ACTA ARITHMETICA
124.4 (2006)

The Galois relation $x_1 = x_2 + x_3$ and Fermat over finite fields

by

Kurt Girstmair (Innsbruck)

1. Introduction and results. Let K be a field of characteristic 0 and $f = Z^n + c_1 Z^{n-1} + \cdots + c_n \in K[Z]$ an irreducible polynomial of degree n over K. By $x_1, \ldots, x_n$ we denote the zeros of f in some algebraic closure of K, and by G the Galois group of f; so $G = \mathrm{Gal}(L/K)$, where $L = K(x_1, \ldots, x_n)$ is the splitting field of f. The group G acts as a transitive permutation group on $x_1, \ldots, x_n$. This action is completely described by the pair (G, H), where H is the stabilizer $G_{x_1} = \{s \in G : s(x_1) = x_1\}$. But this pair yields more: it also determines the set of possible linear relations

$$a_1 x_1 + \cdots + a_n x_n = 0, \quad a_1, \ldots, a_n \in K, \tag{1}$$

between the zeros of f (see [3]). The said paper develops a framework for a basic understanding of this set. In quite a number of cases this framework allows an explicit description of all possible relations (1) (see also [11]).

It seems more difficult, however, to walk in the converse direction. By this we mean that a relation like

$$x_1 = x_2 + x_3 \tag{2}$$

is given, and that we classify the pairs (G, H) for which (2) is possible. Starting with J. Browkin, a number of people have been interested in this particular relation (see [2], [10]). One of the few satisfactory answers about (2) concerns the *abelian* case. So G is an abelian group, and, since G acts faithfully on $x_1, \ldots, x_n$, the stabilizer H is the trivial subgroup 1 of G. In this situation, the relation (2) is possible if, and only if, the group order $|G|$ is divisible by 6 (see [3]; basically, this was shown in [2] already).

In the present paper we consider, more generally, *regular* permutation groups, i.e., arbitrary groups G but trivial stabilizers $H = 1$. This situation occurs just if f is a *normal* polynomial, i.e., $L = K(x_1)$. We need some additional terminology in order to be able to enounce our results: For the time being, let G be an arbitrary finite group (so it need not be the Galois

2000 *Mathematics Subject Classification*: 12F10, 12E05.

group of a polynomial f). We consider the *group ring*

$$K[G] = \Big\{ \sum_{s \in G} a_s s : a_s \in K \Big\}$$

of G over K. An element $\alpha \in K[G]$ is called *admissible* if there is an element $\tau \in K[G]$ such that $\alpha\tau = 0$ but $G_\tau = \{s \in G : s\tau = \tau\}$ equals 1 (see [3, Section 1]). Admissible elements of the group ring form the right concept for our purpose: Each admissible element represents a linear relation (1) that may actually occur if G is the Galois group of f and $G_{x_1} = 1$; and, conversely, each actually occurring relation is obtained in this way. This assertion has been proved in [3] in a more general context. In order to keep this paper reasonably self-contained, we shall give a short proof at the beginning of Section 2. For the moment, however, we ask the reader to believe this assertion.

In the terminology of the group ring $K[G]$, the relation (2) is represented by an element of the shape

$$\alpha = 1 - s - t, \qquad s, t \in G \setminus \{1\},\ s \neq t. \tag{3}$$

The following "inclusion lemma" will show that an element α of this shape is admissible in many cases.

PROPOSITION 1. *Let G be a finite group, $G' \neq 1$ a subgroup of G and α an admissible element of the group ring $K[G']$. Then α is also an admissible element of the group ring $K[G]$.*

By the aforementioned result on abelian groups, the group ring $K[G']$ of the cyclic group $G' = C_6$ of order 6 contains an admissible element (3). In [3, Example 9], the same was shown for $G' = S_3$, the symmetric group of three elements, and in [10, Section 2], for $G' = A_4$, the alternating group of four elements. Accordingly, Proposition 1 yields

COROLLARY. *Let G be a finite group that contains a subgroup isomorphic to C_6, S_3, or A_4. Then $K[G]$ contains an admissible element of the shape* (3).

The corollary says that there is a good chance that the relation (2) is possible for a normal polynomial f as soon as the order of its Galois group is divisible by 6 (as was asked in [10]). What about groups G of order not divisible by 6? Proposition 1 suggests looking for small subgroups G' such that $K[G']$ contains an admissible element (3). Since $6 \nmid |G'|$, such a group G' cannot be abelian, so a group G' that normalizes a cyclic subgroup C_p of G, p a prime ≥ 5, would be a natural candidate. In many cases this candidate is a solvable group of prime degree, i.e., a subgroup of the affine group $\mathrm{AGL}(1,p)$ of the field $\mathbb{F}_p$ of p elements. An example of A. Dubickas (privately communicated in 2001) shows that $K[G']$ contains an admissible element of the shape (3) if G' is the group $\mathrm{AGL}(1,p)$ itself, and, more generally, if $G' = \mathrm{AGL}(1,q)$, $q = p^e$ (a detailed discussion of this example can be found

at the end of Section 2). Hence it is reasonable to study transitive subgroups of $\mathrm{AGL}(1,q)$. Our main result (Theorem 1) gives an exhaustive answer for these groups.

In what follows, q may be an arbitrary prime power (in particular, we include cases like $q = 2, 3$). The elements of $\mathrm{AGL}(1,q)$ are represented as

$$aX + b, \qquad a \in \mathbb{F}_q^\times,\ b \in \mathbb{F}_q,$$

where $aX + b$ stands for the (affine) mapping $\mathbb{F}_q \to \mathbb{F}_q : x \mapsto ax + b$. A transitive subgroup G of $\mathrm{AGL}(1,q)$ is always a semidirect product $G = HF$. The normal subgroup $F = \{X + b : b \in \mathbb{F}_q\}$ is the group of all translations of $\mathbb{F}_q$, and H is the stabilizer $\{s \in G : s(0) = 0\}$ of $0 \in \mathbb{F}_q$. We consider H as a subgroup of $\mathbb{F}_q^\times$: since each $s \in H$ has the form $s = aX$, $a \in \mathbb{F}_q^\times$, we may identify $aX \in H$ with $a \in \mathbb{F}_q^\times$.

