Bollettino
Unione Matematica Italiana

H. Heineken

Groups generated by two mutually Engel periodic elements

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **3-B** (2000), n.2, p. 461–470.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2000_8_3B_2_461_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2000.

Bollettino U. M. I.
(8) 3-B (2000), 461-470

Groups Generated by two Mutually Engel Periodic Elements.

H. HEINEKEN

Dedicated to Professor Mario Curzio
on the occasion of his seventieth birthday.

Sunto. – *Scriviamo* $[x, y] = [x,_1 y]$ *ed* $[[x,_k y], y] = [x,_{k+1} y]$. *Cerchiamo gruppi* $SL(2, q)$ *con generatori* x, y *tali che* $[x,_m y] = x$ *ed* $[y,_n x] = y$ *per alcuni numeri naturali* m, n.

Introduction.

As usual we put $x^{-1}y^{-1}xy = [x, y]$ and we define successively for all integers $[x, y] = [x,_1 y]$ and $[[x,_k y], y] = [x,_{k+1} y]$. Two elements x and y shall be called *mutually Engel periodic* or shorter *a mep-pair* if there are integers m and n such that $[x,_m y] = x$ and $[y,_n x] = y$. We would like to know for which integers m, n a mep-pair will generate a nontrivial group, and we modify this question by asking in which cases this group has a quotient group (proper or not) isomorphic to some $SL(2, q)$. This question and related ones have for instance been considered in the context of finite varieties by Rolf Brandl [1] who asked there if mep-pairs exist in all minimal simple groups and who showed the existence of epimorphisms of groups defined by mep-pairs onto $SL(2, p)$ for some selected cases. Lemma 1 will show us that this is the case if and only if the same is true for $PSL(2, q)$. The first example of a mep-pair was found quite some time ago in A_5 or rather $PSL(2, 5)$ with two elements of order 5 and $m = n = 5$. This is the first member of a family which is treated in section 4 and which leads to mep-pairs in $SL(2, p)$ for all primes p of the form $5 + 8t$ and some of the form $1 + 8t$. In this case the mep-pair consists of elements with trace -2. Later we will find mep-pairs for $SL(2, q)$ where q is a prime such that $q^3 - q$ is divisible by 7, for the remaining primes p we find mep-pairs for $q = p^3$. The main task will be to solve a functional equation in two variables; this is done here under the further assumption that one of the variables has the period two. This leads to an equation which is connected with the seventh roots of unity. A special role is played by mep-pairs of elements of order 10 (or 5 if the characteristic of the field is 2). They always generate a subgroup isomorphic to $SL(2, 5)(SL(2, 4))$.

1. – Elementary properties.

We collect here statements of general nature.

LEMMA 1. – *Assume that* (x, y) *is a mep-pair. Then*:

(1) $\langle x, y\rangle$ *is perfect,*

(2) x, xy^{-1} *and* y^{-1} *are conjugate in* $\langle x, y\rangle$,

(3) *if* G *is perfect,* G *is generated by a mep-pair if and only if* $G/Z(G)$ *is.*

PROOF. – (1) is trivial since the generators are commutators. For (2) assume

$$y = [y, {}_m x] = [[y, {}_{m-1} x], x].$$

Then

$$yx^{-1} = [y, {}_{m-1} x]^{-1} x^{-1} [y, {}_{m-1} x]$$

and so yx^{-1} and x^{-1} are conjugate in $\langle x, y\rangle$. By symmetry, the same is true for y^{-1} and xy^{-1}, and, by taking inverses, for y and yx^{-1}. Being generated by a mep-pair is of course inherited by quotient groups so for (3) it suffices that G has the property if $G/Z(G)$ has it. So let $(aZ(G), bZ(G))$ be a mep-pair generating $G/Z(G)$. Then there are elements $z_1, z_2 \in Z(G)$ such that

$$[a, {}_m b] = az_1; \qquad [b, {}_m a] = bz_2.$$

Now (az_1, bz_2) is a mep-pair generating G.

