$, and thus there is a non-constant function in $L(m\mathfrak{p}_\infty)$. Suppose that $m < q+1$. Then $m < q$. In this case $L(m\mathfrak{p}_\infty)$ contains only constant functions by (9). This contradiction proves our first claim. The second one follows from the first together with Part (a) and Proposition 6.1. ■

We can now prove Geck's conjecture.

Corollary 7.2. *Geck's conjecture* 2.2 *has a positive answer.*

Proof. This follows from Theorem 6.5 together with Lemma 7.1(b). ∎

Let $\mathcal{D}_K^0 := \mathbb{D}_0/\mathcal{H}$ denote the group of divisor classes of degree 0 of K. The next theorem describes the structure of $\mathcal{D}_K^0$.

Theorem 7.3. *The canonical map $M_0 \to \mathcal{D}_K^0$ is surjective and $\mathcal{D}_K^0$ is isomorphic to $[\mathbb{Z}/(q+1)\mathbb{Z}]^{q^2-q}$.*

Proof. The kernel of the map equals $\mathcal{H} \cap M_0 = \mathcal{H} \cap M$. By Lemmas 7.1(b) and 6.3 we have $|M_0/(\mathcal{H} \cap M)| \geq (q+1)^{q^2-q}$.

The order of $\mathcal{D}_K^0$ is finite (see [18, Lemma 5.6]) and equals $L_K(1)$ (see [18, Theorem 5.9]), where L_K denotes the L-polynomial of K. By [19, Example VI.3.5], we have $L_K(t) = (1+qt)^{q^2-q}$, and thus $|\mathcal{D}_K^0| = (q+1)^{q^2-q}$. It follows that the above map is surjective and that $\mathcal{D}_K^0 \cong M_0/(\mathcal{H} \cap M)$. The isomorphism type of $M_0/(\mathcal{H} \cap M)$ can be derived from the second assertion of Lemma 6.3. ∎

As a corollary of the above results we obtain an interpretation of M_0/N_0 as $\mathcal{D}_K^0$.

Corollary 7.4. *We have $N_0 = \mathcal{H} \cap M$. In particular, $M_0/N_0 \cong \mathcal{D}_K^0$.*

Proof. By Lemma 7.1(a) we have $N_0 \leq \mathcal{H} \cap M$. By Corollary 7.2 and Theorem 7.3, we have $|M_0/N_0| = |M_0/(\mathcal{H} \cap M)|$ implying our claim. ∎

Corollary 7.5. *$\mathcal{H} \cap M$ is generated by the divisors $g\mathfrak{n} - (q+1)\mathfrak{p}_\infty$, $g \in G$, in other words by the divisors of* (10) *and* (11). *In particular, every non-zero function in K which has zeroes and poles only in the k-rational places (i.e., the Weierstraß points) of K, is a product of the functions*

$$\alpha u + \beta v + \gamma, \qquad \alpha, \beta, \gamma \in k, \qquad (\alpha, \beta, \gamma) \neq (0,0,0)$$

and their inverses.

Proof. We have $N_0 = \mathcal{H} \cap M$ by Corollary 7.4. The functions $u + \alpha$, $\alpha \in k$, and $\alpha u + v + \beta$, $\alpha, \beta \in k$ give rise to the divisors of (10) and (11) generating N_0 by Lemma 6.2(b). ∎

Note that Corollary 7.5 and Lemma 6.2(b) imply $N_0 = \mathcal{H} \cap M$. This in turn implies $M_0/N_0 \cong [\mathbb{Z}/(q+1)\mathbb{Z}]^{q^2-q}$ by Theorem 7.3. The latter, together with Lemma 6.2(a) (or rafter its proof) implies the truth of Geck's and hence also of Andriamanalimanana's conjecture. From this one can derive the structure of the permutation module for ℓ dividing $q+1$. Finally, this information yields the decomposition numbers of G in this case.

Hence if one could prove Corollary 7.5 without using the representation theory of G, one could complete the ℓ-decomposition matrix of G.