THEOREM 1. *Let $G = HF$ be a transitive subgroup of $\mathrm{AGL}(1,q)$ with $H \subseteq \mathbb{F}_q^\times$ as above. Then $K[G]$ contains an admissible element of the shape (3) if, and only if, there are elements $a, b \in H$ such that $a + b = 1$.*

From Theorem 1 the connection between $x_1 = x_2 + x_3$ and the *Fermat equation* over $\mathbb{F}_q$ is obvious: Let m denote the *index* of H in $\mathbb{F}_q^\times$, so $H = \{x^m : x \in \mathbb{F}_q^\times\}$. Then there are $a, b \in H$ with $a + b = 1$ if, and only if,

$$x^m = y^m + z^m$$

holds for some $x, y, z \in \mathbb{F}_q$ with $xyz \neq 0$.

We briefly highlight some *special cases* of Theorem 1: If $G = \mathrm{AGL}(1,q)$, then $H = \mathbb{F}_q^\times$. As soon as $q > 2$, there are always elements $a, b \in \mathbb{F}_q^\times$ such that $a + b = 1$, so $K[G]$ contains admissible elements (3) (which we mentioned already). As the groups $\mathrm{AGL}(1,3)$ and $\mathrm{AGL}(1,4)$ are isomorphic to S_3 and A_4, respectively, Theorem 1 covers these special cases considered above. For an odd prime p and $G = \mathrm{ASL}(1,p)$ (the subgroup of index 2 of $\mathrm{AGL}(1,p)$), we have $H = \{x^2 : x \in \mathbb{F}_p^\times\}$. It is easy to check that $a + b = 1$ has a solution in H if, and only if, this holds for $a - b = 1$, or, in other words, if there are at least two consecutive *quadratic residues* mod p. This is known to be true for $p \geq 7$ (see, for instance, [4, p. 174 f.]) but false for $p = 3, 5$. Accordingly, the group rings of C_3 and $\mathrm{ASL}(1,5) = D_5$ (the dihedral group of order 10) do not contain admissible elements (3). For the last-mentioned group this was shown in [3, Example 9].

Proposition 1 and Theorem 1 will be proved in the next two sections. Section 4 supplies some additional information about Fermat over $\mathbb{F}_q$ and its connection with $x_1 = x_2 + x_3$. We think that this relation is possible for *every* non-abelian simple Galois group G in the regular case. This will also be discussed in Section 4 (see Proposition 2).

Historically, the first paper about linear relations between zeros of polynomials seems to be [8]. The same author wrote a number of papers about

linear relations in cases where the group G is that of our Theorem 1; his stabilizer, however, is the above group H itself, so the situation is quite different from the present one (see, for instance, [9]).

2. Some explanations and proofs. We begin with the justification of our concept of admissible elements. Let G be the Galois group of a polynomial f as above. We consider $L = K(x_1, \dots, x_n)$ as a left $K[G]$-module in the usual way: For $\alpha = \sum_{s\in G} a_s s \in K[G]$ and $y \in L$ we put $\alpha y = \sum_{s\in G} a_s s(y)$. In a naive sense, a relation between $x_1, \dots, x_n$ is just a vector $(a_1, \dots, a_n) \in K^n$ such that (1) holds. Suppose now $G_{x_1} = 1$. Then the map

$$G \to \{x_1, \dots, x_n\} : s \mapsto s(x_1)$$

is bijective. Therefore, we may identify $(a_1, \dots, a_n) \in K^n$ with an element $\alpha = \sum_{s\in G} a_s s$ of $K[G]$, on putting $a_s = a_j$ if $s(x_1) = x_j$. In particular, a relation $(a_1, \dots, a_n)$ between $x_1, \dots, x_n$ corresponds to an $\alpha \in K[G]$ such that $\alpha x_1 = 0$. The *normal basis theorem* says that there is a $y \in L$ such that

$$\varphi : K[G] \to L : \alpha \mapsto \varphi(\alpha) = \alpha y$$

is a $K[G]$-linear isomorphism. Suppose now that $\alpha \in K[G]$ is a relation between $x_1, \dots, x_n$, i.e., $\alpha x_1 = 0$. Put $\tau = \varphi^{-1}(x_1)$. Then $\alpha\tau = 0$ and, because $G_{x_1} = 1$, we also have $G_\tau = 1$. Hence α is an admissible element of $K[G]$. Conversely, let $\alpha \in K[G]$ be admissible, i.e., $\alpha\tau = 0$ for some $\tau \in K[G]$ with $G_\tau = 1$. Put $\widetilde{x} = \varphi(\tau)$. Then $G_{\widetilde{x}} = 1$ and $\alpha\widetilde{x} = 0$, so α is a relation between the zeros of the irreducible normal polynomial

$$\widetilde{f} = \prod_{s\in G} (Z - s(\widetilde{x})) \in K[Z].$$

Proof of Proposition 1. Let $G' \neq 1$ be a subgroup of G and suppose $\alpha \in K[G']$ is admissible. Let $\tau \in K[G']$ be such that $\alpha\tau = 0$ and $G'_\tau = 1$. We show that every $s \in G_\tau$ lies in G'. Then it lies in $G'_\tau = 1$, and since $\alpha\tau = 0$, α is an admissible element of $K[G]$.

