RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

J. L. BRENNER
L. CARLITZ

Covering theorems for finite nonabelian simple groups. III. - Solutions of the equation $\alpha x^2 + \beta t^2 + \gamma t^{-2} = a$ in a finite field

Rendiconti del Seminario Matematico della Università di Padova, tome 55 (1976), p. 81-90

<http://www.numdam.org/item?id=RSMUP_1976__55__81_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 55 (1976)

Covering Theorems for Finite Nonabelian Simple Groups.

III. - Solutions of the equation $\alpha x^2 + \beta t^2 + \gamma t^{-2} = a$ in a finite field.

J. L. BRENNER - L. CARLITZ (*)

SUMMARY - Elementary arguments can be used to establish that, if $w \neq 0, \pm 2$, the class C of trace w in $G = PSL(2, q)$, q odd > 3, satisfies $CC \supset G$. A second proof is given, involving the equation of the title. The arguments do not use group characters, and hence may have application to $PSL(n, q)$. An explicit formula is given for the number of solutions of the equation in the title. (Also if q is even > 2, there are classes C such that $CC \supset G$.)

1. – Introduction.

This is one of a series of papers concerning multiplication of conjugacy classes. The existence of a class C in Alt(n) ($n > 4$) such that CC covers the group was established by Xu (1965) and Bertram (1972) in answer to a question of Brenner (1960). From this follows a theorem of Ore (1951) that every element of Alt(n) is a commutator.

1.01. THEOREM. *Let C be a conjugacy class in the group G, and let every element of G be expressible as a product of two elements of C ($CC \supset G$). Then every element of G is a commutator.*

PROOF. Let $a \in C$. From $1 \in CC$, it follows that x, y exist such that $xax^{-1} \cdot yay^{-1} = 1$, so that $a^{-1} = y^{-1}xax^{-1}y$. Now let $g = zaz^{-1} \cdot waw^{-1}$. Set $d = zaz^{-1}$, $f = wy^{-1}xz^{-1}$, and note $g = dfd^{-1}f^{-1}$.

In many matrix groups, it is known that every element is a com-

---

(*) Indirizzo degli AA.: JLB: 10 Phillips Rd, Palo Alto, Cal. USA 94303 - LC: Duke University, Durham, N. C., USA 27706.

mutator. See Thompson (1961), Ree (1964). The stronger statement that a conjugacy class C exists such that CC covers the group seems difficult to establish, although this property may well be enjoyed by all known finite nonabelian simple groups. In some infinite groups, even infinite simple groups, there is no such class (Brenner, 1960, 1973).

If the character table for a group is given explicitly, it can be determined whether the class C has this property by noting whether every one of the sums $\sum_{\chi} \chi(C)\chi(C)\chi(C_j)/\chi(1)$, taken over all irreducible characters, is nonzero. But for some groups, or series of groups, the character table is not likely ever to become available with the required degree of explicitness. Further, it is not necessary to compute a character table to settle the covering question.

In this article, the existence of such a class C in $PSL(2, q)$ is established; in fact every class of trace $\neq 0, \pm 2$ has the covering property. Further if $q \equiv 1 \bmod 4$, but not if $q \equiv 3 \bmod 4$, the class of trace 0 has the property.

We give two direct proofs (not involving characters). The first is extremely elementary, using only first principles. The second proof uses character sums over a finite field. Although less elementary, this proof has the likely advantage of being extendable to the groups $PSL(n, q)$.

In the latter group, the class C of $I +$ superdiag $[1, 1, \ldots, 1]$ probably satisfies $CC \supset G$. In fact, it can be shown that CC contains every triangular matrix with 1's on the diagonal. The class of a (circulant) permutation matrix may also have this property.

2. – Preliminary lemmas.

The group $SL(2, q)$ consists of all 2×2 matrices of determinant 1, with elements from the finite field F_q of q elements. $PSL(2, q)$ is the central quotient group; the center has order 2 if q is odd; for $q > 3$, $PSL(2, q)$ is a simple group.

Two matrices of the same trace $\neq \pm 2$ are necessarily conjugate in $SL(2, q)$. If -1 is a square, there is a single class of noncentral matrices for each of the traces $2, -2$. If -1 is a nonsquare, the noncentral matrices of the same trace (2 or -2) separate into the two conjugacy classes represented by N, N' in $SL(2, q)$ $[N = (0, 1; -1, \pm 2)]$. In $PSL(2, q)$, every element, and hence every conjugacy class, can be represented by a pair $(M, -M)$. See Dickson (1900).

3. – The covering theorems.