COROLLARY 1. – (1) *The two elements of a mep-pair have the same order,*

(2) *the elements of a mep-pair can not have order* 2,

(3) *whenever* $SL(2, q)$ *is perfect, the existence of a generating mep-pair is equivalent to the existence of a generating mep-pair for* $PSL(2, q)$.

2. – Consequences for 2×2-matrices.

It seems easier to consider the groups $SL(2, q)$ since we have the matrix presentation here. We are in the position to consider a «normal form», and this form we will use throughout.

LEMMA 2. – (1) *Assume that* $x, y \in SL(2, q)$ *is a mep-pair and the eigenvalues of* x, y *belong to* $GF(q)$. *If* λ *is an eigenvalue of* x, *the elements* x, y *can*

be described in matrix form in the following way:

$$x = \begin{pmatrix} \lambda & \tau \\ 0 & \lambda^{-1} \end{pmatrix}, \qquad y = \begin{pmatrix} \lambda^{-1} & 0 \\ 1 & \lambda \end{pmatrix},$$

with $\tau = \lambda^2 + \lambda^{-2} - \lambda - \lambda^{-1}$.

(2) *Every mep-pair* (x', y') *in* $SL(2, q)$ *with the same eigenvalue* λ *is conjugate to* (x, y) *by an element of* $GL(2, q)$.

(3) *For a mep-pair with eigenvalue* λ *we have*

$$(\lambda - 1)(\lambda^2 + 1)(\lambda^2 + \lambda + 1)(\lambda^2 - \lambda + 1) \neq 0 .$$

PROOF. – Since $\lambda \in GF(q)$, the eigenvectors of x and y exist in the vector space. No eigenvector of x can be an eigenvector of y at the same time, otherwise (x, y) do not generate a perfect group. By conjugation in $GL(2, q)$ we are able to modify (x, y) in such a way, that $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is eigenvector of x to the eigenvalue λ while $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is eigenvector of y to the eigenvalue λ. The second eigenvalue is clearly λ^{-1}. Also (by conjugation with a diagonal matrix) it is possible to obtain 1 in the lower left corner of y. The value of τ now follows from the fact that xy^{-1} must have the same trace as x and y by conjugacy, see Lemma 1(2). This shows (1), and also (2) can be seen from this argument. For (3) we see that $\tau = 0$ for $\lambda = 1$ and $\lambda^2 + \lambda + 1 = 0$. For $\lambda^2 + 1 = 0$ we obtain for $\langle x, y \rangle$ a quaternion group of order 8, which is impossible. Finally, if $\lambda^2 - \lambda + 1 = 0$, the images of all the three elements x, y, xy^{-1} in $PSL(2, q)$ would have order 3, while the image of xy would have order 2. This leads to a group isomorphic to A_4 (see Coxeter and Moser [2], p. 137), and we have again a contradiction, and the inequality is shown.

COROLLARY 2. – *For a mep-pair in* $SL(2, q)$ *with (minimal) periods* m *and* n, *always* $m = n$, *and it suffices to prove one of the two commutator equations.*

PROOF. – By Lemma 2(2) there is an element $z \in GL(2, q)$ such that $z^{-1}xz = y$; $z^{-1}yz = x$.

In Lemma 2 we assumed the scalar field $GF(q)$ to be «big enough» to have all eigenvalues of x, y in $GF(q)$. We will now consider the case in which the trace $\lambda + \lambda^{-1}$ is contained in a proper subfield $GF(r)$ of $GF(q)$. In this case there are matrices in $SL(2, r)$ with the same characteristic polynomial as x. We want to decide where the subgroup $\langle x, y \rangle$ is situated.