If $\tau = 0$, then $G' = G'_\tau = 1$, which we have excluded. Hence $\tau = \sum_{t\in G'} c_t t \neq 0$, and there is an element $u \in G'$ with $c_u \neq 0$. If $s \in G$ stabilizes τ, we have $\tau = s\tau = \sum_{t\in G'} c_t st$; in particular, $c_u su$ must be equal to an element $c_t t$ for some $t \in G'$. This, however, requires $su = t$ and $s \in G'$. ∎

Remark 1. Proposition 1 shows that, as a rule, many relations are possible if the Galois group G of f acts regularly on $x_1, \dots, x_n$. For instance, if p is a prime dividing $|G|$, then G contains a cyclic subgroup G' of order p. Since $\alpha = \sum_{s\in G'} s \in K[G']$ is admissible, it is also an admissible element of $K[G]$. This shows that both $x_1 + x_2 = 0$ and $x_1 + x_2 + x_3 = 0$ are possible relations in the regular case if $|G|$ is divisible by 6. It does not show, however,

that these relations hold *simultaneously*: We cannot conclude that there is an element $x_1 \in L$ with $G_{x_1} = 1$ such that $x_1 = -x_2$ and $x_1 = -x_3 - x_4$ for K-conjugates x_2, x_3, x_4 of x_1. If this were true, the relation (2) would be possible in the regular case whenever $6 \mid |G|$.

As concerns the *proof of Theorem 1*, we start with the simpler direction now (the more complicated one is postponed to Section 3). Let $G = HF$ be a transitive subgroup of $\mathrm{AGL}(1, q)$ with F and H as above. We consider the K-vector space $K[\mathbb{F}_q]$ with basis $\mathbb{F}_q$. In order to avoid confusion, we write (a) if we consider $a \in \mathbb{F}_q$ as a basis vector of $K[\mathbb{F}_q]$ (which is actually rather different from a as an element of the finite field $\mathbb{F}_q$). Accordingly,

$$K[\mathbb{F}_q] = \bigoplus_{a \in \mathbb{F}_q} K(a).$$

Now $K[\mathbb{F}_q]$ is a $K[G]$-module in a natural way: In particular, $s = aX + b \in G$ acts on $K[\mathbb{F}_q]$ by

$$(aX + b) \sum_{c \in \mathbb{F}_q} r_c(c) = \sum_{c \in \mathbb{F}_q} r_c(ac + b), \qquad r_c \in K.$$

Note that $K[\mathbb{F}_q]$ is just the $K[G]$-module that is usually attached to the permutation representation of G on $\mathbb{F}_q$; in particular, $H \subset \mathbb{F}_q^\times$ is the stabilizer of $(0) \in K[\mathbb{F}_q]$.

Now suppose $a, b \in H$ are such that $a + b = 1$. Consider $x = (0) - (a^{-1}) \in K[\mathbb{F}_q]$ and $\alpha = (X) - (aX) - (bX + 1) \in K[G]$. If $s \in G$ stabilizes x, it must fix the basis vectors (0) and (a^{-1}) and, hence, the elements 0 and $a^{-1} \in \mathbb{F}_q$. But an element $s \in G$ with two fixed points in $\mathbb{F}_q$ equals 1 (a well-known fact, which can be checked directly for the fixed points in question). Moreover,

$$\alpha x = (0) - (a^{-1}) - (a \cdot 0) + (a \cdot a^{-1}) - (b \cdot 0 + 1) + (b \cdot a^{-1} + 1) = -(a^{-1}) + (ba^{-1} + 1),$$

since the other terms obviously cancel each other. The equation $a^{-1} = b \cdot a^{-1} + 1$, however, is equivalent to $1 = a + b$, which we assumed to be true. Thus, $\alpha x = 0$.

The $K[G]$-module $K[\mathbb{F}_q]$ is cyclic, since the basis vector (c), $c \in \mathbb{F}_q$, arises from (0) by $(c) = (X + c)(0)$ for $X + c \in F \subseteq G$. Then Maschke's theorem shows that $K[\mathbb{F}_q]$ is isomorphic to a (left) $K[G]$-submodule V of $K[G]$. Any $K[G]$-linear isomorphism $K[\mathbb{F}_q] \to V$ maps our above x onto an element $\tau \in K[G]$ with $G_\tau = 1$ and $\alpha\tau = 0$. This implies that α is an admissible element of $K[G]$.

Remark 2. Our first attempt to prove the converse direction of Theorem 1 was based on the assumption that for an admissible element $\alpha = 1 - s - t$ as in (3) there must be an $x \in K[\mathbb{F}_q]$ such that $\alpha x = 0$ and $x = (i) - (j)$ for some elements $i, j \in \mathbb{F}_q$, $i \neq j$. Such an x will henceforth be called a *simple difference* in $K[\mathbb{F}_q]$. The existence of a simple difference

that is annihilated by an α of this kind requires, indeed, that $a+b=1$ has a solution in H. The said assumption is *false*, however: In general there are admissible elements (3) that do not annihilate any simple difference, as we shall show in Section 4 (and so our first attempt failed).

REMARK 3. At this point we should say some words about *Dubickas' example*: He only considered the case $\mathrm{AGL}(1,5)$, but his idea remains valid if only the action of the Galois group G on the zeros $x_1,\dots,x_n$ of f is doubly transitive. Define $y_{ij}=x_i-x_j$ (a simple difference of zeros), where i,j, $i\neq j$, run through all elements of $\{1,\dots,n\}$. Because of the double transitivity, the elements y_{ij} are all conjugate, so $\widetilde{f}=\prod_{i\neq j}(Z-y_{ij})$ is an irreducible polynomial over K with Galois group G. Since $y_{12}-y_{32}-y_{13}=0$, we have a relation of type (2).