Let $R = (r, s; t, u)$ denote the 2×2 matrix with first row (r, s) and second row (t, u). First, a negative result.

3.01. THEOREM. *Let M have trace 0, $q \equiv 3 \bmod 4$. There is no matrix R in $SL(2, q)$ such that $\tau = \text{trace } MRMR^{-1}$ is ± 2.*

PROOF. If $M = (0, 1; -1, 0)$ and $\tau = \pm 2$, then $(rt + su)^2 = -(t^2 + u^2 + 1)^2$; this is impossible, since -1 is a nonsquare.

3.02. COROLLARY. If $q \equiv 3 \bmod 4$, the class C of trace 0 in $G = PSL(2, q)$ does not satisfy $CC \supset G$.

3.03. LEMMA. Let $M = (0, 1; -1, w)$, $R = (r, s; t, u)$, $\det R = 1$. Then $\tau = \text{trace } MRMR^{-1}$ can be written

$$\tau = \{\xi_1^2 - (w^2 - 4)\xi_2^2 - 2\}\,, \tag{3.04}$$

where

$$\xi_1 = s - (g-1)/s + \tfrac{1}{2}w(r - g/r)\,, \tag{3.05}$$

$$\xi_2 = \tfrac{1}{2}(r + g/r)\,, \qquad g = ru\,, \tag{3.06}$$

and where it is understood that g/r means 0 if $r = 0$, and $(g-1)/s$ means 0 if $s = g - 1 = 0$. Further, the $(1, 2)$ element of $MRMR^{-1}$ is $-r\big(s - (g-1)/s\big) + s(r + g/r) + wg$.

3.07. LEMMA (Dickson, p. 46). If w, W are fixed, $w \neq \pm 2$, there always exist numbers v, V such that

$$v^2 - (w^2 - 4)V^2 = -W + 2\,.$$

3.08. LEMMA. If ξ_1, ξ_2 are defined as in (3.05), (3.06), and if w, W are preassigned, $w \neq \pm 2$, a matrix $R = (r, s; t, u)$ exists with $\det R = 1$ such that

$$\xi_1^2 - (w^2 - 4)\xi_2^2 = -w + 2\,. \tag{3.09}$$

PROOF. In view of lemma 3.07, it is only necessary to show that, with v, V determined, numbers r, s can be found so that $\xi_1 = v$, $\xi_2 = V$.

All solutions of $\xi_2 = V$ are given by taking $g = V^2 - z^2$, $r = z + V$, where z^2 runs through the squares. To solve the equation $\xi_1 = v$ for s, it is necessary to select z so that $(\frac{1}{4}w^2 - 1)[z - wv/(w^2-4)]^2 + V^2 - -1 - \frac{1}{4}w^2v^2/(w^2-4)$ is a square; this condition can always be met.

3.10. COROLLARY TO 3.03. If $w = \pm 2$, the class C of M in either $G = SL(2, q)$ or $PSL(2, q)$ does *not* satisfy $CC \supset G$.

3.11. THEOREM. *Let $w^2 - 4$ be a nonsquare. Then the class C of M in $G = SL(2, q)$ does not satisfy $CC \supset G$.*

PROOF. This also follows from lemma 3.03, with some additional calculation. It turns out that if $\tau = 2$, and thus $\xi_1 = \xi_2 = 0$, then $MRMR^{-1}$ must be the identity matrix.

The failure to cover in $SL(2, q)$ is healed by the process of taking quotients: in $PSL(2, q)$, trace 2 is the same as trace -2. Let w be arbitrary $\neq \pm 2$. There are two separate lines of argument, according as $w^2 - 4$ is a square or a nonsquare.

3.12. THEOREM. *Let $w^2 - 4 = z^2 \neq 0$. The class C of $M = (0, 1; -1, w)$ in $G = PSL(2, q)$ satisfies $CC \supset G$.*

PROOF. In view of lemma 3.08, it is only necessary to show that r, s, g can be found so that $\tau = -2$, (3.04), and so that the $(1, 2)$ element of $MRMR^{-1}$ is a nonzero square [nonsquare].

To achieve $\tau = -2$, try to solve $\xi_2 = 0$, $\xi_1 = 2$. All solutions of $\xi_2 = 0$ are given by $g = -r^2$, where r is arbitrary. Thus $r - g/r = = -2r$ (even when $g = r = 0$), and $\xi_1 = 2$ requires that

$$[s - (1 - \tfrac{1}{2}wr)]^2 = \tfrac{1}{4}z^2[r - 2w/z^2]^2 - w^2/z^2 . \tag{3.13}$$

This will have a solution if the right member is a square X^2. To arrange this, set

$$\tfrac{1}{2}z[r - 2w/z^2] + X = \varrho , \qquad \tfrac{1}{2}z[r - 2w/z^2] - X = w^2/\varrho z^2 , \tag{3.14}$$

where ϱ is an arbitrary nonzero number. All solutions of (3.13) thus arise from

$$r = \varrho/z + w^2/\varrho z^3 + 2w/z^2 .$$

From lemma 3.03, the $(1, 2)$ element of $MRMR^{-1}$ is $-2r = -(2/\varrho z)$.