LEMMA 3. – *Let $x, y \in SL(2, q)$ be a mep-pair with eigenvalue λ. Then $\langle x, y\rangle$ is isomorphic to a subgroup of $SL(2, r)$, where r is the order of the smallest subfield of $GF(q)$ that contains $\lambda + \lambda^{-1}$.*

PROOF. – If $\lambda \in GF(t)$ with t minimal, then x and y are written as elements of $SL(2, t)$ if they are in the form given in Lemma 2. Assume that $r < t$; in this case we have $r^2 = t$. The 2-dimensional vector space over $GF(t)$ on which x and y act can also be considered as a 4-dimensional vector space over $GF(r)$, and x and y act on 2-dimensional subspaces of this vector space since they have characteristic polynomials with coefficients in $GF(r)$. It has to be shown that there is a 2-dimensional subspace which is left invariant both by x and by y. For this we begin with a vector $d = \begin{pmatrix} 1 \\ \alpha \end{pmatrix}$ and we want to choose the value of $\alpha \in GF(t)$ in such a way that the vectors d, xd, yd are linearly dependant with coefficients in $GF(r)$. In other words, we are looking for $\alpha \in GF(t)$ together with $a, b, c \in GF(r)$ such that $ad + bxd + cyd = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. We obtain the following equations for the components:

$$a + b(\lambda + \tau\alpha) + c\lambda^{-1} = 0\,,$$

$$a\alpha + b\lambda^{-1}\alpha + c(1 + \lambda\alpha) = 0\,.$$

If r is a power of 2, we multiply the first equation with α and obtain $b((\lambda + \lambda^{-1})\,\alpha + \tau\alpha^2) + c(1 + (\lambda + \lambda^{-1})\,\alpha) = 0$, and this is satisfied by $b = c$; $\tau\alpha^2 = 1$. Substituting this in the first equation yields $a + b(\lambda + \lambda^{-1} + \tau\alpha) = 0$. We see furthermore that τ, α and $\lambda + \lambda^{-1}$ belong to $GF(r)$, and so a, b, c can also be chosen from $GF(r)$.

If r is odd, we will use the automorphism mapping every element onto its r-th power to find two further equations. This automorphism fixes a, b, c and τ, it maps λ onto λ^{-1}. The two new equations are

$$a + b(\lambda^{-1} + \tau\alpha^r) + c\lambda = 0\,,$$

$$a\alpha^r + b\lambda\alpha^r + c(1 + \lambda^{-1}\alpha^r) = 0\,.$$

Multiplying the first of the four equations by α^r and subtracting from the fourth leads to $c = b\tau\alpha^{r+1}$, on the other hand, subtracting the first from the third equation leads to $b(\lambda - \lambda^{-1} + \tau(\alpha - \alpha^r)) + c(\lambda^{-1} - \lambda) = 0$ or $c = b(1 + \tau(\alpha - \alpha^r)(\lambda - \lambda^{-1})^{-1})$. Comparing the coefficients and rearranging yields

$$(\alpha + (\lambda - \lambda^{-1})^{-1})^{r+1} = \tau^{-1} - (\lambda - \lambda^{-1})^{-2}.$$

Inserting c in the first equation leads to $a + b(\lambda^{-1} + \tau\alpha^r + \lambda\tau\alpha^{r+1}) = 0$, and by the preceding equation on α it follows that the coefficient of b is contained in

$GF(r)$, so a, b, c can be chosen in $GF(r)$, and we have found a 2-dimensional $GF(r)$ subspace which is left invariant by both x and y, in particular, $\langle x, y\rangle$ is isomorphic to a subgroup of $SL(2, r)$.

Lemma 3 shows that the extension of the scalar field does not lead to any new difficulties, we will therefore keep to the tactics of Lemma 2; the field is taken big enough to contain the eigenvalues of x.

3. – The functional equation.

We will use the form for x and y we have laid down for a mep-pair. First we will show that for a matrix which is a commutator with y all information is contained in the right hand column provided the upper right position is non-zero (since in this case there can not be an engel period, this restriction is not serious). This will then allow us to find a system of two functional equations in two functions as variables.