In this way one also obtains examples quite different from the regular case; for instance, if $G=S_n$, the stabilizer of y_{12} is isomorphic to S_{n-2}.

In the case $G=\mathrm{AGL}(1,q)$, $q>2$, this technique is essentially identical with what we have done in the above proof: We may assume that f has the zeros x_a, $a\in\mathbb{F}_q$, and that an element $s\in G$ acts on x_a by $s(x_a)=x_{s(a)}$. Put $y=x_0-x_1$ and choose $a\in\mathbb{F}_q^\times$, $a\neq 1$. Moreover, let $s,t\in G$ be such that $s(0)=a$, $s(1)=1$, $t(0)=0$, $t(1)=a$. Then $(1-s-t)y=0$ and $s=(1-a)X+a$, $t=aX$. Since $1-a\neq 0$, the equation $a+b=1$ has the solution $a,b=1-a$ in $H=\mathbb{F}_q^\times$.

REMARK 4. In the example of Remark 3 we have $y_{12}=y_{32}+y_{13}$ and, simultaneously, $y_{12}=-y_{21}$. This situation differs from the following case: Let $p\equiv 3 \bmod 4$, $p\geq 7$, and suppose $G=\mathrm{ASL}(1,p)$ is the Galois group of f. Then there is an irreducible normal polynomial $\widetilde{f}\in K[Z]$ with group G such that $y_1=y_2+y_3$ holds for the zeros $y_1,\dots,y_n$ of $\widetilde{f}$ (see introduction). However, $y_k=-y_1$ cannot be true for any k, $2\leq k\leq n$. Otherwise, there would be an $s\in G$ with $s(y_1)=y_k$ and $s(y_k)=s(-y_1)=-y_k=y_1$. As y_1 generates the splitting field of $\widetilde{f}$, s would be an involution, which is impossible since $n=|G|=p\,(p-1)/2$ is odd.

3. Proof of the converse direction. Let the notations of Section 2 hold, in particular, $G=HF$ is a transitive subgroup of $\mathrm{AGL}(1,q)$, $q=p^e$. We assume that there is an admissible element $\alpha=1-s-t\in K[G]$, $s,t\in G\setminus\{1\}$, $s\neq t$. We have to show that this implies $a+b=1$ for certain elements $a,b\in H$, $H\subseteq\mathbb{F}_q^\times$.

The plan of this proof is as follows: First we construct a certain simple $K[G]$-submodule V of $K[G]$ which contains an element $\varrho\neq 0$ with $\alpha\varrho=0$ (recall that $K[G]$-modules are always *left* modules!). Then we construct a K-basis of V such that the matrix of the K-linear map $V\to V:\varrho\mapsto\alpha\varrho$

can easily be read off. Since the determinant of this matrix must vanish, we have a condition that implies the desired equation in H.

Let ξ denote a primitive $p(q-1)$th root of unity (in some algebraic closure of K). We put $K' = K(\xi)$. Then α is also an admissible element of $K'[G]$; indeed, if $\tau \in K[G]$ is such that $\alpha\tau = 0$ and $G_\tau = 1$, then α does not loose these properties if it is considered as an element of $K'[G]$. Therefore, we may assume, without loss of generality, that K contains ξ. Under this assumption the K-irreducible characters of G are absolutely irreducible, so we simply speak of "irreducible characters" of G. These characters fall into two categories (see [6, p. 239]): First, 1-dimensional characters ψ of the cyclic group $G/F \cong H$, considered as characters of G by means of the canonical map $G \to G/F$. Second, characters induced by nontrivial 1-dimensional characters $\chi : F \to K^\times$ of the group F. Hence we distinguish between two categories of simple $K[G]$-modules, namely, those belonging to irreducible characters of the first and of the second category, respectively. This leads to the decomposition

$$K[G] = I \oplus J,$$

where I is the sum of the $K[G]$-submodules of $K[G]$ of the first and J the sum of those of the second category.

We now define the K-vector space

$$S = \{\sigma \in K[G] : \alpha\sigma = 0\}.$$

We shall show that there is a simple $K[G]$-submodule V of J such that $S \cap V \neq 0$. To this end we use the following

LEMMA 1. *In the above setting, let W be a $K[G]$-submodule of $K[G]$ and*

$$W = V_1 \oplus \cdots \oplus V_k \tag{4}$$

a direct decomposition of W into arbitrary $K[G]$-submodules. Then

$$W \cap S = (V_1 \cap S) \oplus \cdots \oplus (V_k \cap S).$$

Proof. Let $\sigma \in W \cap S$. Then $\sigma = \varrho_1 + \cdots + \varrho_k$ with $\varrho_j \in V_j$ for each $j = 1, \ldots, k$. Now $\alpha\sigma = 0 = \alpha\varrho_1 + \cdots + \alpha\varrho_k$, and since V_j is a (left) $K[G]$-module, we have $\alpha\varrho_j \in V_j$, $j = 1, \ldots, k$. The decomposition (4) being direct, we conclude $\alpha\varrho_j = 0$, $j = 1, \ldots, k$, so each ϱ_j lies in $V_j \cap S$. ∎

The lemma shows

$$S = (I \cap S) \oplus (J \cap S).$$

Suppose $J \cap S = 0$. We know that there is an element $\tau \in K[G]$ such that $\alpha\tau = 0$ and $G_\tau = 1$. In particular, $\tau \neq 0$. Since $J \cap S = 0$, τ lies in $I \cap S$. However, the group F acts trivially on I: Each simple $K[G]$-submodule V of I belongs to the first category. Therefore, it has K-dimension 1, and for

all $u \in G$ and $\varrho \in V$,

$$u\varrho = \psi(u)\varrho,$$

where $\psi : G \to K^\times$ is a group homomorphism with $\psi(F) = 1$. Accordingly, G_τ contains the group F, a contradiction.

