BULL. AUSTRAL. MATH. SOC. 20G40
VOL. 14 (1976), 371-377.

On conjugacy classes in certain isogenous groups

T.A. Ketter and G.I. Lehrer

We give some results on the number of G-orbits $(G = \mathrm{GL}(n, q))$ on groups isogenous (in the algebraic-geometric sense) to $\mathrm{SL}(n, q)$. The conjectured isogeny invariance of this number is contradicted by computer calculations.

Introduction and notation

Let G be the group $\mathrm{GL}(n, q)$ of non-singular matrices over $\mathrm{GF}(q)$. For each divisor d of $(q-1)$ define the group P_d as follows: let S_d be the unique subgroup of G which contains $\mathrm{SL}(n, q)$ and has index d in G; if $d' = (q-1)/d$ take $P_d = S_d/Z_{d'}$, where $Z_{d'}$ is the unique subgroup of $Z(G)$ of order d'. The following duality theorem was proved in [3].

THEOREM. *G acts by conjugation on P_d and has the same number of orbits on P_d and P_e if $de = (q-1)$.*

We shall denote the number of G-orbits on P_d by N_d.

It was remarked in [3] that one might expect to be able to prove the related result that G has the same number of orbits on all groups in the isogeny class of $\mathrm{SL}(n, q)$. The main purpose of this note is to report that some computer studies have been carried out and show that the isogeny-invariance of the number of orbits may or may not occur, and so is not a theorem. In this note we tabulate the results, give an indication of the

Received 9 February 1976.

https://doi.org/10.1017/S0004972700025259 Published online by Cambridge University Press

methods used in the computation and prove a result about F^* orbits of irreducible polynomials over a finite field F which expedites the computation.

Isogenous groups

The groups isogenous to $SL(n, q)$ arise as follows: let $\overline{S} = SL(n, \overline{F})$ where $\overline{F}$ is the algebraic closure of $GF(q)$ and let σ be the Frobenius q-automorphism of $\overline{F}$; denote by σ also the endomorphism $(a_{ij}) \to \left(a_{ij}^q\right)$ of $\overline{S}$. The centre Z of $\overline{S}$ is cyclic, of order n. Hence for each d dividing n, Z has a unique subgroup D of order d, and we have an isogeny (rational surjection with finite central kernel) $\pi : \overline{S} \to \overline{S}/D$. Since $\sigma(D) \leq D$, σ acts on $\overline{S}/D$ and we define P_D as the group $(\overline{S}/D)_\sigma$ of σ-fixed points of $\overline{S}/D$. Thus $P_Z = PGL(n, q)$ and $P_1 = SL(n, q)$. While it is not true that P_D is always isomorphic to one of the groups P_f (in contradiction of the statement in [3]; an example is P_D where $|D| = 2$, $n = 4$, and $q = 5$ - one obtains a split extension of $SL(4, 5)/D$ which is not isomorphic to P_2), one always has $|P_D| = |SL(n, q)|$ (see [1]) and one can often compute the number of G-orbits on P_D $(G = GL(n, q))$ in terms of the N_f. We give below a selection of precise results (all easy to prove), relevant to the present work ($\overline{G}$ is $GL(n, \overline{F})$ and $\overline{Z}$ is the centre of $\overline{G}$).

LEMMA 1. *For $x \in \overline{S}$, the following are equivalent:*

(i) xD *is* σ-*fixed;*

(ii) $x^\sigma = xz$ *with* $z \in D$,

(iii) $\exists z \in \overline{Z}$ *with* $z^{(q-1)d} = 1$ *such that* $xz \in G$.

Moreover if $e = n/d$ *and* $e|(q-1)$ *these conditions are equivalent to*

(iv) $\exists z \in \overline{Z}$ *such that* $xz \in S_e$ (see Introduction).