LEMMA 4. – *Let y be as in Lemma 2 and $w \in SL(2, q)$. The matrix $[w, y]$ is completely defined by the right hand column provided the upper right hand position is non-zero.*

PROOF. – Let $[w, y] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We have $\det([w, y]) = 1$, also $[w, y]y^{-1}$ is conjugate to y^{-1} and has the same trace as y. This yields

$$ad - bc = 1\,,$$

$$a\lambda - b + d\lambda^{-1} = \lambda + \lambda^{-1}.$$

Now the statement follows easily.

In the following we will modify the notation of the preceding lemma by putting $w(i) = \begin{pmatrix} a(i) & b(i) \\ c(i) & d(i) \end{pmatrix}$.

LEMMA 5. – *Let y be as in Lemma 2 and $w(i) \in SL(2, q)$ such that $w(0) = x$ and $w(i+1) = [w(i), y]$ for $i > 0$. Then*

$$b(i+1) = b(i)(\lambda b(i) + (\lambda^2 - 1)\, d(i))\,,$$

$$d(i+1) = \lambda^2 - (1 + \lambda^{-2} + \lambda^{-1} b(i) - \lambda^{-2} d(i))(\lambda b(i) + (\lambda^2 - 1)\, d(i))\,.$$

PROOF. – The first equation is obtained by direct computation. As for the

second, we have

$$d(i+1) = -\lambda^2 c(i)\, b(i) - \lambda a(i)\, b(i) + a(i)\, d(i) =$$

$$\lambda^2 (1 - a(i)\, d(i)) - \lambda a(i)\, b(i) + a(i)\, d(i).$$

Now $d(i+1) = \lambda^2 + a(i)((1-\lambda^2)\, d(i) - \lambda b(i))$, and the equation follows by eliminating $a(i)$.

4. – The special case $\lambda = -1$.

The not so transparent system of functional equations becomes much easier if $\lambda = -1$. This case was considered much earlier (coming from considerations in A_5, then in $SL(2, 5)$) by Professor Rolf Brandl and the author. The author is indebted to R. Brandl for many discussions regarding this question.

LEMMA 6. – *Let* -4 *be an element of odd multiplicative order in* $GF(p)$, *where* p *is a prime. Then*:

(a) *There is a mep-pair of eigenvalue* -1 *generating* $SL(2, p)$.

(b) *The (minimal) period of this mep-pair is* kp *or* k, *where* k *is minimal such that* $2^k - 1$ *is a multiple of the order of* -4 *modulo* p.

PROOF. – For $\lambda = -1$ the equations reduce to

$$b(i+1) = -b(i)^2,$$

$$d(i+1) = 1 + 2b(i) - b(i)^2 - b(i)\, d(i).$$

with initial values $b(0) = 4$; $d(0) = -1$. The first equation is restricted to the function $b(i)$ and we obtain $b(i) = -(-4)^{2^i}$. We see that $b(0) = b(k)$ if and only if $(-4)^{(2^k - 1)} = 1$, and this happens for some k if and only if -4 is of odd order. Also we have $b(i) = b(i+k)$ for all i if $b(0) = b(k)$ is true. We consider now the second equation. We have $d(k) = Rd(0) + S(0)$ where $R = (-1)^k \prod_{i=0}^{k-1} b(i) = 1$ and $S(0)$ can be written as a polynomial in $d(0)$. Now $d(sk) = d(0) + S(0) + S(k) + \ldots + S((s-1)\, k) = d(0) + sS(0)$, and so $b(0) - b(pk) = d(0) - d(pk) = 0$. From Corollary 2 we see that we have a mep-pair with period of length pk (or k, if $S(0) = 0$).

$SL(2, p)$ is generated by this pair since $SL(2, p)$ is always generated by two different Sylow-p-subgroups of it.

