Real and strongly real classes in $SL_n(q)$

Journal Item

How to cite:

Gill, Nick and Singh, Anupam (2011). Real and strongly real classes in SLn(q). Journal of Group Theory, 14(3) pp. 437–459.

For guidance on citations see FAQs.

Version: Version of Record

Link(s) to article on publisher's website:
http://dx.doi.org/doi:10.1515/JGT.2010.054

(054)

J. Group Theory ▌ (2010), 1–23
DOI 10.1515/JGT.2010.054

Journal of Group Theory

Real and strongly real classes in $\mathrm{SL}_n(q)$

Nick Gill and Anupam Singh

(Communicated by W. M. Kantor)

Abstract. We classify the real and strongly real conjugacy classes in $\mathrm{GL}_n(q)$ and $\mathrm{SL}_n(q)$. In each case we give a formula for the number of real, and the number of strongly real, conjugacy classes.

This paper is the first of two that together classify the real and strongly real classes in $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, $\mathrm{PSL}_n(q)$, and all quasi-simple covers of $\mathrm{PSL}_n(q)$.

1 Introduction

Let G be a group. An element g of G is called *real* if there exists $h \in G$ such that $hgh^{-1} = g^{-1}$. If h can be chosen to be an involution (i.e. $h^2 = 1$) then we say that g is *strongly real*. In all cases we say that h is a *reversing element* for g. If g is real (resp. strongly real) then all conjugates of g are real (resp. strongly real), hence we talk about *real classes* and *strongly real classes* in G.

Tiep and Zalesski [9] have listed all quasi-simple groups of Lie type for which every element is real. In this paper we generalize one part of the work of Tiep and Zalesski by identifying exactly which conjugacy classes are (strongly) real in the quasi-simple groups which cover $\mathrm{PSL}_n(q)$; furthermore we count these classes.

This paper is structured as follows: in Section 2 we outline results concerning a special class of polynomials. In Section 3 we use information from Section 2 to classify the real and strongly real classes in $\mathrm{GL}_n(q)$. While this work is not new, the theory that we develop in the process of studying $\mathrm{GL}_n(q)$ forms the foundation for the rest of the paper. In Sections 4 to 6 we classify the real and strongly real classes in $\mathrm{SL}_n(q)$.

In a companion paper to this one [1] we classify the real and strongly real elements in $\mathrm{PGL}_n(q)$, $\mathrm{PSL}_n(q)$ and those quasi-simple groups which cover $\mathrm{PSL}_n(q)$. To understand reality in $\mathrm{PGL}_n(q)$ and $\mathrm{PSL}_n(q)$ we need to study the ζ-*real elements* in $\mathrm{GL}_n(q)$ and $\mathrm{SL}_n(q)$; the ζ-real elements are defined in Section 2 of this paper, and we will study them in parallel with real elements throughout Sections 3 to 5.

Sections 4 to 6 all include a theorem at the end, which summarizes the main results of the section. An interesting consequence of this paper and [1] is the following statement, the proof of which is scattered throughout the two papers.

Theorem 1.1. *Let G be isomorphic to* $\mathrm{GL}_n(q)$, $\mathrm{PGL}_n(q)$, *or a cover of* $\mathrm{PSL}_n(q)$. *Then all real elements are strongly real if and only if G is in the following list*:

(1) $\mathrm{GL}_n(q)$;

(2) $\mathrm{PGL}_n(q)$;

(3) $\mathrm{SL}_n(q)/Y$ *with* $n \not\equiv 2 \pmod 4$ *or q even*; *here Y is any central subgroup in* $\mathrm{SL}_n(q)$;

(4) $\mathrm{SL}_n(q)/Y$ *with* $n \equiv 2 \pmod 4$ *and* $q \equiv 1 \pmod 4$, *here Y is any even order central subgroup in* $\mathrm{SL}_n(q)$;

(5) $\mathrm{PSL}_2(q)$;

(6) $3.\mathrm{PSL}_2(9)$.

As we have mentioned, the work on $\mathrm{GL}_n(q)$ is not new: Gow has already enumerated the real classes for $\mathrm{GL}_n(q)$ and given a generating function for this count [2]. The work on $\mathrm{SL}_n(q)$ is partially new; a version of Proposition 4.4, which deals with the case when $n \not\equiv 2 \pmod 4$ or $q \not\equiv 3 \pmod 4$, was first proved by Wonenburger [10]. Results concerning the remaining case, when $n \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$, are new.

2 Self-reciprocal and ζ-self-reciprocal polynomials

As we shall see, real elements in $\mathrm{GL}_n(q)$ will turn out to correspond to sequences of self-reciprocal polynomials. In this section we define what a self-reciprocal polynomial is and we gather together some basic facts about such polynomials.

We also introduce the notion of a ζ-real element in H, a subgroup of $\mathrm{GL}_n(q)$, as follows: fix ζ, a non-square in $\mathbb{F}_q$. We say that g is *ζ-real* in H if $tgt^{-1} = g^{-1}(\zeta I)$ for some $t \in H$; we say that g is *strongly ζ-real* if t can be taken to be an involution. Once again we say that t is a *reversing element* for g. The ζ-real elements of $\mathrm{GL}_n(q)$ will turn out to be of vital importance when we come to examine the real elements of $\mathrm{PGL}_n(q)$ and $\mathrm{PSL}_n(q)$ in [1]. Note that we will sometimes abuse notation and, for an element $g \in \mathrm{GL}_n(q)$, write ζg when we mean $(\zeta I)g$.

It turns out that ζ-real elements will correspond to sequences of ζ-self-reciprocal polynomials. Thus in this section we also examine these polynomials. Throughout what follows ζ is a fixed non-square of $\mathbb{F}_q$.

2.1 Definitions. Consider a polynomial $f(t) \in \mathbb{F}_q[t]$ of degree d with roots $[\alpha_1, \dots, \alpha_d]$ in $\overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$. We say that $f(t)$ is *self-reciprocal* if

$$[\alpha_1, \dots, \alpha_d] = [\alpha_1^{-1}, \dots, \alpha_d^{-1}].$$

We say that $f(t)$ is *ζ-self-reciprocal* if

$$[\alpha_1, \dots, \alpha_d] = [\zeta\alpha_1^{-1}, \dots, \zeta\alpha_d^{-1}].$$

For both definitions, by $[\,, \dots, \,]$ we mean an unordered list of roots, taken with multiplicity. Note that, since ζ is a non-square in $\mathbb{F}_q$, when we talk about ζ-self-reciprocal polynomials we assume that q is odd.

(AutoPDF V7 31/8/10 11:14) WDG (170×240mm) Tmath J-2340 JGT, : () PMU: C(C) 18/8/2010 pp. 1–23 2340_054 (p. 2)

2.2 Self-reciprocal polynomials. We are interested in T_d, the set of self-reciprocal degree d polynomials in $\mathbb{F}_q[t]$ with constant term equal to 1.

It is easy enough to prove that $T_d = F_d \cup G_d$ where

$$F_d = \{f(t) = t^d + a_1 t^{d-1} + a_2 t^{d-2} + \cdots + a_2 t^2 + a_1 t + 1\},$$
$$G_d = \{g(t) = -t^d + a_1 t^{d-1} - a_2 t^{d-2} + \cdots + a_2 t^2 - a_1 t + 1\},$$

and the a_i vary over $\mathbb{F}_q$. Note that if q is even then F_d and G_d coincide. We define $n_{q,d}$ to be the number of self-reciprocal polynomials f in $\mathbb{F}_q[t]$ of degree d which satisfy $f(0) = 1$.

Lemma 2.1. *The number $n_{q,d}$ is given in the following table*:

	q *is odd*	q *is even*
d *is odd*	$2q^{(d-1)/2}$	$q^{(d-1)/2}$
d *is even*	$(q+1)q^{d/2-1}$	$q^{d/2}$

Before we leave self-reciprocal polynomials we make one more definition. Let $p(t) = t^n + a_1 t^{n-1} + \cdots + a_n$ be a monic polynomial over k. We define $\tilde{p}(t) = a_n^{-1} t^n p(t^{-1})$; this is the monic polynomial whose roots are precisely the inverse of the roots of $p(t)$. Thus a monic polynomial $p(t)$ is self reciprocal if and only if $p(t) = \tilde{p}(t)$. Note too that $p(t)$ is irreducible in $k[t]$ if and only if $\tilde{p}(t)$ is irreducible in $k[t]$.

2.3 ζ-self-reciprocal polynomials. Let q be odd and let f be a ζ-self-reciprocal polynomial with roots in $[\alpha_1, \ldots, \alpha_d] \in \overline{\mathbb{F}_q}$. Suppose that

$$\alpha_i = \zeta \alpha_j^{-1}, \quad \alpha_j = \zeta \alpha_k^{-1}.$$

Clearly $\alpha_i = \alpha_k$. Thus the roots of f can be partitioned into subclasses of size at most 2. Observe that, within these subclasses, $\alpha_i \alpha_j = \zeta$. Now if the subclass is of size 1 then $\alpha_i^2 = \zeta$ and so does not lie in $\mathbb{F}_q$. We conclude that d must be even.

Now, for d even, define the set S_d to be the union of the following two sets:

$$\left\{ f(t) = \frac{1}{\zeta^{d/2}} t^d + a_1 \frac{1}{\zeta^{d/2-1}} t^{d-1} + a_2 \frac{1}{\zeta^{d/2-2}} t^{d-2} + \cdots + a_2 t^2 + a_1 t + 1 \right\},$$
$$\left\{ g(t) = -\frac{1}{\zeta^{d/2}} t^d + a_1 \frac{1}{\zeta^{d/2-1}} t^{d-1} - a_2 \frac{1}{\zeta^{d/-2}} t^{d-2} + \cdots + a_2 t^2 - a_1 t + 1 \right\},$$

where the a_i vary over $\mathbb{F}_q$. For d odd, define S_d to be empty.

(AutoPDF V7 31/8/10 11:14) WDG (170×240mm) Tmath J-2340 JGT, : () PMU: C(C) 18/8/2010 pp. 1–23 2340_054 (p. 3)

Lemma 2.2. *The set S_d is precisely the set of ζ-self-reciprocal polynomials of degree d with constant term equal to* 1. *Moreover*, $|S_d| = n_{q,d}\sigma_d$ *where σ_d equals* 1 *if d is even and* 0 *otherwise*.