For simplicity, we assume henceforth that n divides $(q-1)$. We then have (using Lemma 1)

https://doi.org/10.1017/S0004972700025259 Published online by Cambridge University Press

PROPOSITION 2. *Let* $\bar{Z}_d = \{z \in \bar{Z} \mid z^{d(q-1)} = 1\}$ *and define* $\bar{G}_d = G\cdot\bar{Z}_d$. *Then*

$$P_D = (\bar{S}/D)_\sigma \cong (\bar{G}_d \cap \bar{S})/D .$$

Now $\bar{G}_d \cap \bar{S}$ is an extension of degree d of S, but is not in general isomorphic to $S_{(q-1)/d}$ (for example, $q = 5$, $n = 4$, $d = 2$). By selecting coset representatives for S in $\bar{G}_d \cap \bar{S}$ appropriately and combining with Lemma 1 ((*iii*) and (*iv*)) one can show:

PROPOSITION 3. *The number of* G*-classes in* $(\bar{G}_d \cap \bar{S})/D$ *is equal to* $\frac{1}{m}\#$ (G *classes of* S_e/D), *where* $m = (q-1)/n$.

If $(d, m) = 1$, coset representatives for $S_{(q-1)/d}$ in S_e can be chosen from $Z(S_e) = Z(G) = \tilde{Z}$ (say). Thus we have:

COROLLARY 3'. *If* $n \mid (q-1)$ *and* $(d, m) = 1$ *(where* $|D| = d$ *and* $m = (q-1)/n$ *) then* $\#(G\text{-classes of } P_D) = \#(G\text{-classes of } P_{(q-1)/d}) = N_d$.

On the other hand if Y is the subgroup of $Z(G)$ of order $(q-1)/e$ $(e = n/d)$, then provided $(e, m) = 1$, $Y \cap \tilde{Z} = D$. Hence no element of Y/D fixes any G-class of S_e/D (any element of $Z(G)$ fixing a G-class must be in $\tilde{Z}/D$). We deduce:

COROLLARY 3". *If* $n \mid (q-1)$ *and* $(e, m) = 1$ *(where* $d = |D|$, $e = n/d$ *and* $m = (q-1)/n$ *) then*

$$\#(G\text{-classes of } P_D) = \#(G\text{-classes of } P_e) = N_e .$$

Putting these two corollaries together we obtain:

COROLLARY 3"'.. *With notation as above, if* $(n, m) = 1$ *then* $N_d = N_e$.

We shall refer to Corollaries 3' and 3" in the section presenting the results.

https://doi.org/10.1017/S0004972700025259 Published online by Cambridge University Press

METHOD

Let $\mathcal{F}$ denote the set of irreducible polynomials over $F = \mathrm{GF}(q)$. The number N_d of G-orbits on P_d is computed as the number of orbits of a subgroup of F^* acting on Φ, a certain set of partition-valued functions on $\mathcal{F}$. The reader is referred to [3] for details and notation. We recall that if K is a finite extension of F, then an irreducible polynomial over F may be identified with its set of roots in K, which forms a σ-orbit, σ being the Frobenius automorphism $a \mapsto a^q$ of K. Now F^* acts on $\mathcal{F}$ in a degree-preserving fashion by taking $\langle a \rangle$ to $\langle \alpha a \rangle$ for $a \in K$, $\alpha \in F^*$. Thus F^* acts contragrediently on Φ, taking $\lambda \in \Phi$ to λ^α, where $\lambda^\alpha(f) = \lambda(f^\alpha)$. Let $d|(q-1)$ and let H be the subgroup of F^* of order $e = (q-1)/d$. We then have

$$\#\{G\text{-orbits on } P_d\} = \#\{H\text{-orbits } H\lambda \text{ on } \Phi : \delta(\lambda) \in H\} = N_d .$$

For precise definitions of Φ and δ, see [3]. N_d is computed by dividing the functions $\lambda \in \Phi$ into types which are preserved by the F^* action. These types are equivalent to those discussed by Green in [2]. To compute the number of H orbits of a given type, the following algorithm is used.

(1) Order the functions in the type in some fashion.

(2) Taking each function with determinant (that is, δ value) in H in order, generate its H orbit.

(3) Inspect the orbit for any function previous to the present function and discard the orbit if one appears.

(4) Find the size of the orbit for verification purposes and record the orbit.

We conclude this section by proving a result which makes it possible to confine attention to functions taking non-zero values only on polynomials of degree less than n (in the case $\mathrm{GL}(n, q)$). Let K be a finite extension of $F = \mathrm{GF}(q)$ (as above) of degree n. Let N_{KF} be the norm function $N_{KF} : K^* \to F^*$. For an irreducible polynomial (that is, σ-orbit) $f = \langle a \rangle$ in K define $\delta(f) = N_{KF}(a)$ (assume $a \neq 0$).

https://doi.org/10.1017/S0004972700025259 Published online by Cambridge University Press

PROPOSITION. *Let* H *be any subgroup of* F^* *and let* F_H *be the set of* H*-orbits of irreducible polynomials* f *in* K^* *such that* $\delta(f) \in H$. *Then* $|\mathsf{F}_H|$ *is independent of* H .