THEOREM 1. – *If* p *is a prime such that* $p - 5$ *is divisible by* 8, *then* $SL(2, p)$ *possesses a mep-pair with eigenvalue* -1.

PROOF. – We have to show that -4 is an element of odd order. If p is as as-

sumed in the theorem, -1 is a square and not a fourth power, also 2 is not a square and its square 4 is not a fourth power. The product is a fourth power and therefore of odd order.

REMARK. – The condition of Lemma 6 is also satisfied for some primes p having the property that $p-1$ is divisible by 8, for instance by 41 and by 113, but never by Fermat primes different from 5.

5. – The functional equation, rearranged.

In this section we shall assume throughout that $\lambda^2 \neq 1$.

We will try to simplify the system of equations by taking the factor appearing in the first equation as a new variable, so we put $e(i) = \lambda b(i) + (\lambda^2 - 1)\, d(i)$. For $\lambda^2 \neq 1$ the pairs of functions $(b(i),\, d(i))$ and $(b(i),\, e(i))$ can be computed from one another, and periodicity of one gives periodicity with the same period for the other. The new equations are

$$b(i+1) = b(i)\, e(i)\,,$$

$$e(i+1) = \lambda^4 - \lambda^2 + ((\lambda^{-2} - \lambda^2) + \lambda^{-2} e(i))\, e(i)\,.$$

Again we have one equation on only one variable, this time on $e(i)$. We will consider the situation that $e(i)$ has a short given period.

LEMMA 7. – $e(0) = e(1)$ *if and only if* $e(0) = \lambda^4$ *if and only if* $\lambda^5 = -1 \neq \lambda$.

PROOF. – The second equation of the system leads to

$$e(0)^2 + (1 - \lambda^2 - \lambda^4)\, e(0) + \lambda^6 - \lambda^4 = 0$$

which reduces to the alternatives $e(0) = \lambda^4$ and $e(0) = \lambda^2 - 1$. From $b(0) = \tau = \lambda^2 + \lambda^{-2} - \lambda - \lambda^{-1}$ and $d(0) = \lambda^{-1}$ we find $e(0) = \lambda^3 - \lambda^2 + \lambda - 1$. Now $e(0) = \lambda^2 - 1$ leads to $\lambda^3 - 2\lambda^2 + \lambda = 0$ which is impossible. The other case $e(0) = \lambda^4$ leads to the equation $-\lambda^4 + \lambda^3 - \lambda^2 + \lambda - 1 = 0$ which is equivalent to the given one.

COROLLARY 3. – *A mep-pair of elements of order* 10 *in* $SL(2, q)$ *for* q *odd generates a subgroup isomorphic to* $SL(2, 5)$, *a pair of order* 5 *in* $SL(2, 2^m)$ *generates a subgroup isomorphic to* $SL(2, 4)$.

It is well known that $SL(2, q)$ with q odd possesses a subgroup isomorphic to $SL(2, 5)$ whenever it possesses elements of order 5, and that $SL(2, 2^m)$ possesses a subgroup isomorphic to $SL(2, 4)$ under the same circumstances, i.e. if m is even. The statement of Corollary 3 now follows from the uniqueness stated in Lemma 2: a mep-pair can always be brought into the «canonical form» given there, and the subgroups $SL(2, 5)$, $SL(2, 4)$ possess these mep-pairs. It can be seen easily that the period is always 5.

We will now consider the case that $e(i)$ is of period 2. It shows to be helpful to exclude period 1 at the same time.

LEMMA 8. – *Let* $e(0) = e(2) \neq e(1)$. *Then*

$$\lambda^{-2} - \lambda^2 + 1 + \lambda^{-2}(e(0) + e(1)) = 0\,,$$

$$e(1)e(0) = \lambda^2,$$

and, for $t = \lambda + \lambda^{-1}$, $t^3 - 2t^2 - t + 1 = 0$.