Appendix

In this appendix we sketch a proof of Theorem 4.1 in case F has characteristic 2. Moreover, Geck's argument of [7] showing that ${F_B}^G$ is uniserial does not apply if F has characteristic 3 and the 3-part of $q+1$ is exactly 3. In this case we replace Geck's argument by a reference to [11]. The details are given at the end of this appendix. For the convenience of the reader we also give the ordinary character tables of $B = UT$ and $B_0 = Z(U)T$.

The character tables of B and B_0. The following table introduces names and representatives for the conjugacy classes of these groups and gives the corresponding centralizer orders.

Class Parameters	Representative	Centralizer order in B	Centralizer order in $Z(U)T$
B_1	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$q^3(q^2-1)$	$q(q^2-1)$
B_2	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \beta & 0 & 1 \end{pmatrix}$	$q^3(q+1)$	$q(q+1)$
B_3	$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \gamma & -1 & 1 \end{pmatrix}$	q^2	—
$B_4^{(k)}$ $1 \leq k \leq q$	$\begin{pmatrix} \rho^{-k} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \bar{\rho}^k \end{pmatrix}$	$q(q^2-1)$	$q(q^2-1)$
$B_5^{(k)}$ $1 \leq k \leq q$	$\begin{pmatrix} \rho^{-k} & 0 & 0 \\ 0 & 1 & 0 \\ \beta & 0 & \bar{\rho}^k \end{pmatrix}$	$q(q+1)$	$q(q+1)$
$B_6^{(k)}$ $0 \leq k \leq q^2-1$ $k \nmid q-1$	$\begin{pmatrix} \zeta^{-k} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \bar{\zeta}^k \end{pmatrix}$	q^2-1	q^2-1

The conjugacy classes for B and B_0 are parametrized in the same way except that B_0 does not contain elements of the class B_3. Here, β and γ are elements of $k = \mathbb{F}_{q^2}$ with $\beta + \bar{\beta} = 0$ and $\gamma + \bar{\gamma} + 1 = 0$, respectively. Moreover, ζ is a primitive element of $k^\times$ and $\rho := \zeta^{q-1}$.

We now give the character table of B_0.

	B_1	B_2	$B_4^{(k)}$	$B_5^{(k)}$	$B_6^{(k)}$
$\tau_1^{(i)}$ $0 \leq i \leq q^2-2$	1	1	ε^{ik}	ε^{ik}	δ^{ik}
$\tau_{q-1}^{(i)}$ $0 \leq i \leq q$	$q-1$	-1	$(q-1)\varepsilon^{ik}$	$-\varepsilon^{ik}$	0

Finally, we give the character table of B (see also [8, Table 2.1]).

	B_1	B_2	B_3	$B_4^{(k)}$	$B_5^{(k)}$	$B_6^{(k)}$
$\vartheta_1^{(i)}$ $0 \leq i \leq q^2-2$	1	1	1	ε^{ik}	ε^{ik}	δ^{ik}
$\vartheta_{q(q-1)}^{(i)}$ $0 \leq i \leq q$	$q(q-1)$	$-q$	0	$(1-q)\varepsilon^{ik}$	ε^{ik}	0
ϑ_{q^2-1}	q^2-1	q^2-1	-1	0	0	0

In these tables, δ denotes a complex primitive (q^2-1)st root of unity, and $\varepsilon := \delta^{q-1}$.

Proof of Theorem 4.1 for characteristic 2. Suppose then that q is odd and let F denote an algebraically closed field of characteristic 2. Let T_0 denote the unique subgroup of T of order $q+1$ and let D and D_0 be the Sylow 2-subgroup of T and T_0 respectively. Let $|D_0| = 2^a$ and $|D| = 2^b$.

The group B has q^2-1 linear complex characters $\vartheta_1^{(i)}$, an irreducible character ϑ_{q^2-1} of degree q^2-1, and $q+1$ irreducible complex characters $\vartheta_{q(q-1)}^{(i)}$ of degree $q(q-1)$ (see the character table given above). The characters of a fixed degree form a union of 2-blocks. The characters of degree $q(q-1)$ lie in 2-blocks with defect group D_0. Every 2-block contains a unique irreducible FB-module.