Hence we have $J \cap S \neq 0$. Let $J = V_1 \oplus \cdots \oplus V_k$ be a decomposition of V into simple $K[G]$-submodules. Since $J \cap S \neq 0$, Lemma 1 entails $V_j \cap S \neq 0$ for some $j \in \{1, \ldots, k\}$. In particular, there is a simple submodule V of J with $V \cap S \neq 0$, as desired.

In the next step we choose a suitable K-basis of this module V and study the matrix of the K-linear map

$$V \to V : \varrho \mapsto \alpha\varrho$$

with respect to this basis (where α is our admissible element). The irreducible character connected with V is induced by some character $\chi : F \to K^\times$, $\chi \neq 1$. Since $F \cong \mathbb{F}_q$ is an elementary-abelian p-group, the values of χ are pth roots of unity.

A $K[G]$-module V' isomorphic to V can be constructed in the following way (see [6, p. 216]): The group H is cyclic, so $H = \langle v \rangle$ for some v of order $m = |H| = [G : F]$, $m \mid q - 1$. Let $K \cdot \varepsilon$ be the 1-dimensional $K[F]$-module belonging to χ, i.e., $u \in F$ acts on $K \cdot \varepsilon$ by

$$u \cdot \varepsilon = \chi(u) \cdot \varepsilon. \tag{5}$$

Then V' has the K-basis $v^j \otimes \varepsilon$, $j = 1, \ldots, m$. Each element of G has the shape $v^k u$, where $k \in \{1, \ldots, m\}$ and $u \in F$ are uniquely determined. Since F is a normal subgroup of G, we may write

$$w^{-1}uw = u^w \in F \tag{6}$$

for each $w \in H$ and $u \in F$. The action of G on V' is now defined by

$$v^k u \cdot (v^j \otimes \varepsilon) = v^{k+j} \otimes u^{v^j} \cdot \varepsilon = v^{k+j} \otimes \chi(u^{v^j}) \cdot \varepsilon = \chi(u^{v^j}) \cdot v^{k+j} \otimes \varepsilon \tag{7}$$

(in other words, we first apply the "exchange rule" $uv^j = v^j u^{v^j}$ contained in (6) and then (5)). Let $\varphi : V' \to V$ be a $K[G]$-linear isomorphism. Then φ maps the basis vectors $v^j \otimes \varepsilon$ onto basis vectors ϱ_j of V, $j = 1, \ldots, m$. The action of G on these vectors can be read off from (7), namely,

$$v^k u\varrho_j = \chi(u^{v^j})\varrho_{k+j}, \qquad k, j \in \{1, \ldots, m\},\ u \in F \tag{8}$$

(observe that the subscript $k + j$ has to be understood mod m, i.e., as an element of $\{1, \ldots, m\}$).

Let $\beta \in K[G]$. We consider the $m \times m$-matrix $M(\beta)$ that belongs to the K-linear map $V \to V : \varrho \mapsto \beta\varrho$; the elements b_{ij} of its jth column are given by

$$\beta\varrho_j = \sum_{i=1}^{m} b_{ij}\varrho_i.$$

In the special case $\beta = u \in F$, equation (8) yields

$$M(u) = \operatorname{diag}(\chi(u^v), \chi(u^{v^2}), \ldots, \chi(u^{v^m})), \tag{9}$$

and for $\beta = v^k$ we obtain

$$M(v^k) = \begin{pmatrix} & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \\ 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \end{pmatrix}; \tag{10}$$

the nonzero entries of this matrix (all of them $= 1$) are placed at the positions $(k+1, 1), (k+2, 2), \ldots, (m, m-k)$, and at $(1, m-k+1), (2, m-k+2)$, $\ldots, (k, m)$.

With these tools at hand it is no more difficult to establish $M(\alpha)$ for our admissible element $\alpha = 1 - s - t \in K[G]$. Because $V \cap S \neq 0$, there is a vector $\varrho \in V$, $\varrho \neq 0$, such that $\alpha\varrho = 0$ and, thus, $\det M(\alpha)$ must vanish. Regrettably, $M(\alpha)$ may take a number of different forms:

Case 1: $s, t \in F$. Here we read off from (9):

$$M(\alpha) = \operatorname{diag}(1 - \chi(s^v) - \chi(t^v), \ldots, 1 - \chi(s^{v^m}) - \chi(t^{v^m})).$$

This matrix is singular only if $1 - \chi(s^{v^j}) - \chi(t^{v^j}) = 0$ for some $j = 1, \ldots, m$. Since the values of χ are pth roots of unity, this is impossible: It is an exercise to show that $1 - \eta - \eta' = 0$ can hold for roots of unity η, η' only if η has order 6 and $\eta' = \eta^{-1}$.

Case 2: $s \in F$, $t \notin F$. Observe that G is a normal subgroup of $\mathrm{AGL}(1, q)$. Hence conjugation by elements of $\mathrm{AGL}(1, q)$ defines an automorphism of G. Such an automorphism can be considered as an automorphism of $K[G]$. It maps α onto an admissible element of the shape $1 - s' - t'$; here s' remains in the characteristic subgroup F of G and t' can be chosen equal to v^k, $1 \leq k \leq m-1$. We may, therefore, assume $\alpha = 1 - s - v^k$, which yields

$$M(\alpha) = \operatorname{diag}(1 - \chi(s^v), \ldots, 1 - \chi(s^{v^m})) - M(v^k), \tag{11}$$

with $M(v^k)$ as in (10). The entries of $M(\alpha)$ lie in $\mathbb{Z}[\zeta_p]$, where ζ_p is a primitive pth root of unity. Consider the prime ideal $\mathfrak{p} = (1 - \zeta_p)$ of $\mathbb{Z}[\zeta_p]$ (which lies over p) and the residue class field $R = \mathbb{Z}[\zeta_p]/\mathfrak{p}$. Since $1 - \chi(s^{v^j}) \in \mathfrak{p}$ for all $j = 1, \ldots, m$, (11) yields the identity

$$\overline{M(\alpha)} = \overline{-M(v^k)} \in R^{m \times m}$$

of matrices over R (the bar denotes residue classes mod $\mathfrak{p}$, not complex

conjugation). Thus, inspection of (10) gives $\det \overline{M(\alpha)} = \pm \det \overline{M(v^k)} = \pm 1 \in R$, and, in particular, $\det M(\alpha) \neq 0$. So this case is also impossible.