PROOF. – Let $\alpha = \lambda^{-2}$; $\beta = \lambda^{-2} - \lambda^2$; $\gamma = \lambda^4 - \lambda^2$. Then $e(i+1) = \alpha e(i)^2 + \beta e(i) + \gamma$ and $e(2) - e(0) = e(2) - e(1) + e(1) - e(0) = \alpha(e(1)^2 - e(0)^2) + (\beta + 1)(e(1) - e(0))$. Division by $e(1) - e(0)$ leads to the first statement:

$$\alpha(e(1) + e(0)) + \beta + 1 = 0\,.$$

We multiply this with $e(0)$ and obtain $0 = \alpha e(1)\, e(0) + \alpha e(0)^2 + \beta e(0) + e(0) = \alpha e(1)\, e(0) + e(1) + e(0) - \gamma$, and, by the previous result,

$$e(1)\, e(0) = (\beta + 1)\alpha^{-2} + \gamma\alpha^{-1}.$$

The first two equations now follow by elimination of α, β, γ. If further $e(1)$ is eliminated in the first equation and if we use $e(0) = \lambda^3 - \lambda^2 + \lambda - 1$ we obtain

$$\lambda^6 - 2\lambda^5 + 2\lambda^4 - 3\lambda^3 + 2\lambda^2 - 2\lambda + 1 = 0\,,$$

and $t^3 - 2t^2 - t + 1 = 0$ for $t = \lambda + \lambda^{-1}$.

We will now have a special look at the polynomial just mentioned.

LEMMA 9. – *The polynomial* $P(t) = t^3 - 2t^2 - t + 1$ *over* $GF(q)$ *is product of three linear factors if* $q^3 - q$ *is divisible by* 7 *and irreducible for all other* q. *If* r *is a zero of* $P(t)$, *the other two are* $r^2 - 2r$ *and* $-r^2 + r + 2$.

PROOF. – For q a power of 7 we see $t^3 - 2t^2 - t + 1 = (t-3)^3$. In all other cases choose $u = -t^{-1}$. Then $u^3 P(-u^{-1}) = u^3 + u^2 - 2u - 1$ is the polynomial to be considered, and the zeros of this polynomial are the sums $\sigma + \sigma^{-1}$, where σ is a primitive seventh root of unity. The polynomial is product of three linear factors if $q^2 - 1$ is divisible by 7 and irreducible otherwise; the same applies obviously for the polynomial of the lemma. The statement on the roots is checked easily.

6. – Consequences.

We state the existence of mep-pairs for period 2 of the function $e(n)$.

THEOREM 2. – (a) *There is a mep-pair generating* $SL(2, p)$ *for all*

primes p with the property that $p^3 - p$ is divisible by 7. For all other primes p there is a mep-pair generating $SL(2, p^3)$.

(b) *If k is the order of the elements of the mep-pair, the (minimal) period of the mep-pair is k if k is even and $2k$ if k is odd.*

PROOF. – For primes p with $p^3 - p$ divisible by 7 we have by Lemma 8 and Lemma 9 that there are elements x, y forming a mep-pair of period 2 with $\lambda + \lambda^{-1} \in GF(p)$, since $e(0) = e(2)$ and $b(2) = \lambda^2 b(0)$ we have $(b(0), e(0)) = (b(2k), e(2k))$ where $2k$ is the smallest even number that is divisible by the order of λ. For the other primes the same argument leads to a mep-pair of period 2 generating a subgroup of $SL(2, p^3)$, which, in addition, has to be perfect. By the famous theorem of Dickson (see for instance Huppert [3], p. 213), we know that the only perfect subgroups of $PSL(2, p^f)$ are isomorphic to $PSL(2, p^g)$ for divisors g of f and possibly $PSL(2, 5)$, the corresponding statement is true for $SL(2, p^f)$. Since $e(0) \neq e(1)$, and because of Lemma 2(3), the order of λ is different from 10 and higher than 6, the mep-pair does not generate a subgroup isomorphic to $SL(2, 5)$. This clears the first case, in the second case, the mep-pair can not generate a subgroup isomorphic to $SL(2, p)$ since the trace $\lambda + \lambda^{-1}$ is not contained in $GF(p)$. The proof is complete.