$\cdot(\varrho + w/z)^2$. It is clear that nonzero ϱ can be chosen different from $-w/z$ so that this is (a) a nonzero square, (b) a nonsquare.

REMARK. All solutions of $\tau = -2$ can be parametrized, and the number of solutions counted, by an extension of the above elementary methods.

3.15. THEOREM. *Let $w^2 - 4$ be a nonsquare, $w \neq 0$. The conclusion of theorem* 3.12 *holds.*

The proof is omitted; but see Dickson, p. 46.

4. – The second proof.

In this section, an approach is given that establishes the covering, but that cannot be extended to compute the Burnside covering constants γ_{ijk}, as the first proof can be. Although the calculations involve fewer parameters, the underlying field (number) theory is deeper. This second approach uses either a lemma from number theory that appears to be new, or, in another modification, a device that should be applicable to the covering question in $PSL(n, q)$, where detailed enumeration of conjugacy classes is impossible.

The basic idea is to use only those matrices $R = (r, s; t, u)$ for which $r = 0$. Set $R = (0, -t^{-1}; t, x - \frac{1}{2}w(t + t^{-1}))$, $M = (0, 1; -1, w)$.

4.01. LEMMA. The trace τ of $MRMR^{-1}$ is given by $-\tau = x^2 - \frac{1}{4} \cdot (w^2 - 4)(t^2 + t^{-2}) - \frac{1}{2}w^2$, and the (1, 2) element is $-xt^{-1} + \frac{1}{2}w(1 + t^{-2})$.

4.02. LEMMA. Let $w^2 - 4 = \delta^2$ be a nonzero square; M, R as above. Then $MRMR^{-1}$ covers all classes.

PROOF. Set $x = \frac{1}{2}\delta(t + t^{-1})$. Then $\tau = 2$, and the (1, 2) element $\frac{1}{2}t^{-2}(\delta - w)(t^2 + 1)$ can be a nonzero square or a nonsquare by choice of t (this is an elementary result).

For $q > 7$, the remainder of the proof follows from the next lemma.

4.03. LEMMA. Let α, β, γ be nonzero, and let a be arbitrary, $q > 7$.

i) if $a^2 - 4\beta\gamma \neq 0$, the equation

$$\alpha x^2 + \beta t^2 + \gamma t^{-2} = a \tag{4.04}$$

has a solution (x, t).

ii) If $a^2-4\beta\gamma=0$, (4.04) has a solution unless $-\beta\alpha$ and $2a\beta$ are both nonsquares, in which case there is no solution.

There is no loss of generality in assuming $\alpha=1$. [Multiply (4.04) by α and set $X=\alpha x$.]

From $\beta t^2+\gamma t^{-2}=a-x^2$, we conclude that $(\beta t^2-\gamma t^{-2})^2=(a-x^2)^2-4\beta\gamma$. This shows that there is no solution unless $(a-x^2)^2-4\beta\gamma$ can be a square. All solutions of

$$(a-x^2)^2-4\beta\gamma=v^2 \tag{4.05}$$

are given by writing

$$a-x^2+v=\varrho\,,$$

$$a-x^2-v=\sigma\,,$$

where $\sigma=4\beta\gamma/\varrho$. Thus

$$\beta t^2+\gamma t^{-2}=\tfrac{1}{2}(\varrho+\sigma)\,; \qquad \beta t^2-\gamma t^{-2}=\tfrac{1}{2}(\varrho-\sigma)\,.$$

Thus it is necessary that $\varrho=2\beta t^2$, so that $2\beta\varrho=z^2$ must be a square. Furthermore, the relation

$$a-x^2=\tfrac{1}{2}(\varrho+4\beta\gamma/\varrho)$$

must have a solution x. Solving this for x^2, it is seen that

$$4x^2=-\beta\{(z^2/\beta-2a)^2-4(a^2-4\gamma\beta)\}/z^2$$

must be a square (for some choice of z). The conclusion ii) of the lemma follows at once. (If $a^2=4\beta\gamma$, set $z^2=2a\beta$, $x=0$, $\varrho=\sigma=a$. Also if $a^2=4\beta\gamma$, $-\beta=\xi^2$, take z arbitrary, set $x=\tfrac{1}{2}\xi(z^2/\beta-2a)/z$, $y=\tfrac{1}{2}z/\beta$.)