Case 3: Both $s, t \notin F$. Here the conjugation argument of Case 2 shows that we may assume $s = v^k$, $t = v^l u$, with $u \in F$ and $1 \leq k \leq l \leq m-1$. We distinguish two subcases:

Subcase 1: $u = 1$. Then $k < l$ (recall $s \neq t$) and $M(\alpha) = I_m - M(v^k) - M(v^l)$, where I_m is the $m \times m$ unit matrix. But in this case $M(\alpha)$ is a *cyclic group matrix*, whose determinant is well known. Indeed, put

$$b_i = \begin{cases} 1 & \text{if } i \equiv 0 \bmod m, \\ -1 & \text{if } i \equiv k \text{ or } i \equiv l \bmod m, \\ 0 & \text{otherwise.} \end{cases}$$

Then $M(\alpha) = (b_{i-j})_{i,j=1,\dots,m}$ and $\det M(\alpha) = \prod_\eta (1 - \eta^k - \eta^l)$, where η runs through all mth roots of unity. The argument of Case 1 shows that $\det M(\alpha) = 0$ only if $6 \mid m$ (and $k \equiv -l \bmod 6$). But then H contains an element r of order 6 and $r + r^{-1} = 1$ is a solution of $a + b = 1$ in H.

Subcase 2: $u \neq 1$. Again we consider the prime ideal $\mathfrak{p}$ and the field R of Case 2. Since $\overline{M(u)} = I_m$, we have $\overline{M(v^l u)} = \overline{M(v^l)}\,\overline{M(u)} = \overline{M(v^l)}$ and

$$\overline{M(\alpha)} = \overline{M(k,l)} \in R^{m \times m},$$

with $M(k,l) = I_m - M(v^k) - M(v^l)$. This matrix is essentially the group matrix of Subcase 1, with the only difference that the case $k = l$ is *not* excluded now. We obtain $\det \overline{M(\alpha)} = \det \overline{M(k,l)}$, where

$$\det M(k,l) = \prod_{\eta^m = 1} (1 - \eta^k - \eta^l) \in \mathbb{Z}. \tag{12}$$

Now $\det M(\alpha)$ vanishes, hence $\det M(k,l) \equiv 0 \bmod \mathfrak{p}$, and $\det M(k,l) \in \mathbb{Z}$ requires $\det M(k,l) \equiv 0 \bmod p$ (recall $\mathfrak{p} \cap \mathbb{Z} = \mathbb{Z}p$). Let ζ_m denote a primitive mth root of unity and $\mathfrak{P}$ a prime ideal of $\mathbb{Z}[\zeta_m]$ lying over p. The residue class degree f_p of $\mathfrak{P}$ equals the order of p mod m (see [13, p. 14]). Since $m \mid q - 1$, $p^e \equiv 1 \bmod m$, so $f_p \mid e$ and $\mathbb{Z}[\zeta_m]/\mathfrak{P}$ is a subfield of $\mathbb{F}_q$ (up to an isomorphism). From $p \mid M(k,l)$ and (12) we infer that $1 - \overline{\eta}^k - \overline{\eta}^l$ must vanish in $\mathbb{Z}[\zeta_m]/\mathfrak{P}$ for some mth root of unity η, hence also in $\mathbb{F}_q$. However, $H = \{a \in \mathbb{F}_q : a^m = 1\}$. So $a = \overline{\eta^k}$ and $b = \overline{\eta^l}$ form a solution of $a + b = 1$ in H. This concludes the proof of the converse direction of Theorem 1.

4. Additional remarks. Here we compile some additional information that may be of interest for the reader. First consider the determinant

$\det M(k,l)$ of (12). It can be written

$$\det M(k,l) = \prod_{d|m} N_d(1 - \zeta_d^k - \zeta_d^l),$$

where ζ_d is a primitive dth root of unity and $N_d : \mathbb{Q}(\zeta_d) \to \mathbb{Q}$ is the norm of the dth cyclotomic field. We call

$$W_d^{k,l} = N_d(1 - \zeta_d^k - \zeta_d^l)$$

the *Wendt factor* of order d that belongs to $\{k,l\}$ (note that $k = l$ is possible). The number $W_d^{k,l}$ is a divisor of *Wendt's determinant*, which has chiefly been studied in connection with the Fermat equation over $\mathbb{F}_p$ (see, for instance, [12]). If $H \subseteq \mathbb{F}_q^\times$ is as in Section 3, $|H| = m$, then the equation $a + b = 1$ is solvable in H only if there is a Wendt factor $W_d^{k,l}$, $d \mid m$, such that $p \mid W_d^{k,l}$. Conversely, suppose $p \mid W_d^{k,l}$. Then $W_d^{k,l}$ is divisible by $q' = p^{f_{p,d}}$, where $f_{p,d}$ is the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$. Since $p^e \equiv 1 \bmod d$, $f_{p,d} \mid e$ and $\mathbb{F}_{q'}$ is a subfield of $\mathbb{F}_q$. Moreover, the discussion at the end of Section 3 shows that $a + b = 1$ has a solution in the subgroup of order d of $\mathbb{F}_{q'}^\times$, and, in particular, in $H \cap \mathbb{F}_{q'}^\times$.

