

NUMBERS OF CONJUGACY CLASSES IN SOME FINITE CLASSICAL GROUPS

I. G. MACDONALD

In this paper we calculate the number of conjugacy classes in the following finite classical groups: $GL_n(F_q)$; $PGL_n(F_q)$, $SL_n(F_q)$, and more generally $G(F_q)$, where G is any algebraic group isogenous to SL_n ; $PSL_n(F_q)$; $U_n(F_{q^2})$; $PU_n(F_{q^2})$, $SU_n(F_{q^2})$ and more generally $G(F_{q^2})$ where G is any group isogenous to SU_n over F_q ; and $PSU_n(F_{q^2})$.

Introduction

Let G be a semisimple algebraic group isogenous to SL_n and let k be a finite field. In this paper we calculate the number of conjugacy classes in the finite group $G(k)$ of k -rational points of G , for all choices of G and k . The result is as follows. If G is the image of SL_n under a central isogeny of degree f , and $e = n/f$, then the number of conjugacy classes in $G(k)$ is

$$(q-1)^{-1} \sum_{d_1, d_2} \phi_1(d_1) \phi_2(d_2) e_{n/d_1 d_2}$$

summed over all pairs of positive integers d_1, d_2 such that d_1 (respectively d_2) divides f and $q-1$ (respectively e and $q-1$),

Received 25 July 1980.

and the notation is as follows:- q is the number of elements in k ; c_n is the number of conjugacy classes in $GL_n(k)$; and for any positive integers n and r ,

$$\phi_r(n) = n^r \prod_{p|n} (1-p^{-r})$$

(product over the primes dividing n), so that ϕ_1 is Euler's ϕ -function.

In particular, the expression

$$(q-1)^{-1} \sum_{d|(n,q-1)} \phi_r(d) c_{n/d}$$

gives the number of conjugacy classes in $PGL_n(k)$ (respectively $SL_n(k)$) when $r = 1$ (respectively $r = 2$). These two formulas were also found by Wall [7].

For convenience of exposition, we deal with these two cases first, in §2 and §3 respectively, and the general case in §4. We also calculate in §5 the number of conjugacy classes in the simple group $PSL_n(k)$. Finally, in §6, we establish analogous formulas for unitary groups. For example, if k_2 is the quadratic extension of k and if γ_n is the number of conjugacy classes in the unitary group $U_n(k_2)$, the expression

$$(q+1)^{-1} \sum_{d|(n,q+1)} \phi_r(d) \gamma_{n/d}$$

gives the number of conjugacy classes in $PU_n(k_2)$ (respectively $SU_n(k_2)$) when $r = 1$ (respectively $r = 2$).

We conclude this introduction with a few remarks on notation and terminology. A *partition* is any finite or infinite sequence

$\lambda = (\lambda_1, \lambda_2, \dots)$ of integers such that $\lambda_1 \geq \lambda_2 \geq \dots \geq 0$ and

$|\lambda| = \sum \lambda_i < \infty$. The non-zero λ_i are called the *parts* of λ , and we

denote by $m_i(\lambda)$, for each $i \geq 1$, the number of parts λ_j equal to i .

If λ, μ are partitions, $\lambda \cup \mu$ denotes the partition for which

$m_i(\lambda \cup \mu) = m_i(\lambda) + m_i(\mu)$, and similarly for any set of partitions.

Finally, for any finite group G , we denote by $c(G)$ the number of conjugacy classes in G .

1. Conjugacy classes in $GL_n(k)$

Let $g \in GL_n(k)$. Then g acts on the vector space k^n , and hence defines on k^n a $k[t]$ -module structure (where t is an indeterminate) such that $t.v = gv$ for $v \in k^n$. Let V_g denote this $k[t]$ -module. It is clear that two elements $g, h \in GL_n(K)$ are conjugate in $GL_n(k)$ if and only if the $k[t]$ -modules V_g and V_h are isomorphic. The conjugacy classes in $GL_n(k)$ are therefore in one-one correspondence with the isomorphism classes of $k[t]$ -modules V such that

- (i) $\dim_k V = n$,
- (ii) $tv = 0$ implies $v = 0$.