If $a^2-4\beta\gamma\neq 0$, it remains to be shown that $z\neq 0$ can be chosen in such a way that the quartic $\{\ \}$ in z has the same quadratic character as $-\beta$.

To see this let θ, $\varkappa$, λ, μ be arbitrary nonzero numbers. We assert that if $q>7$, there is a $z\neq 0$ and that $\theta[(\varkappa z^2-\lambda)^2-\mu]$ is a square. It is enough to show that for every ξ, $\eta\neq 0$, there is a $z\neq 0$ such that $(z^2-\xi)^2-\eta$ is a square [nonsquare]. This can be verified directly for $q=9, 11, 13$. Take $q>13$. Let ψ be the quadratic character in F_q, i.e. $\psi(y)=0, 1, -1$ according as y is 0, a nonzero square, or a non-

square in F_q. Consider

$$\begin{aligned}\Sigma_1 &= \sum_{z\neq 0} \psi((z^2-\xi)^2-\eta) \\ &= -\psi(\xi^2-\eta) + \sum_y (1+\psi(y))\psi((y-\xi)^2-\eta) \\ &= -\psi(\xi^2-\eta) + \Sigma_2 + \Sigma_3 ,\end{aligned}$$

where

$$\Sigma_2 = \sum_y \psi((y-\xi)^2-\eta) = -1 ,$$

$$\Sigma_3 = \sum_y \psi(y[(y-\xi)^2-\eta]) ,$$

and (Weil)

$$|\Sigma_3| \leqq 2q^{\frac{1}{2}} .$$

Hence $|\Sigma_1| \leqq 2(1+q^{\frac{1}{2}})$. If every term in Σ_1 were a nonsquare [square], the relation $|\Sigma_1| = q-1$ [or $\leqq q-5$] would hold, since $(z^2-\xi)^2-\eta = 0$ has at most four solutions. This establishes the assertion, and with it, lemma 4.03 and theorem 3.12. (For $q = 5, 7$ special formulas have to be given, to show that there is a class C such that $CC \supset G$. Note that the class C of trace 0 has this property if $q \equiv 1 \bmod 4$.)

Another proof of lemma 4.03 is given in the next section.

5. – The number of solutions of $\alpha x^2 + \beta t^2 + \gamma t^{-2} = a$ in a finite field.

Another way to establish lemma 4.03 is to give a formula for the number of solutions. Since this result and the method of obtaining it are interesting in themselves, details are given here, together with a generalization. A critique of the various methods ends this article.

5.01. THEOREM. Let $\alpha, \beta, \gamma \neq 0$. The number of solutions of $N = N(a)$ of

$$\alpha x^2 + \beta t^2 + \gamma t^{-2} = a \tag{5.02}$$

(in the finite field F_q of q elements) is given by the formula

$$N = q - 1 - \psi(-\alpha\gamma) + \psi(-\alpha)\sum_y \psi(\beta y^4 - a y^2 + \gamma) ; \tag{5.03}$$

if $a^2 = 4\beta\gamma$ this reduces to

$$N = (1 + \psi(-\alpha\beta))(q-1) - \psi(-\alpha\gamma) - \psi(-2\alpha a)\,, \tag{5.04}$$

where $\psi(z)$ is the quadratic character of z.

Let $\alpha = \beta = \gamma = 1$; the proof in the more general case is analogous.

Let $N(a)$ denote the number of solutions (x, y) of

$$x^2 + y^2 + \frac{1}{y^2} = a \qquad (a \in F_q)\,,$$

where q is odd but otherwise arbitrary. Put $q = p^n$, where p is an odd prime and define

$$t(a) = a + a^p + \ldots + a^{p^{n-1}}\,, \qquad e(a) = e^{2\pi i t(a)/p}\,.$$

Thus $t(1) = n$. Also let $\psi(a)$ denote the quadratic character, that is

$$\psi(a) = \begin{cases} 1 & \text{if } a = b^2,\ b \in F_q,\ b \neq 0 \\ -1 & \text{if } a \text{ is not a square in } F_q \\ 0 & \text{if } a = 0\,. \end{cases}$$