Let Y_1 be the irreducible FB-module of the block containing $\vartheta_{q(q-1)}^{(0)}$. More generally, for $1 \leq i \leq 2^a$, let Y_i denote the uniserial FB-module with i copies of Y_1 as composition factors. The following proposition is the analogue of [15, Propostion 1.2].

Proposition. *The following statements hold.*

(a) $\left(F_B{}^G\right)_B \cong F_B \oplus F_T{}^B$.

(b) $F_T{}^B = F_B \oplus Y_{2^a-1} \oplus Y''$, *where* Y'' *does not have any composition factor isomorphic to* Y_1 *or* F_B.

(c) $\dim_F \mathrm{Hom}_{FT}(F_T, Y_i) = i$ *for* $1 \leq i \leq 2^a - 1$.

Proof. Part (a) is just Mackey's theorem and the fact that $G = B \cup Bw_0B$.

To prove (b), observe that $C_B(D_0) = N_B(D_0) = B_0$. We first consider $F_T{}^{B_0}$. Since T_0 acts trivially on this module, it follows that $F_T{}^{B_0} \cong F_{B_0} \oplus S$ with an irreducible FB_0-module S of degree $q-1$. The character of $F_{B_0}{}^B$ is the sum of the trivial character of B with the character of degree q^2-1. The module S has vertex D_0 and trivial source. Observe that D_0 is a trivial intersection subgroup of B and hence, by Green correspondence, S^B has a unique indecomposable direct summand Y with a trivial source and vertex D_0, and the other direct summands are projective. Trivial source modules are uniquely determined by the ordinary characters of their lifts. The character of the lift of S equals $\tau_{q-1}^{(0)}$ which gives $\sum_{i=1}^{q} \vartheta_{q(q-1)}^{(i)}$ when induced to B. This implies in particular that the Green correspondent Y of S lies in the block containing Y_1.

We aim to show that $Y = \Omega(Y_1) = Y_{2^a-1}$. Since Green correspondence commutes with the Heller operator (see [1, Proposition 20.7, p. 148]), it suffices to show that the Green correspondent of Y_1 in B_0 is equal to ΩS. By the theory of blocks with cyclic defect groups, the Green correspondent of Y_1 is uniserial of length 1 or $2^a - 1$

(see [6, Theorem VII.2.7]). Hence the Green correspondent of Y_1 equals S or $\Omega(S)$. But the character value of $\vartheta^{(0)}_{q(q-1)}$ on a generator of D_0 equals $1-q<0$, and so Y_1 does not have a trivial source. It follows that $Y=\Omega(Y_1)=Y_{2^a-1}$. This proves (b).

To prove (c), observe that there is an $F[UT_0]$-module Z_1 of degree q such that ${Z_1}^B = Y_1$. The blocks of UT_0 and $UT = B$ containing Z_1 and Y_1, respectively, are Morita equivalent (by Clifford theory). For $1 \le i \le 2^a$, we let Z_i denote the uniserial $F[UT_0]$-module with i composition factors Z_1. We also let X_i denote the uniserial FT_0-module with i trivial composition factors, also viewed as as an $F[UT_0]$-module via inflation. Then $Z_i \cong Z_1 \otimes_F X_i$ and $(Z_i)^B \cong Y_i$.

By Mackey's theorem we have $(Y_i)_T \cong \left((Z_i)^B\right)_T \cong \left((Z_i)_{T_0}\right)^T$. Moreover, $(Z_i)_{T_0} \cong (Z_1)_{T_0} \otimes_F X_i$. Now Z_1 is an indecomposable UT_0 module with vertex D_0 and co-trivial source (i.e., $\Omega(Z_1)$ has trivial source). Green correspondence (between UT_0 and $Z(U)T_0$) implies that $(Z_1)_{Z(U)T_0}$ has a unique non-trivial direct summand with vertex D_0 and co-trivial source. The other direct summands are projective and do not lie in the principal block. It follows that $(Z_1)_{T_0} = \Omega(F_{T_0}) \oplus W$, where W is a projective FT_0-module without trivial composition factors.