Proof. Let $h(t)$ be a polynomial of degree d and write the list of roots for $h(t)$ as $[\alpha_1, \dots, \alpha_d]$. Clearly $t^d h(\zeta/t)$ is a polynomial of degree d and its list of roots is $[\zeta\alpha_1^{-1}, \dots, \zeta\alpha_d^{-1}]$. Thus $h(t)$ will be ζ-self-reciprocal if and only if $h(t)$ is equal to a scalar multiple of $t^d h(\zeta/t)$.

Examining $f(t)$ and $g(t)$ given in the form above in S_d we observe that $f(t) = (t^d/\zeta^{d/2})f(\zeta/t)$, while $g(t) = -(t^d/\zeta^{d/2}g(\zeta/t)$; hence all elements of S_d are indeed ζ-self-reciprocal.

We must now show that S_d contains all ζ-self-reciprocal polynomials. Let $h(t)$ be a ζ-self-reciprocal polynomial and consider the roots $[\alpha_1, \dots, \alpha_d]$ of $h(t)$ split into subclasses of size at most 2 as described above.

Let us consider the subclasses of size 1; these have form $\{\alpha\}$ where $\alpha^2 = \zeta$. There are an even number of these. What is more, since α is a root of $f(t)$, so is α^q. As $\alpha^{q^2} = \alpha \in \mathbb{F}_{q^2}$ this yields a pairing on the set of subclasses of size 1. Thus we can join subclasses of form $\{\alpha\}$ and $\{\alpha^q\}$ together, so that all subclasses have size 2. Note, moreover, that if $\alpha^2 = \zeta$, then

$$\alpha^q = (\alpha^2)^{(q-1)/2}\alpha = \zeta^{(q-1)/2}\alpha = -\alpha;$$

thus in this case our subclass has form $\{\alpha, -\alpha\}$.

In general then our subclasses satisfy either $\alpha_i\alpha_j = \zeta$ or $\alpha_i\alpha_j = -\zeta$, and in the latter case $\alpha_i = -\alpha_j$. Let us consider these two cases. Firstly if $\alpha_i\alpha_j = \zeta$ then we can multiply the corresponding linear factors, $t - \alpha_i$ and $t - \alpha_j$, to obtain an $\mathbb{F}_q$-scalar multiple of

$$\frac{1}{\zeta}t^2 + at + 1$$

where $a \in \overline{\mathbb{F}_q}$. Alternatively, if $\alpha_i = -\alpha_j^{-1}$ and $\alpha_i\alpha_j = -\zeta$, then multiplying the corresponding linear factors yields an $\mathbb{F}_q$-scalar multiple of

$$-\frac{1}{\zeta}t^2 + 1.$$

If we multiply such pairs together we generate polynomials of the following forms:

$$f(t) = \frac{1}{\zeta^{d/2}}t^d + a_1\frac{1}{\zeta^{d/2-1}}t^{d-1} + a_2\frac{1}{\zeta^{d/2-2}}t^{d-2} + \dots + a_2t^2 + a_1t + 1,$$

$$g(t) = -\frac{1}{\zeta^{d/2}}t^d + a_1\frac{1}{\zeta^{d/2-1}}t^{d-1} - a_2\frac{1}{\zeta^{d/2-2}}t^{d-2} + \dots + a_2t^2 - a_1t + 1,$$

(AutoPDF V7 31/8/10 11:14) WDG (170×240mm) Tmath J-2340 JGT, : () PMU: C(C) 18/8/2010 pp. 1–23 2340_054 (p. 4)

for some $a_i \in \overline{\mathbb{F}_q}$. Now $h(t)$ is of this form and lies in $\mathbb{F}_q[t]$; in other words, for $h(t)$, the coefficients a_i lie in $\mathbb{F}_q$ and we have the required form.

The formula for the size of S_d is an easy consequence of its definition. $\square$

We make one more definition: for $p(t)$ a monic polynomial of degree d in $k[t]$, define $\check{p}(t)$ to be the monic polynomial which is a scalar multiple of $t^d p(\zeta/t)$. Clearly $p(t)$ will be ζ-self-reciprocal if and only if $p(t) = \check{p}(t)$.

3 Background information and $\mathrm{GL}_n(q)$

We start by collecting some basic facts which we will need in the sequel. Recall that, for g an element of a group G, we denote the centralizer of g by $C_G(g)$. We define the *reversing group* of g,

$$R_G(g) = \{h \in G \mid hgh^{-1} = g \text{ or } hgh^{-1} = g^{-1}\}.$$

When $G \leqslant \mathrm{GL}_n(\mathbb{F})$, for some field $\mathbb{F}$, we define a related group: fix ζ to be a non-square in k and let

$$R_{G,\zeta}(g) = \{h \in G \mid hgh^{-1} = g \text{ or } hgh^{-1} = \zeta g^{-1}\}.$$

It is easy to check that $R_G(g)$ and $R_{G,\zeta}(g)$ are indeed groups and that they contain $C_G(g)$, the centralizer of g in G, as a subgroup of index at most 2. In fact, if $g^2 \neq 1$, the index of $C_G(g)$ in $R_G(g)$ (resp. $R_{\zeta,G}(g)$) is 2 if and only if g is real (resp. ζ-real) in G; in this case $R_G(g) \backslash C_G(g)$ (resp. $R_{G,\zeta}(g) \backslash C_G(g)$) is the set of all reversing elements for g.

When G is a subgroup of $\mathrm{GL}_n(\mathbb{F})$ we can use the *Jordan decomposition* of elements of $\mathrm{GL}_n(\mathbb{F})$. We need only a few basic facts about it (more details can be found in [8, p. 20]). Any element $g \in \mathrm{GL}_n(\mathbb{F})$ can be written uniquely as $g = g_s g_u$ where g_s is a semi-simple element, g_u is a unipotent element and $g_s g_u = g_u g_s$. We have the following generalization of [7, Lemma 2.2.1]:

Lemma 3.1. *Let $g = g_s g_u$ be the Jordan decomposition of g in $\mathrm{GL}_n(\mathbb{F})$. Let G be a subgroup of $\mathrm{GL}_n(\mathbb{F})$ which contains g. Then g is real (resp. ζ-real) in G if and only if g_s is real (resp. ζ-real) in G and g_u^{-1} is conjugate to $x g_u x^{-1}$ in $C_G(g_s)$ where $x g_s x^{-1} = g_s^{-1}$ (resp. $x g_s x^{-1} = \zeta g_s^{-1}$).*

Proof. We prove this statement for the situation when g is ζ-real; for the case where g is real we simply remove all instances of ζ.

Suppose that g is ζ-real. Then

$$hgh^{-1} = hg_s g_u h^{-1} = (hg_s h^{-1})(hg_u h^{-1}) = \zeta g^{-1} \tag{1}$$

for some $h \in G$. Now the Jordan decomposition of ζg^{-1} gives $(\zeta g^{-1})_s = \zeta g_s^{-1}$ and $(\zeta g^{-1})_u = g_u^{-1}$. But, since $hg_s h^{-1}$ is semi-simple and $hg_u h^{-1}$ is unipotent and they commute, we have already given a Jordan decomposition of ζg^{-1} in (1). Since this decomposition is unique we must have

$$hg_sh^{-1} = \zeta g_s^{-1} \quad \text{and} \quad hg_uh^{-1} = g_u^{-1}.$$

This implies that g_s is ζ-real, and that g_u^{-1} is conjugate to hg_uh^{-1} in $C_G(g_s)$ (in fact, in this case, the two are equal).

Now for the converse: suppose that $h \in C_G(g_s)$ satisfies $hg_u^{-1}h^{-1} = xg_ux^{-1}$. Then

$$(h^{-1}x)g(h^{-1}x)^{-1} = h^{-1}xgx^{-1}h = h^{-1}xg_sx^{-1}xg_ux^{-1}h = \zeta g_s^{-1}g_u^{-1} = \zeta g^{-1}. \quad \square$$

In the next subsection we will discuss the real conjugacy classes in $\mathrm{GL}_n(\mathbb{F})$, and we will need an understanding of Jordan canonical forms. We mention one last fact closely related to Jordan canonical forms, but of a slightly different nature. Let $g \in \mathrm{GL}_n(q)$ where q is a prime power. Write $g = g_sg_u$, the Jordan decomposition of g. To apply Lemma 3.1 we need to understand the structure of $C_G(g_s)$ for $G = \mathrm{GL}_n(q)$. We describe its structure in a particular case.

Lemma 3.2. *Take $g \in G = \mathrm{GL}_n(q)$ and suppose that the characteristic polynomial of g and the minimal polynomial of g coincide and are equal to $f(t)^r$ where $f(t)$ is an irreducible polynomial of degree d and $n = dr$. Then*

$$\mathrm{GL}_r(q^d) \cong C_G(g) \leqslant R_G(g) \leqslant \mathrm{GL}_r(q^d).\langle\sigma\rangle$$

where σ is a field automorphism of order d.

Proof. Let V_q be the vector space of dimension n over $\mathbb{F}_q$ on which $\mathrm{GL}_n(q)$ acts naturally, and let V_{q^d} be an r-dimensional vector space over $\mathbb{F}_{q^d}$. There is a natural $\mathbb{F}_q$-vector space isomorphism $\varphi : V_q \to V_{q^d}$ which induces an embedding of $\mathbb{F}_{q^d}^*$ into G (as the centre of $\mathrm{GL}(V_{q^d}) \leqslant \mathrm{GL}(V_q)$) such that g lies in $\mathbb{F}_{q^d}^*$.

Now suppose that $h \in \mathrm{GL}(V_q)$ centralizes g, i.e. $hgh^{-1} = g$. We demonstrate that h lies in $\mathrm{GL}(V_{q^d})$. It is clear, first of all, that $h(v_1 + v_2) = h(v_1) + h(v_2)$ for all $v_1, v_2 \in V_{q^d}$; this follows from the linearity of the action of h on V_q. We need to demonstrate that h preserves scalar multiplication, for scalars in $\mathbb{F}_{q^d}$.

Observe that $\langle g\rangle$ has a well-defined action on V_1 where V_1 is any 1-dimensional subspace of V_{q^d}. Again we can think of V_1 as a vector space over $\mathbb{F}_q$ or $\mathbb{F}_{q^d}$; the element $g|_{V_1}$ acts as an $\mathbb{F}_q$-vector space endomorphism with minimal polynomial $f(t)$, and as an element of $\mathbb{F}_{q^d}$ by multiplication.