For a fixed number m there are only finitely many primes p dividing a Wendt factor $W_d^{k,l}$, $d \mid m$. For such a p we consider $q = p^e$, where e must be a multiple of $f_{p,d}$ and m must divide $q - 1$. Let $G = HF$, $|H| = m$, be the uniquely determined subgroup of $\mathrm{AGL}(1,q)$ of order qm. By the above, $K[G]$ contains an admissible element α of the shape (3).

In order to find all these primes p one may proceed as follows: Fix a divisor d of m. The definition of $W_d^{k,l}$ shows that it suffices to consider subsets $\{k,l\}$ of $\{1,\dots,d-1\}$. We may further assume that these subsets are *primitive*, i.e., $(k,l,d) = 1$. Indeed, for any common divisor r of k, l, d we have

$$W_d^{k,l} = (W_{d/r}^{k/r,l/r})^{\varphi(d)/\varphi(r)}.$$

Two numbers $W_d^{k,l}$, $W_d^{k',l'}$ coincide if the sets $\{k,l\}$ and $\{k',l'\}$ arise from each other under the action of the group $(\mathbb{Z}/d\mathbb{Z})^\times$, i.e., $\{k',l'\} = \{jk, jl\}$ for some integer j, $(j,d) = 1$ (jk, jl must be understood mod d). Accordingly, one has to establish a set of representatives of the orbits of $(\mathbb{Z}/d\mathbb{Z})^\times$ on the primitive subsets of $\{1,\dots,d-1\}$ with at most two elements. If $\{k,l\}$ is such a representative, $W_d^{k,l}$ can easily be computed by means of the identity

$$\overline{W_d^{k,l}} = \prod_{r^d=1} (1 - r^k - r^l) \in \mathbb{Z}/\widetilde{p}\,\mathbb{Z},$$

where $\widetilde{p}$ is a (sufficiently large) prime number, $\widetilde{p} \equiv 1 \bmod d$, and r runs through all dth roots of unity in $\mathbb{Z}/\widetilde{p}\,\mathbb{Z}$.

EXAMPLE. Take $m = 16$. The group $(\mathbb{Z}/16\mathbb{Z})^\times$ has 13 orbits of primitive subsets of $\{1,\dots,15\}$ with one or two elements. They yield the Wendt factors

$W_{16}^{1,1} = 257$, $W_{16}^{1,2} = 49$ and $W_{16}^{1,3} = 17$. The Wendt factors belonging to the remaining ten orbits either coincide with these or are equal to 1. Whereas $f_{p,16} = 1$ for $p = 17, 257$, we have $f_{7,16} = 2$. The seven orbits of $(\mathbb{Z}/8)^\times$ produce the Wendt factors 17, 9 and $f_{17,8} = 1$, $f_{3,8} = 2$. In the case $d = 4$ we have three orbits yielding the Wendt factor 5, and for $d = 2$ there is one orbit yielding 3. Altogether, the prime 3 occurs twice and in different roles: as a divisor of $W_8^{1,2}$ and of $W_2^{1,1}$, corresponding to the identity $r + r^2 = 1$ that holds for a certain generator r of $\mathbb{F}_9^\times$, and to $\overline{2}+\overline{2} = 1 \in \mathbb{F}_3$, respectively.

We now return to Remark 2 of Section 2 (about simple differences). In the (most interesting) Subcase 2 of Section 3, $\alpha \in K[G]$ has the shape $\alpha = (X)-(aX)-(bX+c)$ with $a, b \in H \subseteq \mathbb{F}_q^\times$, $c \in \mathbb{F}_q$. If $a+b = 1$, there is a simple difference $x = (i)-(j) \in K[\mathbb{F}_q]$ such that $\alpha x = 0$, and this proves the admissibility of α (which is, essentially, what we did in Section 2). Conversely, it is not hard to check that $\alpha x = 0$ can hold for a simple difference x only if $a + b = 1$. The K-vector space $K[\mathbb{F}_q]$ has a natural nondegenerate bilinear form defined by

$$\Big\langle \sum_{j\in\mathbb{F}_q} a_j(j), \sum_{j\in\mathbb{F}_q} b_j(j) \Big\rangle = \sum_{j\in\mathbb{F}_q} a_j b_j.$$

We consider the K-linear map $K[\mathbb{F}_q] \to K[\mathbb{F}_q] : y \mapsto \alpha y$. By abuse of terminology, this map is called α again. Let α^* be the *adjoint* map of α with respect to $\langle -, - \rangle$. One readily verifies that α^* is the K-linear map defined by

$$\alpha^* = (X) - (aX)^{-1} - (bX + c)^{-1},$$

the inverse elements being taken in $\mathrm{AGL}(1, q)$. So $\alpha^* = (X) - (a^{-1}X) - (b^{-1}X + c')$, $c' \in \mathbb{F}_q$. The linear map α and its adjoint α^* have the same rank. Therefore, $a+b = 1$ implies that there must be a $y \in K[\mathbb{F}_q] \smallsetminus \{0\}$ such that $\alpha^* y = 0$. However, the identity $a^{-1} + b^{-1} = 1$ is false in general, and then y *cannot* be a simple difference. One can show that α^* is, nevertheless, admissible at least if $m = |H|$ is a prime number.