Using the self-duality of X_i, we find

$$\begin{aligned}
\dim_F \mathrm{Hom}_{FT}(F_T, Y_i) &= \dim_F \mathrm{Hom}_{FT}(F_T, ((Z_1)_{T_0} \otimes_F X_i)^T) \\
&= \dim_F \mathrm{Hom}_{FT_0}(F_{T_0}, (Z_1)_{T_0} \otimes_F X_i) \\
&= \dim_F \mathrm{Hom}_{FT_0}(X_i, (Z_1)_{T_0}) \\
&= \dim_F \mathrm{Hom}_{FT_0}(X_i, X_{2^a-1}) + \dim_F \mathrm{Hom}_{FT_0}(X_i, W) \\
&= \dim_F \mathrm{Hom}_{FT_0}(X_i, X_{2^a-1}) = i.
\end{aligned}$$

This concludes the proof of Part (c) and hence of the proposition. ■

To finish the proof we need some information on the possible modular constituents of ${F_B}^G$. Writing 1_G for the Brauer character of the trivial FG-representation, the Brauer character of ${F_B}^G$ equals $1_G + \alpha\varphi + \vartheta$, with $\alpha \ge 1$, and $\alpha \ge 2$ if $4 \mid q+1$. This is proved exactly as for odd characteristics (see [8, Theorem 4.2(a)]). Namely, the three ordinary unipotent characters χ_1 (the trivial character), $\chi_{q(q-1)}$ (the lift of φ), and χ_{q^3} (the Steinberg character), form a basic set of ordinary characters for the principal 2-block of G (see [9, Theorem 5.1]). Thus it suffices to determine the decomposition numbers for these three characters. It is easy to see that an approximation to the decomposition matrix is given by

χ_1	1	0	0
$\chi_{q(q-1)}$	0	1	0
χ_{q^3}	1	α	1

for some non-negative integer α. Furthermore, the principal 2-block contains an ordinary irreducible character of degree $q(q^2-q+1)$ which has the same restriction as $\chi_{q^3} - \chi_{q(q-1)}$ to the 2-regular elements of G. Thus $\alpha \ge 1$. If $4 \mid q+1$, the principal 2-block contains an ordinary irreducible character of degree $(q-1)(q^2-q+1)$ which restricts in the same way $\chi_{q^3} - 2\chi_{q(q-1)} + \chi_1$ to the 2-regular elements. Thus in this case we even have $\alpha \ge 2$.

We can now give an alternative proof for the decomposition numbers in case $4 \mid q-1$ as follows. Here, $a=1$ and $\vartheta^{(0)}_{q(q-1)} + \vartheta^{((q^2-1)/2)}_{q(q-1)}$ is a projective character of B. By Part (b) of the above proposition, the restriction of χ_{q^3} to B contains only one constituent of the 2-block containing $\vartheta^{(0)}_{q(q-1)}$. Since $\chi_{q(q-1)}$ restricts to $\vartheta^{(0)}_{q(q-1)}$, this implies that inducing $\vartheta^{(0)}_{q(q-1)} + \vartheta^{((q^2-1)/2)}_{q(q-1)}$ to G yields a projective character containing each of $\chi_{q(q-1)}$ and χ_{q^3} exactly once. Thus $\alpha = 1$ in this case.

Suppose then that $4 \mid q+1$. Since ${F_B}^G$ is a trivial source module with a two-dimensional endomorphism ring, it is indecomposable with a unique maximal submodule. The module V considered in the proof of Corollary 5.1 does not have φ as a top composition factor, and thus $V_B \cong Y_i \oplus Y''$ for some $0 \leq i \leq 2^a - 1$. From [15, Proposition 1.4] we obtain $i \geq 2^a - 2$, just as in the proof of [15, Lemma 2.2]. Since $2^a - 2 \geq 2$, this also implies that V is uniserial.