Suppose that $g|_{V_1}$ fixes a proper subspace W of V_1. Let v be a non-zero vector in W and consider the elements $v, gv, g^2v, \dots$. Since these all lie in W and $\dim W = c < d$, there exist scalars $a_i \in \mathbb{F}_q$ such that

$$0 = a_0v + a_1gv + a_2g^2v + \cdots + a_cg^cv = (a_0 + a_1g + \cdots + a_cg^c)v.$$

Since $v \neq 0$ this implies that $a_0 + a_1 g + \cdots + a_c g^c = 0$ which contradicts the fact that $f(t)$ is the minimal polynomial of $g|_{V_1}$. Thus, for any $v \in V_1$, there is an $\mathbb{F}_q$-basis for V_1 of form $\{v, gv, g^2 v, \ldots, g^{d-1} v\}$.

Now take $v \in W$ and $\alpha \in \mathbb{F}_{q^d}$. Note that α commutes with g since they both lie in $\mathbb{F}_{q^d}$. Then

$$\alpha v = (b_0 v + b_1 g v + b_2 g^2 v + \cdots + b_{d-1} g^{d-1} v),$$

for some $b_0, \ldots, b_{n-1} \in \mathbb{F}_q$. This implies that, for $i = 1, \ldots, d-1$,

$$\begin{aligned} \alpha g^i v = g^i \alpha v &= g^i (b_0 v + b_1 g v + b_2 g^2 v + \cdots + b_{d-1} g^{d-1} v) \\ &= (b_0 I + b_1 g + b_2 g^2 + \cdots + b_{d-1} g^{d-1}) g^i v. \end{aligned}$$

Thus $\alpha = b_0 I + b_1 g + b_2 g^2 + \cdots b_{n-1} g^{d-1}$. Now observe that, for $h \in C_G(g)$, $v \in V$,

$$\begin{aligned} h(\alpha v) &= h(b_0 I + b_1 g + b_2 g^2 + \cdots + b_{d-1} g^{d-1}) v \\ &= (b_0 I + b_1 g + b_2 g^2 + \cdots + b_{d-1} g^{d-1}) h(v) = \alpha h(v). \end{aligned}$$

We conclude that $C_G(g) \leqslant \mathrm{GL}(V_{q^d})$. It follows immediately that

$$C_G(g) = \mathrm{GL}(V_{q^d}) \cong \mathrm{GL}_r(q^d).$$

Now we wish to study the normalizer of $C_G(g)$. Write $d = d_1 \ldots d_l$ where $d_1, \ldots, d_l$ are primes. Then $\mathrm{GL}(V_{q^d}).\langle\delta\rangle$ is a maximal subgroup of $\mathrm{GL}(V_{q^{d/d_1}})\langle\delta_1\rangle$ where δ (resp. δ_1) is a field automorphism of $\mathrm{GL}(V_{q^d})$ (resp. $\mathrm{GL}(V_{q^{d/d_1}})$) of order d (resp. d/d_1). (Details can be found in [4, §4.3]; see, in particular, [4, p. 116].) Similarly $\mathrm{GL}(V_{q^{d/d_1}})\langle\delta_1\rangle$ is a maximal subgroup of $\mathrm{GL}(V_{q^{d/(d_1 d_2)}})\langle\delta_2\rangle$ where δ_2 is a field automorphism of $\mathrm{GL}(V_{q^d})$ of order $d/(d_1 d_2)$, and so on. We conclude that $C_G(g)$ is normal in $\mathrm{GL}_r(q^d).\langle\sigma\rangle$ where σ is a field automorphism of $\mathrm{GL}(V_{q^d})$ of order d.

Therefore $N_{\Gamma L_n(q)}(C_G(g))$ must contain $\mathrm{GL}_r(q^d).\langle\bar{\sigma}\rangle$ where $\bar{\sigma}$ is a field automorphism of $\mathrm{GL}_r(q^d)$ of order $d \log_p q$. Now any element of $\Gamma L_r(q^d)$ which normalizes $C_G(g)$ must normalize $\mathbb{F}_{q^d}^* = Z(C_G(g))$ and so must induce a field automorphism on $\mathbb{F}_{q^d}$; these are all accounted for and so we conclude that $N_{\Gamma L_n(q)}(C_G(g)) = \mathrm{GL}_r(q^d).\langle\bar{\sigma}\rangle$. Therefore $N_G(C_G(g)) = \mathrm{GL}_r(q^d).\langle\sigma\rangle$, as required. $\square$

Note that, in the language of Jordan canonical forms, g is semi-simple and conjugate to a Jordan block matrix. Note too that we could replace $R_G(g)$ with $R_{G,\zeta}(g)$ in the statement of the lemma and it would remain true. Finally observe that, for g to be real (resp. ζ-real) in $\mathrm{GL}_n(q)$, we must have d even and $x(g) = g^{-1}$ (resp. $x(g) = (\zeta I)g^{-1}$) where x is a field automorphism of $\mathrm{GL}_r(q^d)$ of order 2.

3.1 Real conjugacy classes in $\mathrm{GL}_n(\mathbb{F})$. Let $\mathbb{F}$ be a field. The conjugacy classes in $\mathrm{GL}_n(\mathbb{F})$ are determined using the theory of Jordan canonical forms. We will assume a basic understanding of this theory (more details can be found in [3]). The theory is based upon the idea that, given an element g of $\mathrm{GL}_n(\mathbb{F})$, we can create an n-dimensional $\mathbb{F}[t]$-module V by defining a scalar multiplication,

$$t.v = gv, \quad \text{for } v \in V,$$

and extending linearly. The isomorphism classes of V constructed in this way are in one-to-one correspondence with the conjugacy classes of $\mathrm{GL}_n(\mathbb{F})$. They are also in one-to-one correspondence with the set of all multi-sets of form

$$\{f_1(t)^{a_1}, \ldots, f_r(t)^{a_r}\}$$

where, for $i = 1, \ldots, r$, $f_i(t)$ is a monic irreducible polynomial in $\mathbb{F}[t]$ which is not equal to t, a_i is a positive integer, and $\sum_{i=1}^r \deg(f_i)a_i = n$. These correspondences allow us to classify conjugacy in $\mathrm{GL}_n(q)$.

Before we state the main result that we shall need, we introduce some notation. A *partition* v of n is a finite multi-set of positive integers $v = \{v_1, \ldots, v_r\}$ that sums to n; we say $|v| = n$. Write $v = 1^{n_1}2^{n_2}3^{n_3}\ldots$ to mean that

$$n = \underbrace{1 + \cdots + 1}_{n_1} + \underbrace{2 + \cdots + 2}_{n_2} + \cdots.$$

The following theorem is classical.

Theorem 3.3. *Let g be an element of $\mathrm{GL}_n(\mathbb{F})$. The $\mathrm{GL}_n(\mathbb{F})$-conjugacy class of g is the $\mathrm{GL}_n(\mathbb{F})$-conjugacy class of the matrix $\bigoplus_p J_{v_p,p}$ where the sum is over all irreducible factors p of the minimal (or characteristic) polynomial. Here $v_p = \{r_1, \ldots, r_k\}$ is a partition, and $\sum_p |v_p| \deg(p) = n$; the matrix $J_{v,p}$ is $J_{r_1,p} \oplus \cdots \oplus J_{r_k,p}$ where each $J_{r_i,p}$ is a Jordan block matrix involving a companion matrix corresponding to p.*

This theorem allows us to construct the multi-set which corresponds to the conjugacy class of g. It is simply $\bigcup_{p(t)}\{p(t)^{r_1}, \ldots, p(t)^{r_k}\}$ where the union is taken over all irreducible factors of the characteristic polynomial of g.

To classify real conjugacy classes of $\mathrm{GL}_n(\mathbb{F})$, first we need to look at a Jordan block. Recall that, for a monic irreducible polynomial $p(t)$, $\tilde{p}(t)$ is the monic irreducible polynomial whose roots are the inverses of the roots of $p(t)$.

Lemma 3.4. *Let $p(t)$ be an irreducible polynomial of degree d. Then $J_{r,p}^{-1}$ is conjugate in $\mathrm{GL}_{rd}(\mathbb{F})$ to $J_{r,\tilde{p}}$, while $\zeta J_{r,p}^{-1}$ is conjugate in $\mathrm{GL}_{rd}(\mathbb{F})$ to $J_{r,\breve{p}}$.*

Proof. The theory of Jordan canonical forms tells us that $J_{r,p}^{-1}$ and $\zeta J_{r,p}^{-1}$ must be conjugate in $\mathrm{GL}_{dr}(\mathbb{F})$ to Jordan block matrices. Now the characteristic polynomial of $J_{r,p}$ is $p(t)^r$ and so, by considering roots, the characteristic polynomial of $J_{r,p}^{-1}$ must be $\tilde{p}(t)^r$. Thus $J_{r,p}^{-1}$ is conjugate to $J_{r,\tilde{p}}$ as required. Similarly, the characteristic polynomial of $\zeta J_{r,p}^{-1}$ must be $\breve{p}(t)^r$. Thus $\zeta J_{r,p}^{-1}$ is conjugate to $J_{r,\breve{p}}$ as required. □

Proposition 3.5. *A matrix $g \in \mathrm{GL}_n(\mathbb{F})$ is real if and only if g is conjugate in $\mathrm{GL}_n(\mathbb{F})$ to*

$$\left[\bigoplus_{p \neq \tilde{p}} (J_{v,p} \oplus J_{v,\tilde{p}})\right] \oplus \left[\bigoplus_{p = \tilde{p}} J_{\mu,p}\right].$$

A matrix g in $\mathrm{GL}_n(\mathbb{F})$ is ζ-real if and only if g is conjugate in $\mathrm{GL}_n(\mathbb{F})$ to

$$\left[\bigoplus_{p \neq \check{p}} (J_{v,p} \oplus J_{v,\check{p}})\right] \oplus \left[\bigoplus_{p = \check{p}} J_{\mu,p}\right].$$

Here μ and v are partitions which vary with p.