Proof. Consider the complex character group $(K^*/H)^\wedge \cong K^*/H$. We compute $[(K^*/H)/(F^*/H)]^\wedge$ in two different ways. Now

$$[(K^*/H)/(F^*/H)]^\wedge \cong \{\chi \in (K^*/H)^\wedge : \chi(F^*/H) = 1\}$$

$$= \left\{\chi \in (K^*/H)^\wedge \middle| \chi^{(q^n-1)/(q-1)} = 1 \in (K^*/H)^\wedge\right\} = \{\alpha \in K^*/H | \delta(\alpha) \in H\} .$$

Note that K^*/H is the group of H-orbits in K^* . On the other hand $(K^*/H)/(F^*/H) \cong K^*/F^*$, whence $K^*/F^* \cong \{\alpha \in K^*/H | \delta(\alpha) \in H\}$.

Now σ acts on these (isomorphic) groups, and the set of σ-orbits on the right hand side is F_H , while that on the left is F_{F^*} . Thus $|\mathsf{F}_H| = |\mathsf{F}_{F^*}|$ for each H and the result follows.

Results

Computer studies were done for the cases $n = 4$ with $q = 5, 13$, and $n = 6$ with $q = 7$ and 13 . If $|D| = d$ $(D \leq Z)$ we write M_d for the number of G-orbits on P_D (see above) and for $f|(q-1)$, N_f is the number of G-orbits on P_f . From Corollary 3''' we have that $M_1 = M_4 = N_1 = N_4$ and $M_2 = N_2$ for $n = 4$ and $q = 5$ or 13 . Similarly for $n = 6$, $q = 7$ we have $M_1 = N_1 = N_6 = M_6$, and $M_2 = M_3 = N_2 = N_3$. By Corollaries 3' and 3'', for $n = 6$, $q = 13$ we have $M_1 = N_1$, $M_2 = N_3 = M_3$, $M_6 = N_{12} = N_1 = M_1$. The N_f were also computed for $n = 4$, $q = 17$ but these do not yield the M_d here (as was erroneously stated in Corollary A' of [3]).

The results are as follows (making use of the observations above to relate the N_f to the M_d).

https://doi.org/10.1017/S0004972700025259 Published online by Cambridge University Press

$GL(4, 5)$: $N_1 = N_4 = 163$,

$N_2 = 168$,

$M_1 = M_4 = 163$,

$M_2 = 168$.

$GL(4, 13)$: $N_1 = N_3 = N_4 = N_{12} = 2395$,

$N_2 = N_6 = 2408$,

$M_1 = M_4 = 2395$,

$M_2 = 2408$.

$GL(4, 17)$: $N_1 = N_{16} = 5239$,

$N_2 = N_8 = 5258$,

$N_4 = 5260$.

$GL(6, 7)$: $N_1 = N_2 = N_3 = N_6 = 19674$,

$M_1 = M_2 = M_3 = M_6 = 19674$.

$GL(6, 13)$: Let c be the number of irreducible polynomials f of degree 6 over $GF(13)$ such that $\delta(f) = 1$. Then

$$N_1 = N_3 = N_4 = N_{12} = 335460 + c ,$$

$$N_2 = N_6 = 335644 + c ,$$

$$M_1 = M_6 = 335460 + c ,$$

$$M_2 = M_3 = 335644 + c .$$

The orbits of the irreducible polynomials as well as their sizes and the sizes of the G-classes were also computed and tabulated for verification purposes.

References

[1] Armand Borel, *Linear algebraic groups* (Benjamin, New York, Amsterdam, 1969).

[2] J.A. Green, "The characters of the finite general linear groups", *Trans. Amer. Math. Soc.* 80 (1955), 402-447.

[3] G.I. Lehrer, "Characters, classes, and duality in isogenous groups", *J. Algebra* 36 (1975), 278-286.

Department of Pure Mathematics,
University of Sydney,
Sydney,
New South Wales.

https://doi.org/10.1017/S0004972700025259 Published online by Cambridge University Press