Completion of the proof of Theorem 4.1 for characteristic 3. We finally sketch a proof of Theorem 4.1 in case that the characteristic of F equals 3, and that the 3-part of $q+1$ is exactly 3. In this case the restriction of ϑ to B does not contain any composition factor of the block containing $\vartheta^{(0)}_{q(q-1)}$, and we cannot conclude, as Geck did in [7], that ${F_B}^G$ is uniserial. We can, however, use a result of Koshitani and Kunugi [11] in this case. Let $\bar{G} := \mathrm{PSU}_3(q)$, considered as a normal subgroup of G of index 3. Then $\left({F_B}^G\right)_{\bar{G}} \cong {F_{\bar{B}}}^{\bar{G}}$, where $\bar{B} := \bar{G} \cap B$. By [11, Lemma (4.3)], the latter module is the projective cover of the trivial $F\bar{G}$-module. By the main theorem of the cited paper, the principal $F\bar{G}$-block is Morita equivalent to the principal block of $F[\mathrm{PSU}_3(2)]$. The socle series of the projective cover of the trivial module of the latter group is of length 5 (see [11, Lemma (4.2)(ii)]). Since ${F_B}^G$ has exactly 5 composition factors, it must be uniserial.

Acknowledgement

It is a pleasure to thank B. H. Matzat for numerous discussions, which lead to significant contributions to this work. First of all, Matzat explained all the relevant facts about algebraic function fields to me. Secondly, Proposition 6.1, an important intermediate step in the proof of the main results, is due to him.

I also thank the referee whose helpful comments lead to a rearrangement of some of the material of this paper and so improved its readability.

References

[1] J. L. Alperin, Local representation theory, Cambridge University Press, Cambridge, 1986.

[2] B. R. Andriamanalimanana, Ovals, unitals and codes, PhD-thesis, Lehigh University, 1979.

[3] E. F. Assmus Jr. and J. D. Key, Designs and their codes, Cambridge University Press, Cambridge, 1992.

[4] A. E. Brouwer, H. A. Wilbrink, and W. H. Haemers, Some 2-ranks, *Discrete Math.* **106/107** (1992), 83–92.

[5] K. Erdmann, On 2-blocks with semidihedral defect groups, *Trans. Amer. Math. Soc.* **256** (1979), 267–287.

[6] W. Feit, The representation theory of finite groups, North-Holland Publishing Company, New York, 1982.

[7] M. Geck, Eine Anwendung von MAPLE in der Darstellungstheorie der unitären Gruppen, Diplomarbeit, RWTH Aachen, 1987.

[8] M. Geck, Irreducible Brauer characters of the 3-dimensional special unitary groups in non-defining characteristic, *Comm. Algebra*, **18** (1990), 563–584.

[9] M. Geck and G. Hiss, Basic sets of Brauer characters for finite groups of Lie type, *J. Reine Angew. Math.* **418** (1991), 173–188.

[10] J. D. Key, Some applications of Magma in designs and codes: oval designs, Hermitian unitals and generalized Reed-Muller codes, *J. Symbolic Comput.* **31** (2001), 37–53.

[11] S. Koshitani and N. Kunugi, The principal 3-blocks of the 3-dimensional projective special unitary groups in non-defining characteristic, *J. Reine Angew. Math.* **539** (2001), 1–27.
[12] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.
[13] H.-W. Leopoldt, Über die Automorphismengruppe des Fermatkörpers, *J. Number Theory* **56** (1996), 256–282.
[14] B. Mortimer, The modular permutation representations of the known doubly transitive groups, *Proc. London Math. Soc. (3)* **41** (1980), 1–20.
[15] T. Okuyama and K. Waki, Decomposition numbers of $\mathrm{SU}(3, q^2)$, *J. Algebra* **255** (2002), 258–270.
[16] M. E. O'Nan, Automorphisms of unitary block designs, *J. Algebra* **20** (1972), 495–511.
[17] D. E. Rohrlich, Points at infinity on the Fermat curves, *Invent. Math.* **39** (1977), 95–127.
[18] M. Rosen, Number theory in function fields, Springer, 2002.
[19] H. Stichtenoth, Algebraic function fields and codes, Springer, 1993.

Lehrstuhl D für Mathematik, RWTH Aachen, 52056 Aachen, Germany
E-mail address: Gerhard.Hiss@Math.RWTH-Aachen.DE