Proof. Let g, g^{-1} be conjugate to $J_g = \bigoplus_p J_{v,p}$ and $J_{g^{-1}} = \bigoplus_q J_{v,q}$ respectively. Lemma 3.4 implies that there is a matching between the Jordan blocks of J_g and $J_{g^{-1}}$ which takes $J_{r,p}$ to $J_{r,q} = J_{r,\tilde{p}}$. Similarly there is a matching between the Jordan blocks of J_g and $\zeta J_{g^{-1}}$ which takes $J_{r,p}$ to $J_{r,q} = J_{r,\check{p}}$. This yields the given formulae. □

Proposition 3.5 asserts that a matrix $g \in \mathrm{GL}_n(\mathbb{F})$ is real (resp. ζ-real) if, for any invariant factor i of g and for p irreducible in $k[t]$, p and $\tilde{p}$ (resp. $\check{p}$) occur as factors of i with the same multiplicity.

3.2 Real conjugacy classes in $\mathbf{GL}_n(q)$. We follow the notation of Macdonald in [6] where he gives another way to classify conjugacy classes; we will use Macdonald's method to give a criterion for an element of $\mathrm{GL}_n(q)$ to be real. We begin by stating Macdonald's result regarding $\mathrm{GL}_n(q)$.

Theorem 3.6 ([6, (1.8), (1.9)]). *Let C be a conjugacy class in $\mathrm{GL}_n(q)$. Then we can associate C with a sequence of polynomials $u = (u_1, u_2, \ldots)$ satisfying the following properties*:

(1) $u_i(t) = a_{n_i} t^{n_i} + \cdots + a_1 t + 1 \in \mathbb{F}_q[t]$ *for all i with* $a_{n_i} \neq 0$;

(2) $\sum_i i n_i = n$.

This gives a one-to-one correspondence between conjugacy classes in $\mathrm{GL}_n(q)$ and sequences of polynomials with the given properties.

Note that the sequence $(n_1, n_2, \ldots)$ is equivalent to a partition, $v = 1^{n_1} 2^{n_2} \ldots$, of n; the conjugacy class C described in the theorem is said to be *associated with* the partition v and an element g in C is said to be *of type v*.

We need to describe how the correspondence given in Theorem 3.6 works. Let us start with a conjugacy class C in $\mathrm{GL}_n(q)$. As we described above, this can be associated with a multi-set of polynomials,

$$\{f_1(t)^{a_1}, \ldots, f_r(t)^{a_r}\}$$

(AutoPDF V7 31/8/10 11:14) WDG (170×240mm) Tmath J-2340 JGT, : () PMU: C(C) 18/8/2010 pp. 1–23 2340_054 (p. 9)

where, for each i, $f_i(t)$ is a monic irreducible polynomial in $\mathbb{F}_q[t]$ which is not equal to t, a_i is a positive integer, and $\sum_{i=1}^r \deg(f_i)a_i = n$.

Now define

$$u_i(t) = k \prod_{\{f_j(t):a_j=i\}} f_j(t).$$

Here $k \in \mathbb{F}_q$ is chosen so that $u_i(t)$ has constant term 1. So $u_i(t)$ is simply the product of all irreducible polynomials in the multi-set which have associated exponent equal to i. That this construction gives a one-to-one correspondence with the conjugacy classes of $\mathrm{GL}_n(q)$ is the content of Theorem 3.6.

Proposition 3.7. *An element $g \in \mathrm{GL}_n(q)$ is real (resp. ζ-real) if and only if each of the polynomials u_i in the sequence $u = (u_1, u_2, \dots)$ (associated uniquely to the conjugacy class of g) are self-reciprocal (resp. ζ-self-reciprocal).*

Proof. Suppose that all of the $u_i(t)$ are self-reciprocal. This means that if $p(t)$ is a monic irreducible polynomial dividing $u_i(t)$, then either $p(t) = \tilde{p}(t)$ or $\tilde{p}(t)$ also divides $u_i(t)$ (with the same multiplicity). Each monic irreducible divisor of $u_i(t)$ corresponds to a Jordan block within the Jordan canonical form for g. Referring to Proposition 3.5 this means that g is self-reciprocal.

The converse works the same way: if g is self-reciprocal then we can apply Proposition 3.5; thus if $p(t)$ divides $u_i(t)$ then either $p(t) = \tilde{p}(t)$ or else $\tilde{p}(t)$ also divides $u_i(t)$ (with the same multiplicity). This means that the $u_i(t)$ are self-reciprocal.

The same argument applies for the ζ-real case except that we replace $\tilde{p}(t)$ in our argument with $\breve{p}(t)$. $\square$

Hence to count the number of real conjugacy classes in $\mathrm{GL}_n(q)$ we need to count sequences of polynomials

$$u = (u_1(t), \dots, u_i(t), \dots) \quad \text{such that } u_i(t) = a_i t^{n_i} + \cdots + a_1 t + 1$$

are self-reciprocal polynomials over $\mathbb{F}_q$ with constant term 1 satisfying $\sum_i in_i = n$. Thus for a given partition v we write $gl_v = \prod_{n_i>0} n_{q,n_i}$ for the number of real $\mathrm{GL}_n(q)$-conjugacy classes of type v in $\mathrm{GL}_n(q)$. Then we have

Theorem 3.8. *The total number of real conjugacy classes in $\mathrm{GL}_n(q)$ is*

$$\sum_{\{v:|v|=n\}} gl_v = \sum_{\{v:|v|=n\}} \prod_{n_i>0} n_{q,n_i}.$$

Furthermore all real classes in $\mathrm{GL}_n(q)$ are, in fact, strongly real.

We have not proved the statement about strong reality; however this follows from Corollary 4.5 which we prove later. In fact Wonenburger [10] has proved that reality is equivalent to strong reality in $\mathrm{GL}_n(\mathbb{F})$ for all fields $\mathbb{F}$ of characteristic not 2.

Gow (who effectively proved Theorem 3.8 in [2]) makes in [2, Lemma 2.2] the interesting observation that the number of equivalence classes of non-degenerate bilinear forms of rank n over $\mathbb{F}_q$ is equal to the number of real classes in $\mathrm{GL}_n(q)$; hence Theorem 3.8 also provides a formula for the number of these equivalence classes.

Note that the function $(1+t)^{(2,q-1)}/(1-qt^2)$ is a generating function for $n_{q,d}$, and so the function

$$\prod_{r=1}^{\infty} \frac{(1+t^r)^{(2,q-1)}}{1-qt^{2r}}$$

is a generating function for the number of real conjugacy classes in $\mathrm{GL}_n(q)$.

Finally, for q odd we can also write a formula for the total number of ζ-real conjugacy classes in $\mathrm{GL}_n(q)$:

$$\sum_{\{\nu:|\nu|=n\}} \prod_{n_i>0} n_{q,n_i}\sigma_{n_i}.$$

4 $\mathrm{SL}_n(q)$, $n \not\equiv 2 \pmod 4$ or $q \not\equiv 3 \pmod 4$

We count the real conjugacy classes of $\mathrm{SL}_n(q)$ using the correspondence given by Macdonald, who proves that a $\mathrm{GL}_n(q)$-conjugacy class of type $\nu = \{\nu_1, \dots, \nu_r\}$ contained in $\mathrm{SL}_n(q)$ is the union of h_ν conjugacy classes for $\mathrm{SL}_n(q)$ where $h_\nu = (q-1, \nu_1, \dots, \nu_r)$; see [6, (3.1)].

Proposition 4.1. *Let ν be a partition of n. Then the total number of $\mathrm{GL}_n(q)$-real $\mathrm{GL}_n(q)$-conjugacy classes of type ν contained in $\mathrm{SL}_n(q)$ is*

$$sl_\nu = \begin{cases} \prod_{n_i>0} n_{q,n_i}, & \text{if } q \text{ is even or } n_i \text{ is zero for } i \text{ odd};\\ \frac{1}{2}\prod_{n_i>0} n_{q,n_i}, & \text{if } q \text{ is odd and there exists } i \text{ with } in_i \text{ odd};\\ f_\nu(q) \prod_{i \text{ odd}, n_i>0} q^{n_i/2-1} \prod_{i \text{ even}, n_i>0} n_{q,n_i}, & \text{otherwise.} \end{cases}$$

Here $f_\nu(q) = \frac{1}{2}((q+1)^r + (q-1)^r)$ where r is the number of odd values of i for which $n_i > 0$.

Proof. As outlined in Section 3.2 we write $\nu = 1^{n_1}2^{n_2}\dots$ with $|\nu| = n$. Let c be a conjugacy class of $\mathrm{GL}_n(q)$ of type ν given by $u = (u_1(t), u_2(t), \dots)$ where $u_i(t) = a_i t^{n_i} + \dots + 1$. Suppose that c is real and so $u_i(t)$ is self reciprocal for all i; this means, in particular, that $a_i = \pm 1$ for all i. Now $\det(1-tg)$ is that scalar multiple of the characteristic polynomial of g for which the constant term equals 1. Thus

$\det(1-tg) = \prod_{i\geqslant 1} u_i(t)^i$ and so $\det g = (-1)^n \prod_{n_i>0} a_i^i$; see [6, (1.7)]. Thus a real element of $\mathrm{GL}_n(q)$ must have determinant ± 1. If $p=2$ this means that all real $\mathrm{GL}_n(q)$-conjugacy classes lie in $\mathrm{SL}_n(q)$.

If q is odd and n_i is zero for i odd then n is even, and $\det g = \prod_{n_i>0} a_i^i = 1$; hence, again, all real $\mathrm{GL}_n(q)$-conjugacy classes lie in $\mathrm{SL}_n(q)$.

Now suppose that q is odd and that there exists i such that in_i is odd. Lemma 2.1 implies that there are $2q^{(n_i-1)/2}$ possibilities for $u_i(t)$; half of these will have $a_i = 1$, the other half will have $a_i = -1$. Then it is easy to see that exactly half of the sequences associated to v correspond to elements with determinant 1.

Finally suppose that q is odd and that n_i is even whenever i is odd, with at least one such $n_i > 0$. Clearly n is even, so we require that $\prod_{n_i>0} a_i^i = 1$. When i is even, $a_i^i = 1$ so we must ensure that $\prod_{i\text{ odd}, n_i>0} a_i^i = 1$. So let us suppose, for the moment, that we are dealing with a sequence of length r of self-reciprocal polynomials $(u_{i_1}(t), \dots, u_{i_r}(t))$ where i_j is odd for all j and $\deg u_{i_j}(t)$ is positive and even for all j.