We can also say something about the orders of the elements of a mep-pair. This is collected in

PROPOSITION 1. – *Let p be a prime.*

(a) *If $p^3 - p$ is prime to 7, there are three mep-pairs mapped onto each other by the field automorphism of $GF(p^3)$. The order of the elements of the mep-pairs divides $p^3 - 1$ if p is a square modulo 13; it divides $p^3 + 1$ if p is not a square modulo 13.*

(b) *If $p = 7$, there is one mep-pair for $SL(2, p)$ and the order of the elements is 8.*

(c) *If $p = 13$, there are three mep-pairs for $SL(2, p)$, the orders of the elements are 12, 7, 26.*

(d) *In the remaining cases for p there are three mep-pairs with different traces $\lambda + \lambda^{-1}$. If p is a square modulo 13, there is at least one pair with order dividing $p - 1$; if not, there is at least one pair with order dividing $p + 1$.*

(e) *Except for the third case in* (c), *where Lemma 6 applies, the (minimal) period is k if the order k of the element is even and $2k$ if k is odd.*

PROOF. – The statement (b) follows directly from $P(t) \equiv (t - 3)^3$ modulo 7,

while for statement (c) we have $P(t) \equiv (t-9)(t-8)(t+2)$ modulo 13 and $t \not\equiv -2$ since $\lambda \neq -1$. (For this case Theorem 1 applies.)

For statements (a) and (d) we state first that $t = \lambda + \lambda^{-1}$ and λ belong to the field $GF(q)$ if and only if $t^2 - 4$ is a square in $GF(q)$. If t_1, t_2, t_3 are the three zeros of $P(t)$, then $\prod(t_i^2 - 4) = 13$, and there is an odd number of squares (nonsquares) among these expressions $t_i^2 - 4$ whenever p is a square (nonsquare) modulo 13. Statement (e) follows as in Theorem 2.

REMARK. – Using the second equation in the proof of Lemma 4 we have

$$1 + \lambda^{-2} + \lambda^{-2} e(i) = a(i) + d(i).$$

So if $e(0) = e(h)$, we have by Lemma 2(2) that there is an element $u \in GL(2, q)$ commuting with y such that $[x,_h y] = u^{-1} x u$. Since the order of u is a divisor of $q-1$ (resp. of $q+1$) if the order of y is, and since it follows that $[x,_{hk} y] = u^{-k} x u^k$, we obtain a restriction for the possible periods as multiples of h and divisors of $h(q-1)$ or $h(q+1)$. In the case of Theorem 2 and of Lemma 7 we find by arguing on its order that u must be a power of y.

We close with a list of possible period lengths found with the methods indicated. The first is a list following Theorem 1

prime	5	13	29	37	41	53	61	101	109	113	137
length of period	5	26	87	222	164	636	244	2020	654	339	1096

Using Theorem 2 we find the following cases:

length of period	8	12	14	18	20	22	26	28	30	30
order of scalar field	7	13	13	8	41	43	27	29	29	29
order of elements	8	12	14	9	20	11	13	28	15	30

For elements of order 16 and 24 no examples can be found using Theorem 2.

REFERENCES

[1] R. BRANDL, *Finite Varieties*, manuscript, distributed about 1988.
[2] H. S. M. COXETER - W. O. J. MOSER, *Generators and Relations for Discrete Groups*, Berlin-Heidelberg-New York 1980.
[3] B. HUPPERT, *Endliche Gruppen I*, Berlin-Heidelberg-New York 1967.

Mathematisches Institut, Universitaet Wuerzburg, Am Hubland
97074 Wuerzburg, Germany

Pervenuta in Redazione
il 15 marzo 1999