The above discussion of the matrix $M(k, l)$ and the factors $W_d^{k,l}$ of its determinant shows that from $p \,|\, \det M(k, l)$ one cannot immediately read off a solution of $a+b = 1$ in H. The matrix $M(\alpha)$ of Section 3 seems to contain much more information about possible solutions. We know, for our present α, that $\det M(\alpha)$ vanishes if, and only if, $\det M(\alpha^*)$ vanishes. In general this happens only if $a + b = 1$ or $a^{-1} + b^{-1} = 1$, i.e., in the cases one expects. There are, however, also some unexpected cases: for instance $m = 5$, $q = 31$, $\alpha = (X) - (\overline{4}X) - (\overline{4}X + 1)$, or $m = 8$, $q = 17$, $\alpha = (X) - (\overline{8}X) - (\overline{16}X + 1)$, where $\det M(\alpha)$ vanishes although none of the said identities holds. These cases seem to be rare, but it would, nevertheless, be interesting to know *why* they occur.

Although $M(\alpha)$ looks quite similar to the cyclic group matrix $M(k,l)$ to which it is congruent mod $\mathfrak{p}$ (one just has to replace m entries -1 of $M(k,l)$ by certain values $-\zeta_p^k$), $M(\alpha)$ is, in general, not a cyclic group matrix—whose eigenvalues would lie in a cyclotomic field. Even if $\det M(\alpha) = 0$, the Galois group of the characteristic polynomial of $M(\alpha)$ may be S_{m-1} or S_{m-2} (over the field of definition $\mathbb{Q}(\zeta_p)$ of $M(\alpha)$). This happens, for instance, in the above case $m = 8$, $q = 17$, $\alpha = (X) - (\overline{8}X) - (\overline{16}X + 1)$, where this group is S_6.

Finally, we return to the *inclusion lemma* (Proposition 1), which offers an easy way to prove the possibility of $x_1 = x_2 + x_3$ in the regular case. Another example for this fact is the following

PROPOSITION 2. *Let G be a finite simple linear group, i.e., $G = \mathrm{PSL}(n,q)$, $q = p^e$, $n \geq 3$ or $n = 2$ and $q \geq 4$. Then $K[G]$ contains an admissible element α of the shape* (3).

Proof. If $n \geq 3$, we consider the embedding

$$\mathrm{AGL}(1,q) \to \mathrm{SL}(n,q) : aX + b \mapsto \left(\begin{array}{cc|ccc} a & b & & & \\ 0 & 1 & & & \\ \hline & & a^{-1} & & \\ & & & 1 & \\ & & & & \ddots \end{array}\right).$$

Since $\mathrm{PSL}(n,q) = \mathrm{SL}(n,q)/\{c \cdot I_n : c^n = 1\}$, we see that $\mathrm{AGL}(1,q)$ is isomorphic to a subgroup of $\mathrm{PSL}(n,q)$. For $G' = \mathrm{AGL}(1,q)$ the group ring $K[G']$ contains an admissible element if $q > 2$ (see Remark 3 of Section 2). In the case $q = 2$ we have

$$\mathrm{PSL}(n,q) \cong \mathrm{GL}(n,q) \supseteq \mathrm{GL}(3,q) \cong \mathrm{PSL}(2,7) \supseteq \mathrm{ASL}(1,7)$$

(see [5, p. 183]), which concludes the proof in this case (observe $\overline{4} + \overline{4} = 1 \in \mathbb{F}_7$). In the case $n = 2$ we use $\mathrm{PSL}(2,q) \supseteq \mathrm{ASL}(1,q)$, which proves the assertion for $p \geq 7, e \geq 1$ (see introduction) and $p = 2, e \geq 2$ (where $\mathrm{ASL}(1,q) = \mathrm{AGL}(1,q)$). In the remaining cases one can use $\mathrm{PSL}(2,5) \cong A_5 \supseteq A_4$ and $\mathrm{PSL}(2,3) \cong A_4$ (ibid.). ∎

The *Atlas of Finite Groups* [1] gives the impression that a finite simple non-abelian group always contains a subgroup $\cong S_3$ or $\cong A_4$, with the exception of the Suzuki groups $\mathrm{Sz}(q)$, $q = 2^{2n+1}$. These, however, contain $\mathrm{AGL}(1,5)$, as can be extracted from [7, p. 190]. So it seems realistic that the assertion of Proposition 2 remains true for *all* finite simple nonabelian groups.

Acknowledgements. The author gratefully acknowledges the support by the Austrian Science Fund (FWF Project P16641-N12).

References

[1] J. H. Conway *et al.*, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
[2] M. Drmota and M. Skałba, *Relations between polynomial roots*, Acta Arith. 71 (1995), 65–77.
[3] K. Girstmair, *Linear relations between roots of polynomials*, ibid. 89 (1999), 53–96.
[4] L. K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.
[5] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
[6] —, *Character Theory of Finite Groups*, de Gruyter, Berlin, 1998.
[7] B. Huppert and N. Blackburn, *Finite Groups III*, Springer, Berlin, 1982.
[8] V. A. Kurbatov, *On equations of prime degree*, Mat. Sb. 43 (1957), 349–366 (in Russian).
[9] V. A. Kurbatov and A. N. Novogrudskaya, *Linear relations of conjugate elements in the Galois field of a solvable equation of degree* p^2, Sverdlovsk. Gos. Ped. Inst. Uchen. Zap. 54 (1967), 104–114 (in Russian).
[10] F. Lalande, *La relation linéaire* $a = b + c + \cdots + t$ *entre les racines d'un polynôme*, preprint, 10 pp.
[11] M. Lederer, *Relationenmoduln für konjugierte algebraische Zahlen*, Dissertation, Innsbruck, 2004.
[12] A. Similarides, *Upper bounds for prime divisors of Wendt's determinant*, Math. Comp. 71 (2002), 415–427.
[13] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

Institut für Mathematik
Universität Innsbruck
Technikerstr. 25/7
A-6020 Innsbruck, Austria
E-mail: Kurt.Girstmair@uibk.ac.at

Received on 8.3.2006
and in revised form on 19.4.2006 (5157)