Lemma 2.1 implies that the number of such sequences is $(q+1)^r \prod_{i\text{ odd}, n_i>0} q^{n_i/2-1}$. Those sequences which correspond to a matrix with determinant 1 will have an even number of leading coefficients -1. Counting such sequences is equivalent to counting terms in the expansion of $(q+1)^r$ in which 1 turns up an even number of times; thus the number of such sequences is $f_v(q) \prod_{i\text{ odd}, n_i>0} q^{n_i/2-1}$; here

$$f_v(q) = a_r q^r + a_{r-2} q^{r-2} + a_{r-4} q^{r-4} + \cdots$$

where $(q+1)^r = a_r q^r + a_{r-1} q^{r-1} + \cdots + a_1 q + a_0$. It is an easy matter to see that $f_v(q) = \frac{1}{2}((q+1)^r + (q-1)^r)$.

Now, if we return to the case where n_i may be non-zero for even i, it is clear that there are $\prod_{i\text{ even}, n_i>0} n_{q,n_i}$ polynomials corresponding to even i; these make no difference to the determinant of our element, hence we obtain the given formula. □

Next we need to know how a real (resp. ζ-real) conjugacy class of $\mathrm{GL}_n(q)$ splits in $\mathrm{SL}_n(q)$.

Lemma 4.2. *Let $g \in \mathrm{SL}_n(q)$ and suppose that the conjugacy class of g in $\mathrm{GL}_n(q)$ is $C = C_1 \cup \cdots \cup C_r$ where the C_i are $\mathrm{SL}_n(q)$-conjugacy classes. Take $x_i \in \mathrm{GL}_n(q)$ such that $g^{x_i} \in C_i$ for $i = 1, \dots, r$. Then g is real (resp. ζ-real) in $\mathrm{SL}_n(q)$ if and only if g^{x_i} is real (resp. ζ-real) in $\mathrm{SL}_n(q)$ for all i.*

Proof. Suppose that $tgt^{-1} = g^{-1}$ for $t \in \mathrm{SL}_n(q)$. Then $t^x g^x (t^x)^{-1} = (g^x)^{-1}$ for $x \in \mathrm{GL}_n(q)$. Suppose $tgt^{-1} = \zeta g^{-1}$ for $t \in \mathrm{SL}_n(q)$. Then $t^x g^x (t^x)^{-1} = \zeta (g^x)^{-1}$ for $x \in \mathrm{GL}_n(q)$. (Recall that, for $g \in \mathrm{GL}_n(q)$, we write ζg when we mean $(\zeta I)g$.)

In both cases t^x is in $\mathrm{SL}_n(q)$ since $\mathrm{SL}_n(q)$ is normal in $\mathrm{GL}_n(q)$. Hence we obtain our result. □

For our analysis of the real classes in $\mathrm{SL}_n(q)$, we need an easy arithmetical lemma. We write $|k|_2$ for the largest power of 2 which divides an integer k. That is, $|k|_2 = 2^r$ where 2^r divides k, but 2^{r+1} does not.

(AutoPDF V7 31/8/10 11:14) WDG (170×240mm) Tmath J-2340 JGT, : () PMU: C(C) 18/8/2010 pp. 1–23 2340_054 (p. 12)

Lemma 4.3. *Let $\mathbb{F}_q$ be a finite field with q odd. Then there exists $\alpha \in \mathbb{F}_q^*$ with $\alpha^n = -1$ if and only if $|n|_2 < |q-1|_2$.*

Proof. Recall that $\mathbb{F}_q^*$ is a cyclic group of order $q-1$. Consider the homomorphism $\mathbb{F}_q^* \to \mathbb{F}_q^*$, $x \mapsto x^n$. Its kernel is $\{x \in \mathbb{F}_q^* \mid x^{(n,q-1)} = 1\}$, hence its image $\{x \in \mathbb{F}_q^* \mid x^r = 1\}$ has $r = (q-1)/(n, q-1)$ elements. Now -1 is contained in this image if and only if r is even or, equivalently, if and only if $|n|_2 < |q-1|_2$. $\square$

Proposition 4.4. *Suppose that $n \not\equiv 2 \pmod 4$ or that $q \not\equiv 3 \pmod 4$. Then a real (resp. ζ-real) conjugacy class of $\mathrm{GL}_n(q)$ which is contained in $\mathrm{SL}_n(q)$ is again a union of real (resp. ζ-real) conjugacy classes in $\mathrm{SL}_n(q)$.*

Proof. We generalize the proof of Wonenburger [10].

First consider the even characteristic situation. Let g be a real element in $G = \mathrm{GL}_n(q)$ (remember that, for even characteristic, ζ-real elements do not exist) and consider the group $R_G(g)$, as defined in Section 3. If g is not real in $\mathrm{SL}_n(q)$ then $R_G(g) \cap \mathrm{SL}_n(q) \leqslant C_G(g)$. This implies that $R_G(g)\,\mathrm{SL}_n(q)$ is a group which contains $\mathrm{SL}_n(q)$ with even index. But this is impossible since $R_G(g)\,\mathrm{SL}_n(q)$ is contained in $\mathrm{GL}_n(q)$ which contains $\mathrm{SL}_n(q)$ as a subgroup with odd index. We conclude that g is indeed real in $\mathrm{SL}_n(q)$.

From here on we assume that the characteristic is odd. Let $\delta_1(t), \ldots, \delta_n(t)$ be the invariant factors of g in $\mathbb{F}_q[t]$. Suppose that g is real (resp. ζ-real), so each $\delta_i(t)$ is self-reciprocal (resp. ζ-self-reciprocal). The $\mathbb{F}_q[t]$-module V which we discussed in Section 3 decomposes as $V = \bigoplus_{i=1}^n V_i$, where each V_i is a cyclic submodule of V. Write $g_i = g|_{V_i}$; then $g = \bigoplus_i g_i$ and the characteristic polynomial of g_i is the polynomial $\delta_i(t)$.

Step 1. We shall construct involutions in $\mathrm{GL}(V_i)$, conjugating g_i to g_i^{-1} (resp. ζg_i^{-1}). If $\dim V_i = 2m$ then this involution will have determinant $(-1)^m$, while if $\dim V_i = 2m+1$ then we will construct two such involutions, one of determinant 1 and the other of determinant -1. This construction is enough to prove the proposition except when $q \equiv 1 \pmod 4$ and $n \equiv 2 \pmod 4$; we deal with this exception in Step 2.

When g is real we can write the characteristic polynomial of g_i as $\chi_{g_i}(t) = (t-1)^r(t+1)^s f(t)$ where $f(\pm 1) \neq 0$ and $V_i = W_{-1} \oplus W_1 \oplus W_0$, where W_{-1}, W_1 and W_0 are the kernels of $(g_i - 1)^r$, $(g_i + 1)^s$ and $f(g_i)$ respectively. To produce the involution h_i on V_i as above, it suffices to do so on each of W_{-1}, W_1 and W_0.

When g is ζ-real we can write $\chi_{g_i}(t) = (t^2 - \zeta)^r f(t)$ where the $\deg(f) = 2m$ and $f(0) = \zeta^m$; then $V_i = W_\zeta \oplus W_0$, where W_ζ and W_0 are the kernels of $t^2 - \zeta$ and $f(t)$ respectively. To produce the involution h_i on V_i as above, it suffices to do so on each of W_ζ and W_0.

It is sufficient to find a reversing involution in the following situations. Let k be a cyclic linear transformation on a vector space W with characteristic polynomial $\chi_k(t)$, one of the following three types:

(1) $\chi_k(t)$ is self-reciprocal (resp. ζ-self-reciprocal) and the degree of $\chi_k(t)$ is even, say $2m$. In this case we deal with the ζ-real, and real, situations simultaneously. We will write the proof for the ζ-real situation; the proof for the real situation is obtained by replacing ζ with 1. We assume that $\chi_k(0) = \zeta^m$.

(2) $\chi_k(t) = (t-1)^{2m+1}$ or $(t+1)^{2m+1}$.

(3) $\chi_k(t) = (t^2 - \zeta)^m$ with m odd.

We claim that in Case 1, k is reversed by an involution with determinant $(-1)^m$; in Case 2 there are reversing involutions with determinant -1, and with determinant 1; in Case 3 there is an involution with determinant -1.

Case 1. Since $\chi_k(t)$ is ζ-self-reciprocal, our assumptions imply that

$$\chi_k(t) = t^{2m} + a_1\zeta t^{2m-1} + a_2\zeta^2 t^{2m-2} + \cdots + a_m\zeta^m t^m + \cdots + a_2\zeta^m t^2 + a_1\zeta^m t + \zeta^m.$$

Since W is cyclic, there is a vector $u \in W$ such that $\mathscr{E} = \{u, ku, \dots, k^{2m-1}u\}$ is a basis of W. By substituting $k^m u = y$ we get $\mathscr{E} = \{k^{-m}y, \dots, y, \dots, k^{m-1}y\}$. Let

$$\mathscr{B} = \{y, (k + \zeta k^{-1})y, \dots, (k^{m-1} + \zeta^{m-1}k^{-m+1})y, (k - \zeta k^{-1})y, \dots, (k^m - \zeta^m k^{-m})y\}.$$

We claim that $\mathscr{B}$ is a basis of W. To see this observe first that, for $i = 1, \dots, m-1$, $(k^i + \zeta^i k^{-i})y$ and $(k^i - \zeta^i k^{-i})y$ span the same 2-dimensional subspace as $k^i y$ and $k^{-i}y$. Also y is independent of $k^i y$ and $k^{-i}y$, hence we need only demonstrate that $(k^m - \zeta^m k^{-m})y$ is linearly independent from the rest. Were this not the case, however, we would have

$$k^m(y) = \zeta^m k^{-m}(y) + f(k^{-m+1}, k^{-m+2}, \dots, k^{m-1})(y)$$

and hence

$$(k^{2m} - f(k, k^2, \dots, k^{2m-1}) - \zeta^m)y = 0,$$

where f is some linear function. But this implies that

$$\chi_k(t) = t^{2m} - f(t^{2m-1}, t^{2m-2}, \dots, t) - \zeta^m$$

which contradicts the form of $\chi_k(t)$ given above.