Put

$$G(a) = \sum_x \psi(x)\, e(ax) = \sum_x e(ax^2)\,,$$

all sums being over F_q. Then

$$G(a) = \psi(a) G(1)\,; \qquad G^2(1) = \psi(-1)\, q\,.$$

The analysis continues with the equalities

$$qN(a) = \sum_\beta \sum_x \sum_{\nu \neq 0} e\left(\beta\left(x^2 + y^2 + \frac{1}{y^2} - a\right)\right) =$$

$$= q(q-1) + \sum_{\beta \neq 0} \sum_x e(\beta x^2) \sum_{y \neq 0} e\left(\beta\left(y^2 + \frac{1}{y^2} - a\right)\right) =$$

$$= q(q-1) + G(1) \sum_{\beta \neq 0} \psi(\beta) \sum_{y \neq 0} e\left(\beta\left(y^2 + \frac{1}{y^2} - a\right)\right).$$

Now

$$\sum_{\beta\neq 0}\psi(\beta)\sum_{y\neq 0}e\left(\beta\left(y^2+\frac{1}{y^2}-a\right)\right)=\sum_{y\neq 0}\sum_{\beta\neq 0}\psi(\beta)\,e\left(\beta\left(y^2+\frac{1}{y^2}-a\right)\right)=$$

$$=\sum_{y\neq 0}\sum_{\beta\neq 0}\psi(\beta)\,e\big(\beta(y^4-ay^2+1)\big)=\sum_{y\neq 0}\psi(y^4-ay^2+1)\cdot G(1)\,.$$

Thus

$$qN(a)=q(q-1)+G(1)^2\sum_{y\neq 0}\psi(y^4-ay^2+1)\,;$$

$$N(a)=q-1+\psi(-1)\sum_{y\neq 0}\psi(y^4-ay^2+1)\,. \tag{5.05}$$

Formula (5.03) is just (5.05) with the term for $y=0$ added and subtracted.

If $\alpha=\beta=\gamma=1$, then $N(2)=2q-4$ if $q\equiv 1 \bmod 4$, but $N(2)=2$ if $q\equiv 3 \bmod 4$. Also, $N(-2)=\big(1+\psi(-1)\big)(q-2)$ in both cases. These results are in evident agreement with (5.04).

The following extension of Theorem 5.01 will be useful in studying $PSL(n, q)$.

5.06. THEOREM. *The number of solutions of*

$$x_1^2+\ldots+x_{2s+1}^2+y^2+y^{-2}=a \tag{5.07}$$

in F_q, q odd, is

$$N(a)=q^{2s}(q-1)+\psi\big((-1)^{s+1}\big)\,q^s\sum_{y\neq 0}\psi(y^4-ay^2+1)\,.$$

For simplicity, the coefficients of (5.07) are taken as 1. The method used to obtain this result is not applicable if the number of x_i is even.

The proof of Theorem 5.06 is similar to the proof of Theorem 5.01.

Critique of the various proofs. Our first is so explicit that it can enumerate the covering constants. The second proof cannot do this, but is still elementary, and can certainly yield (5.03) and (5.04); in fact not only the number of solutions N, but the actual solutions themselves are obtained. However this method apparently will not yield Theorem 5.06, one of the tools we hope to apply in studying $PSL(n, q)$.

REFERENCES

BERTRAM E. A. (1972), *Even permutations as a product of two conjugate cycles*, J. Comb. Theory (A), **12**, pp. 368-380.

BRENNER J. L. (1960), *Research problem in group theory*, Bull. Amer. Math. Soc., **66**, p. 275; (1973) *Covering theorems for finite nonabelian simple groups* - IV, *Jñānabha*, Section A, pp. 77-84.

BURNSIDE W. (1895), *Theory of groups of finite order*, Cambridge University Press.

DICKSON L. E. (1900), *Linear groups*, Berlin, Teubner, reprinted Dover, 1958.

ORE O. (1951), *Some remarks on commutators*, Proc. Amer. Math. Soc., **2**, pp. 307-314.

REE R. (1964), *Commutators in semisimple algebraic groups*, Proc. Amer. Math. Soc., **15**, pp. 457-460.

SIMPSON W. A. - FRAME J. S. (1973), *The character tables for* $SL(3, q)$, $SU(3, q^2)$, $PSL(3, q)$, $PSU(3, q^2)$, Can. J. Math., **25**, pp. 486-494.

THOMPSON R. C. (1961), *Commutators in the special and general linear groups*, Trans. Amer. Math. Soc., **101**, pp. 16-33.

WEIL A. (1941), *On the Riemann hypothesis in function fields*, Proc. Nat. Acad. Sci., **27**, pp. 345-347.

XU C.-H. (1965), *The commutators of the alternating group*, Sci. Sinica, **14**, pp. 339-342.

Manoscritto pervenuto in redazione il 1° aprile 1975.