We denote the subspace generated by the first m vectors of $\mathscr{B}$ by P and that by the latter m vectors by Q. Now observe some facts:

(1) $(k + \zeta k^{-1})(k^i + \zeta^i k^{-i}) = (k^{i+1} + \zeta^{i+1}k^{-(i+1)}) + \zeta(k^{i-1} + \zeta^{i-1}k^{-(i-1)})$;

(2) $(k - \zeta k^{-1})(k^i + \zeta^i k^{-i}) = (k^{i+1} - \zeta^{i+1}k^{-(i+1)}) - \zeta(k^{i-1} - \zeta^{i-1}k^{-(i-1)})$;

(3) $(k - \zeta k^{-1})(k^i - \zeta^i k^{-i}) = (k^{i+1} + \zeta^{i+1}k^{-(i+1)}) - \zeta(k^{i-1} + \zeta^{i-1}k^{-(i-1)})$;

(4) $k^m + \zeta^m k^{-m} = -a_1(k^{m-1} + \zeta^{m-1}k^{-m+1}) - a_2(k^{m-2} + \zeta^{m-2}k^{-m+2}) - \cdots$.

Now (1), (2) and (4) imply that $(k + \zeta k^{-1})(P) \subseteq P$ and that $(k - \zeta k^{-1})(P) \subseteq Q$. If we apply $k - \zeta k^{-1}$ to both sides of (4) we find that $(k^{m+1} - \zeta^{m+1} k^{-m-1})(y) \in Q$. This, along with (2), implies that $(k + \zeta k^{-1})(Q) \subseteq Q$. Similarly, applying $k + \zeta k^{-1}$ to both sides of (4) we obtain $(k^{m+1} + \zeta^{m+1} k^{-m-1})(y) \in P$. This, along with (3), implies that $(k - \zeta k^{-1})(Q) \subseteq P$.

Now let $h = 1|_P \oplus -1|_Q$ and note that

$$h(k + \zeta k^{-1})h = k + \zeta k^{-1}; \quad h(k - \zeta k^{-1})h = -(k - \zeta k^{-1}).$$

This implies that h is an involution which conjugates k to ζk^{-1} and has determinant $(-1)^m$.

Case 2. In this case, we have the characteristic polynomial $\chi_k(t) = (t - \varepsilon)^{2m+1}$ where $\varepsilon = \pm 1$. Since W is cyclic, there is a vector $u \in W$ such that $\mathscr{E} = \{u, ku, \dots, k^{2m}u\}$ is a basis. By substituting $k^m u = y$ we get

$$\mathscr{E} = \{k^{-m}y, \dots, y, \dots, k^m y\}.$$

We consider the basis

$$\mathscr{B} = \{ y, (k + k^{-1})y, \dots, (k^m + k^{-m})y, (k - k^{-1})y, \dots, (k^m - k^{-m})y\}.$$

We denote the subspace generated by the first $m+1$ vectors of $\mathscr{B}$ by P and the latter m vectors by Q. Examining the equation $(k - \varepsilon I)^{2m+1} = 0$ and applying $k \pm \varepsilon I$ to both sides yields the following facts: $k + k^{-1}$ leaves P as well as Q invariant; also $(k - k^{-1})(P) \subseteq Q$ and $(k - k^{-1})(Q) \subset P$. We consider $h = 1|_P \oplus -1|_Q$ and $h' = -1|_P \oplus 1|_Q$. Then h and h' are both involutions which conjugate k to k^{-1} and they have determinants $(-1)^m$ and $(-1)^{m+1}$ respectively.

Case 3. In this case, we have the characteristic polynomial $\chi_k(t) = (t^2 - \zeta)^m$ where m is odd. Since W is cyclic, there is a vector $u \in W$ such that $\mathscr{E} = \{u, ku, \dots, k^{2m-1}u\}$ is a basis. By substituting $k^m u = y$ we get

$$\mathscr{E} = \{k^{-m}y, \dots, y, \dots, k^{m-1}y\}.$$

We consider the basis

$$\begin{aligned}\mathscr{B} = \{ y, (k - \zeta k^{-1})y, (k^2 + \zeta^2 k^{-2})y, (k^3 - \zeta^3 k^{-3})y, \dots, (k^{m-1} + \zeta^{m-1} k^{-m+1})y,\\ (k + \zeta k^{-1})y, (k^2 - \zeta^2 k^{-2})y, (k^3 + \zeta^3 k^{-3})y, \dots, (k^m + \zeta^m k^{-m})y\}.\end{aligned}$$

We denote the subspace generated by the first m vectors of $\mathscr{B}$ by P and the latter m vectors by Q. This time $k - \zeta k^{-1}$ leaves P as well as Q invariant. Also $(k + \zeta k^{-1})(P) \subseteq Q$ and $(k + \zeta k^{-1})(Q) \subseteq P$. Define $h = 1|_P \oplus -1|_Q$ and observe that h is an involution which conjugates k to ζk^{-1} and which has determinant $(-1)^m$.

(AutoPDF V7 31/8/10 11:14) WDG (170×240mm) Tmath J-2340 JGT, : () PMU: C(C) 18/8/2010 pp. 1–23 2340_054 (p. 15)

Step 2. Write $g = \bigoplus_i g_i$, as above; the construction outlined in Step 1 yields a reversing involution, $h = \bigoplus_i h_i$, where h_i is a reversing involution for g_i. Whenever $n \not\equiv 2 \pmod 4$ or q is even, it is easy to see that the construction in Step 1 yields an involution h which has determinant 1. We must deal with the remaining situation: when $n \equiv 2 \pmod 4$ and $q \equiv 1 \pmod 4$.

Suppose that one of the submodules V_i has odd dimension. Then we can choose h_i to have determinant 1 or -1; this ensures that we can choose h to have determinant 1 and we are done.

Suppose that all submodules V_i have even dimension, and that the reversing involution $h = \bigoplus_i h_i$ constructed in Step 1 has determinant -1. Clearly one of the submodules, V_j say, must have dimension $n_j \equiv 2 \pmod 4$. Now Lemma 4.3 implies that there is an $\alpha \in \mathbb{F}_q$ such that $\alpha^{n_j} = -1$. Then we can define

$$h' = \left(\bigoplus_{i=1, i \neq j}^{n} h_i \right) \oplus h_j(\alpha I).$$

Clearly h' is a reversing element for g and $\det h' = 1$ as required. □

Corollary 4.5. *If g is real (resp. ζ-real) in $\mathrm{GL}_n(q)$ then g is strongly real (resp. strongly ζ-real) in $\langle \mathrm{SL}_n(q), k\rangle$ for k an element of determinant -1. If, furthermore, $n \not\equiv 2 \pmod 4$ or q is even, then an involution h exists in $\mathrm{SL}_n(q)$ such that $hgh = g^{-1}$.*

Proof. Take g real (resp. ζ-real) in $\mathrm{GL}_n(q)$. Note that in the proof of Proposition 4.4, we did not use the fact that g is contained in $\mathrm{SL}_n(q)$ and, in all cases, we found a reversing element of determinant 1 or -1. In fact, in the odd characteristic case, we always found a reversing element which was an involution; this proves the first statement when the characteristic is odd.

For $n \not\equiv 2 \pmod 4$ and q odd, we were able to do better: we found an involution in $\mathrm{SL}_n(q)$ which reverses g; this proves the second statement when the characteristic is odd. The only thing left to prove is the following: if g is real in $\mathrm{GL}_n(q)$ with q even, then g is strongly real in $\mathrm{GL}_n(q)$. (This statement is strong enough because, when q is even, there are no ζ-real elements, and all involutions of $\mathrm{GL}_n(q)$ lie in $\mathrm{SL}_n(q)$.)

Take g real in $\mathrm{GL}_n(q)$ with q even. We refer to Proposition 3.5 and write g as a block matrix as follows:

$$\left[\bigoplus_{p \neq \tilde{p}} (J_{\lambda,p} \oplus J_{\lambda,\tilde{p}}) \right] \oplus \left[\bigoplus_{p = \tilde{p}} J_{\lambda,p} \right].$$

We will consider two cases:

(1) $g = J_{r,p} \oplus J_{r,\tilde{p}}$;

(2) $g = J_{r,p}$ and $p = \tilde{p}$.

In both cases p is an irreducible polynomial. Clearly if we can find an involution which reverses g in both of these cases, then we can build an involution which reverses g in general.

Consider the first case. Then g is conjugate to a matrix of form

$$g_1 = \begin{pmatrix} B & 0 \\ 0 & B^{-1} \end{pmatrix},$$

where B is a square $d \times d$ matrix with $d = \deg(p)$. Thus $hg_1h^{-1} = g_1^{-1}$ where

$$h = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

Since $h^2 = 1$, we conclude that g_1 is strongly reversible and thus so is g.

Now consider the second case. If $p = t + 1$ then g is an involution and we are done. Thus we assume that p has even degree, d. Let $g = g_s g_u$ be the Jordan decomposition. Since g is real, Lemma 3.1 implies that g_s is real. Now $C_{\mathrm{GL}_n(q)}(g_s) \cong \mathrm{GL}_r(q^d)$. We denote by x the element which reverses g; it acts as an involutory field automorphism on $\mathrm{GL}_r(q^d)$.

We can think of g as lying inside $\mathrm{GL}_r(q^d)$; then g is conjugate to an element g_1 where

$$g_1 = \begin{pmatrix} \alpha & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \alpha \end{pmatrix}, \quad g_1^{-1} = \begin{pmatrix} \alpha^{-1} & -\alpha^{-2} & \alpha^{-3} & & & \\ & \ddots & \ddots & \ddots & & \\ & & \ddots & \ddots & \alpha^{-3} \\ & & & \ddots & -\alpha^{-2} \\ & & & & \alpha^{-1} \end{pmatrix},$$

where α is an element of $\mathbb{F}_{q^d}$ which satisfies $\alpha^{q^{d/2}} = \alpha^{-1}$. Then g_1 is reversed by an element $h\sigma$ where

$$h = \begin{pmatrix} 1 & 0 & 0 & \cdots & & \\ & -\alpha^2 & \alpha^3 & -\alpha^4 & \cdots & \\ & & \alpha^4 & -2\alpha^5 & 3\alpha^6 & \cdots \\ & & & -\alpha^6 & 3\alpha^7 & \cdots \\ & & & & \ddots & \end{pmatrix}, \quad \text{i.e.} \quad h_{ij} = \begin{cases} (-1)^{j+1}\binom{j-2}{i-2}\alpha^{i+j-2}, & j \geqslant i; \\ 0, & j < i. \end{cases}$$

Here we define $\binom{k}{0} = 1$ and $\binom{k}{-1} = -1$ for k a positive integer (of course, since the characteristic is even, $h_{ij} = 0$ for many i, j). Now $(hx)^2 = hh^x$ acts trivially on $\mathrm{GL}_r(q^d)$. But this means that $(hx)^2 \in Z(\mathrm{GL}_r(q^d))$. Since $Z(\mathrm{GL}_r(q^d))$ has odd order we conclude that hx can be chosen so that $(hx)^2 = 1$. Hence g_1 is strongly real and thus so is g. $\square$

We summarize our results for real elements with the following theorem:

Theorem 4.6. *Suppose that* $n \not\equiv 2 \pmod 4$ *or* $q \not\equiv 3 \pmod 4$. *Then the total number of real conjugacy classes in* $\mathrm{SL}_n(q)$ *is equal to* $\sum_{|\nu|=n} h_\nu sl_\nu$ *where* $\nu = \{\nu_1, \dots, \nu_r\}$, $h_\nu = (q-1, \nu_1, \dots, \nu_r)$ *and the value of* sl_ν *is given in Proposition* 4.1. *Furthermore, if* $n \not\equiv 2 \pmod 4$ *or* q *is even, this is the same as the total number of strongly real conjugacy classes in* $\mathrm{SL}_n(q)$.

5 $\mathrm{SL}_n(q)$, $n \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$

In this section we assume that $n \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$, and we take $\zeta = -1$, a non-square. The formula given in Theorem 4.6 gives the number of conjugacy classes in $\mathrm{SL}_n(q)$ which are real in $\mathrm{GL}_n(q)$. Thus, in order to count the number of real conjugacy classes in $\mathrm{SL}_n(q)$, we take this formula and count how many $\mathrm{GL}_n(q)$-real conjugacy classes in $\mathrm{SL}_n(q)$ fail to be real in $\mathrm{SL}_n(q)$. Our analysis is based on the following:

Lemma 5.1. *Let* $g \in \mathrm{SL}_n(q)$. *Then* g *is real (resp.* ζ*-real) in* $\mathrm{SL}_n(q)$ *if and only if there exists a reversing element* $h \in \mathrm{GL}_n(q)$ *such that* $\det h$ *is a square in* $\mathbb{F}_q$.

Proof. Clearly if g is real (resp. ζ-real) in $\mathrm{SL}_n(q)$ then there exists a reversing element h in $\mathrm{SL}_n(q)$ and $\det h$ is a square in $\mathbb{F}_q$.

Now for the converse: suppose that there exists a reversing element $h \in \mathrm{GL}_n(q)$ such that $\det h$ is a square. For a positive integer c we have $\det h^c = (\det h)^c$ and, if c is odd, then $h^c g h^{-c} = hgh^{-1}$ and so h^c is a reversing element. Since $\det h^c = 1$ for some odd integer c, we are done. □

Now let g be a real (resp. ζ-real) element in $\mathrm{GL}_n(q)$ with reversing element $h \in \mathrm{GL}_n(q)$. In view of Lemma 5.1 we will be interested in determining whether $\det h$ is a square or a non-square in $\mathbb{F}_q$. We will use two commutative diagrams:

$$\begin{array}{ccc} \mathrm{GL}_a(\mathbb{F}_q) & \xrightarrow{i} & \mathrm{GL}_a(\overline{\mathbb{F}_q}) \\ \Big\downarrow{\scriptstyle\det} & & \Big\downarrow{\scriptstyle\det} \\ \mathbb{F}_q^* & \xrightarrow[i]{} & \overline{\mathbb{F}_q}^* \end{array} \qquad \begin{array}{ccc} \mathrm{GL}_a(q^d) & \xrightarrow{i} & \mathrm{GL}_{ad}(q) \\ \Big\downarrow{\scriptstyle\det} & & \Big\downarrow{\scriptstyle\det} \\ \mathbb{F}_{q^d}^* & \xrightarrow[N]{} & \mathbb{F}_q^*. \end{array}$$

The map i denotes a natural inclusion map. The map N is the norm map defined as follows:

$$N : C_{q^d-1} \to C_{q-1}, \quad x \mapsto x^{q^{d-1}+\cdots+q+1}.$$

The commutativity of the first diagram is obvious. The commutativity of the second is explained by the following fact: $N \circ \det : \mathrm{GL}_a(q^d) \to \mathbb{F}_q^*$, when viewed as a map from a subgroup of $\mathrm{GL}_{ad}(q)$, is multilinear, alternating (on columns) and satisfies $(N \circ \det)(I) = 1$; in other words it is a determinant and so must coincide with $\det \circ i : \mathrm{GL}_a(q^d) \to \mathbb{F}_q^*$ by [5, Proposition 4.6, p. 514].

Thanks to the given inclusion maps, there are several determinant maps applicable to any given matrix. In what follows we write $\det_{|k|}$ to specify the field k in which our image lies. Note that the form of N implies that, for $y \in \mathrm{GL}_a(q^d)$, $\det_q(y)$ is square if and only if $\det_{q^d}(y)$ is square.

We will build a reversing element for g, in a similar way to the proof of Corollary 4.5, by considering three basic cases. Let V be the $\mathbb{F}_q[t]$-module associated with V (see Section 3.1) and let $\chi_g(t)$ be the characteristic polynomial of g.

(1) V is a cyclic module for g with $\chi_g(t) = p(t) = (t \pm 1)^a$.

(2) V is a cyclic module for g with $\chi_g(t) = p(t)^a$, where $p(t)$ is a self-reciprocal (or ζ-self-reciprocal) irreducible polynomial of even degree d.

(3) $V = W_p \oplus W_q$, a module for g, such that W_p and W_q are cyclic modules with characteristic polynomials $p(t)^a$ and $\tilde{p}(t)^a$ (or $p(t)^a$ and $\check{p}(t)^a$) such that $p(t)$ is irreducible.

Lemma 5.2. *Let V be a cyclic module associated with g such that $\chi_g(t) = (t \pm 1)^a$. Suppose that h reverses g.*

(1) *If a is odd, then* $\det h$ *may be a square or a non-square in* $\mathrm{GL}_a(q)$.

(2) *If $a \equiv 0 \pmod 4$, then* $\det h$ *is a square in* $\mathrm{GL}_a(q)$.

(3) *If $a \equiv 2 \pmod 4$, then* $\det h$ *is a non-square in* $\mathrm{GL}_a(q)$.

Proof. Write g in upper triangular form. Take h such that $h^{-1}gh = g^{-1}$; then h must be upper triangular with diagonal $(\alpha, -\alpha, \alpha, -\alpha, \ldots)$. The result follows by considering the determinant. □

Lemma 5.3. *Let V be a cyclic module associated with g such that $\chi_g(t) = p(t)^a$ where $p(t)$ is an irreducible polynomial of even degree d. Suppose that h reverses g. If a is odd, then* $\det h$ *may be a square or non-square in* $\mathrm{GL}_{ad}(q)$ *while, if a is even, then* $\det h$ *is a square in* $\mathrm{GL}_{ad}(q)$.

Proof. Write $g = g_s g_u$ for the Jordan decomposition of g. In $\mathrm{GL}_d(q)$, g_s is centralized by $\mathrm{GL}_a(q^d)$ and so g_s can only be reversed by a field automorphism of $\mathrm{GL}_a(q^d)$. Let x be such a field automorphism; then $h = yx$ where y is an element of $\mathrm{GL}_a(q^d)$ which satisfies $(g_u)^{-1} = (yx)(g_u)(yx)^{-1}$ (see Lemma 3.1).

If a is odd then there is a central element in $\mathrm{GL}_a(q^d)$ which has determinant a non-square in $\mathbb{F}_q^d$. Hence $\det h$ may be a square or a non-square in $\mathrm{GL}_{ad}(q)$.

Assume that a is even. Proposition 4.4 implies that there exists a reversing element h in $\mathrm{GL}_{ad}(q)$ such that $\det h$ is a square. Any other reversing element in $\mathrm{GL}_{ad}(q)$ must equal hz where $z \in C_{\mathrm{GL}_{ad}(q)}(g)$. If z centralizes g then it centralizes g_s and we conclude that z must be an element in $\mathrm{GL}_a(q^d)$ which centralizes g_u. We write g_u as an element of $\mathrm{GL}_a(q^d)$:

$$g = \begin{pmatrix} 1 & \alpha & & \\ & \ddots & \ddots & \\ & & \ddots & \alpha \\ & & & 1 \end{pmatrix},$$

where $\alpha \in \mathbb{F}_{q^d}$. Then z must have the form

$$z = \begin{pmatrix} \beta_1 & \beta_2 & & \iddots \\ & \ddots & \ddots & \\ & & \ddots & \beta_2 \\ & & & \beta_1 \end{pmatrix}.$$

Hence, since a is even, $\det_{q^d} z$ is a square. Thus any reversing element for g in $\mathrm{GL}_{ad}(q)$ has determinant a square. $\square$

Lemma 5.4. *Let $V = W_p \oplus W_q$ be the module associated with g. Suppose that W_p and W_q are cyclic modules with characteristic polynomials $p(t)^a$ and $\tilde{p}(t)^a$ (or $\breve{p}(t)^a$). Suppose that $p(t)$ is irreducible of degree d, and that h reverses g. If a is odd then* $\det(h)$ *may be square or non-square while, if a is even, then* $\det(h)$ *is square.*

Proof. We know that g is conjugate in $\mathrm{GL}_{2ad}(q)$ to either

$$g_1 = \begin{pmatrix} B & 0 \\ 0 & B^{-1} \end{pmatrix} \quad \text{or} \quad g_2 = \begin{pmatrix} B & 0 \\ 0 & \zeta B^{-1} \end{pmatrix}.$$

By Lemma 4.2 we can assume that g is equal to g_1 or g_2. If a is odd then $\mathrm{GL}_a(q^d)$ contains a central element with non-square determinant in $\mathbb{F}_{q^d}$; since g is central in a group isomorphic to $\mathrm{GL}_a(q^d) \times \mathrm{GL}_a(q^d)$ we conclude that $\det(h)$ may be square or non-square.

Suppose that a is even. If h preserves blocks then $p = \tilde{p}$ (or $p = \breve{p}$) and Lemma 5.3 implies that $\det(h)$ is a square. Otherwise h reverses blocks and

$$h = \begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix}$$

for some X and Y in $\mathrm{GL}_{ad}(q)$. Thus

$$\begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix} \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix}^{-1} = \begin{pmatrix} C & 0 \\ 0 & B \end{pmatrix},$$

where $C = B$ in the real case, and $C = \zeta B^{-1}$ in the ζ-real case. This implies that $XCX^{-1} = C$ and $YBY^{-1} = B$; now $C_{\mathrm{GL}_{ad}(q)}(B) = C_{\mathrm{GL}_{ad}(q)}(C)$, hence we need to examine the centralizer of B in $\mathrm{GL}_{ad}(q)$.

Clearly $\det_q h = (-1)^{ad}(\det X)(\det Y) = (\det X)(\det Y)$ since a is even. Then X must lie in the centralizer of $g_u|_{W_q}$ and we have seen the form of such a centralizer in Lemma 5.3; we know that the determinant is always a square in $\mathbb{F}_{q^d}$ hence is a square in $\mathbb{F}_q$. □

This concludes our treatment of the three specific cases. We use the lemmas to build up the picture for general V.

Proposition 5.5. *Suppose that g lies in $\mathrm{SL}_n(q)$ with $n \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$. Suppose that the corresponding module V for g splits into r cyclic submodules with corresponding polynomials $p_1(t)^{a_1}, \ldots, p_r(t)^{a_r}$. If g is real in $\mathrm{GL}_n(q)$, then g is real in $\mathrm{SL}_n(q)$ if and only if a_i is odd for some i. If g is ζ-real in $\mathrm{GL}_n(q)$ then g is ζ-real in $\mathrm{SL}_n(q)$.*

Proof. Suppose first that g is real in $\mathrm{GL}_n(q)$. Let h be any element of $\mathrm{GL}_n(q)$ such that $hgh^{-1} = g^{-1}$. We can break V up into submodules of the three types listed above (call these *h-minimal*). If a_i is odd for some i then consider W, the h-minimal submodule corresponding to a_i. Lemmas 5.2 to 5.4 imply that $g|_W$ is conjugate to its inverse by elements of determinant $+1$ and -1 in $\mathrm{GL}(W)$; this property will then hold for g.

Conversely if all a_i are even then our above calculations show that, restricted to any h-minimal submodule W, $g|_W$ is conjugate to its inverse by an element of determinant $+1$ or -1 in $\mathrm{GL}(W)$, but not both. In fact, of the three types listed above, this determinant is -1 only when W is cyclic and $(p_i(t))^{a_i} = (t \pm 1)^{a_i}$ with $a_i \equiv 2 \pmod 4$ (this is also the only time when $\dim W \not\equiv 0 \pmod 4$).

Since $n \equiv 2 \pmod 4$ there will be an odd number of these -1 h-minimal submodules, thereby ensuring that g is only conjugate to its inverse by an element of determinant -1.

Now suppose that g is ζ-real and all a_i are even. This implies that the dimension of all h-minimal submodules is divisible by 4. Since $n \equiv 2 \pmod 4$ this is a contradiction. Thus a_i is odd for some i. Let W be the h-minimal submodule corresponding to a_i. Once again, Lemmas 5.2 to 5.4 imply that $g|_W$ is conjugate to its inverse by elements of determinant $+1$ and -1 in $\mathrm{GL}(W)$; this property will then hold for g. □

Corollary 5.6. *Suppose that $g \in \mathrm{SL}_n(q)$ is of type $\nu = 1^{n_1}2^{n_2}\ldots$ and is real in $\mathrm{GL}_n(q)$. Then g is real in $\mathrm{SL}_n(q)$ if and only if $n_i > 0$ for some odd i.*

Proof. We simply need to convert the criterion given by Proposition 5.5 into the language of Macdonald, as described in Section 3.2. □

We can use this corollary to count the real classes in $\mathrm{SL}_n(q)$ as follows:

Theorem 5.7. *Suppose that $n \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$. Then the total number of real conjugacy classes in $\mathrm{SL}_n(q)$ is equal to*

$$\sum_{|\nu|=n} h_\nu sl_\nu - \sum_{|\mu|=n} h_\mu sl_\mu$$

where $\nu = (1^{n_1}2^{n_2}\ldots)$, $\mu = (2^{d_2}4^{d_4}\ldots)$ and the values of sl_ν and sl_μ are given in Proposition 4.1.

6 Strongly real conjugacy classes in $\mathrm{SL}_n(q)$

Theorem 6.1. *Let g be an element of $\mathrm{SL}_n(q)$ which is real in $\mathrm{GL}_n(q)$. Let g be of type $\nu = 1^{n_1}2^{n_2}\ldots$, with associated self-reciprocal polynomials u_i of degree n_i.*

(1) *If $n \not\equiv 2 \pmod 4$ or if q is even then g is real as well as strongly real in $\mathrm{SL}_n(q)$.*

(2) *If $n \equiv 2 \pmod 4$ and q is odd then, g is strongly real in $\mathrm{SL}_n(q)$ if and only if there is an odd i for which ± 1 appears as a root of $u_i(t)$.*

Proof. The first statement follows directly from Corollary 4.5. Now suppose that $n \equiv 2 \pmod 4$ and q is odd.

Take g a strongly real element in $\mathrm{GL}_n(q)$. We use the same notation as the previous section except that this time we require that $h^2 = 1$. Let W be a h-minimal submodule of V; W will have one of the same three types as before.

Suppose that $W = W_p \oplus W_q$ where W_p and W_q are cyclic with corresponding characteristic polynomials $p(t)^a$ and $\tilde{p}(t)^a$ such that $p(t)$ and $\tilde{p}(t)$ are distinct irreducible polynomials of degree d. Then

$$h|_W = \begin{pmatrix} 0 & X \\ Y & 0 \end{pmatrix}$$

for some X and Y in $\mathrm{GL}_{ad}(q)$ and $\det h|_W = (-1)^{ad}(\det X)(\det Y)$. But, since $h^2 = 1$, we have $X = Y^{-1}$ and $\det h|_W = (-1)^{ad}$.

Suppose that W is cyclic and $d > 1$. Write the corresponding characteristic polynomial as $p(t)^a$ where $p(t)$ has even degree d. We can consider $W \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$. Then $g|_W$ is clearly real in $\mathrm{GL}(V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q})$ but is reducible. In fact there are pairings of blocks. As we have already seen, this implies that we have determinant $(-1)^b$ over these pairings, where b is the size of the block. Thus h must have determinant $(-1)^{ad/2}$.

Suppose that W is cyclic and $p(t) = t \pm 1$. It is easy to check that

(1) if a is odd then $\det h|_W$ may be 1 or -1,

(2) if $a \equiv 0 \pmod 4$ then $\det h|_W = 1$,

(3) if $a \equiv 2 \pmod 4$ then $\det h|_W = -1$.

(AutoPDF V7 31/8/10 11:14) WDG (170×240mm) Tmath J-2340 JGT, : () PMU: C(C) 18/8/2010 pp. 1–23 2340_054 (p. 22)

We have now treated the three types. If V does not have a cyclic submodule corresponding to a polynomial $(t \pm 1)^a$ where a is odd, then $\det h|_W = (-1)^{(\dim W)/2}$ and so $\det h = (-1)^{n/2} = -1$; in particular g is not strongly real in $\mathrm{SL}_n(q)$. On the other hand if V does have a cyclic submodule corresponding to a polynomial $(t \pm 1)^a$ where a is odd, then we can choose h to have $\det h = 1$.

The proof is completed once we observe that V has a cyclic submodule corresponding to a polynomial $(t \pm 1)^a$ where a is odd if and only if there is an odd i for which ± 1 is a root of $u_i(t)$. $\square$

Acknowledgement. Part of this work was completed when both authors were postdoctoral fellows at IMSc, Chennai. The first author is grateful to Ian Short, and others at the National University of Ireland, Maynooth, who took an interest in this work. Both authors would like to thank Rod Gow, Bill Kantor, and Amritanshu Prasad for helpful comments, and in addition the authors owe a large debt of gratitude to the anonymous referee; their insight has been invaluable.

References

[1] N. Gill and A. Singh. Real and strongly real classes in $\mathrm{PGL}_n(q)$ and quasi-simple covers of $\mathrm{PSL}_n(q)$. *J. Group Theory*

[2] R. Gow. The number of equivalence classes of nondegenerate bilinear and sesquilinear forms over a finite field. *Linear Algebra Appl.* **41** (1981), 175–181.

[3] N. Jacobson. *Lectures in abstract algebra*, vol. 2. *Linear algebra* (van Nostrand, 1953).

[4] P. Kleidman and M. Liebeck. *The subgroup structure of the finite simple groups*. London Math. Soc. Lecture Note Ser. 129 (Cambridge University Press, 1990).

[5] S. Lang. *Algebra*, 3rd edn. Graduate Texts in Math. 211 (Springer-Verlag, 2002).

[6] I. G. Macdonald. Numbers of conjugacy classes in some finite classical groups. *Bull. Austral. Math. Soc.* **23** (1981), 23–48.

[7] A Singh and M. Thakur. Reality properties of conjugacy classes in algebraic groups. *Israel J. Math.* **145** (2005), 157–192.

[8] T. A. Springer. Linear algebraic groups. In *Algebraic Geometry IV*, Encyclopaedia of Math. Sci. 55 (Springer-Verlag, 1994), pp. 1–121.

[9] P. H. Tiep and A. E. Zalesski. Real conjugacy classes in algebraic groups and finite groups of Lie type. *J. Group Theory* **8** (2005), 291–315.

[10] M. J. Wonenburger. Transformations which are products of two involutions. *J. Math. Mech.* **16** (1966), 327–338.

Received 20 January, 2009; revised 12 June, 2010

Nick Gill, Department of Mathematics, University Walk, Bristol, BS8 1TW, United Kingdom
E-mail: nickgill@cantab.net

Anupam Singh, IISER, Central Tower, Sai Trinity Building, near Garware Circle, Pashan, Pune 411021, India
E-mail: anupamk18@gmail.com