Now $k[t]$ is a principal ideal domain, and therefore V_g is a direct sum of cyclic modules of the form $k[t]/(f)^m$, where $m \geq 1$ and f is an irreducible monic polynomial in $k[t]$, the polynomial t being excluded, and (f) is the ideal generated by f in $k[t]$. Let Φ denote the set of these polynomials. Then we may write

$$(1.1) \quad V_g \cong \bigoplus_{f,i} k[t]/(f)^{\lambda_i(f)}$$

where the direct sum is over all $f \in \Phi$ and integers $i \geq 1$, and the exponents satisfy $\lambda_1(f) \geq \lambda_2(f) \geq \dots \geq 0$, so that

$\lambda(f) = (\lambda_1(f), \lambda_2(f), \dots)$ is a *partition* for each $f \in \Phi$. Since

$\dim_k(k[t]/(f)^m) = m \deg(f)$, the partition-valued function λ on Φ must satisfy

$$(1.2) \quad \sum_{f \in \Phi} |\lambda(f)| \deg(f) = n .$$

The conjugacy classes of $GL_n(k)$ are thus in one-one correspondence with the partition-valued functions λ on Φ which satisfy (1.2).

For later use it is convenient to modify this parametrization. Let \bar{k} be an algebraic closure of k , and let $M = \bar{k}^*$ be its multiplicative group. The Frobenius automorphism $F : x \rightarrow x^q$ (where $q = \text{Card}(k)$) acts on M , and the roots in \bar{k} of a polynomial $f \in \Phi$ form a single F -orbit in M , and conversely. We may therefore replace λ by the partition-valued function μ on M defined by $\mu(x) = \lambda(f)$, where f is the minimal polynomial of x over k . The condition (1.2) becomes

$$(1.3) \quad \sum_{x \in M} |\mu(x)| = n$$

and moreover μ must satisfy

$$(1.4) \quad \mu(Fx) = \mu(x)$$

for all $x \in M$. The conjugacy classes in $GL_n(k)$ are now parametrized by partition-valued functions μ on M satisfying (1.3) and (1.4).

The function μ rather than λ arises when we decompose the $\bar{k}[t]$ -module $\bar{V}_g = V_g \otimes_k \bar{k}$, for we have

$$(1.5) \quad \bar{V}_g \cong \bigoplus_{x,i} \bar{k}[t]/(t-x)^{\mu_i(x)}$$

(direct sum over all $x \in M$ and $i \geq 1$).

Now define polynomials u_i by

$$(1.6) \quad u_i = \prod_{x \in M} (1-tx)^{m_i(\mu(x))}$$

where $m_i(\mu(x))$ is the number of parts equal to i in the partition $\mu(x)$, for each $i \geq 1$. Clearly $u_i(0) = 1$, and $u_i \in k[t]$ by virtue of (1.4). Moreover, if $g \in GL_n(k)$ is in the conjugacy class parametrized by μ , we have

$$(1.7) \quad \det(1-tg) = \prod_{i \geq 1} u_i(t)^i.$$

For the characteristic polynomial of g is

$$\det(t-g) = \prod_{f \in \Phi} f(t)^{|\lambda(f)|} = \prod_{x \in M} (t-x)^{|\mu(x)|}$$

and therefore

$$\det(1-tg) = \prod_{x \in M} (1-tx)^{|\mu(x)|} = \prod_{i \geq 1} u_i(t)^i .$$

The sequence of polynomials $u = (u_1, u_2, \dots)$ determines the function μ by (1.6), and hence the conjugacy class. The u_i must satisfy

$$(1.8) \quad u_i \in k[t] , \quad u_i(0) = 1 \quad (i \geq 1)$$

and

$$(1.9) \quad \sum_{i \geq 1} i \deg u_i = n$$

(by (1.3) or (1.7)). It follows that the conjugacy classes of $GL_n(k)$ are in one-one correspondence with the set of sequences $u = (u_1, u_2, \dots)$ which satisfy (1.8) and (1.9).

If $\deg(u_i) = n_i$, so that by (1.7),

$$v = (1^{n_1} 2^{n_2} \dots)$$

is a partition of n , we call v the *type* of the conjugacy class corresponding to u . In terms of μ , we have

$$(1.10) \quad v = \bigcup_{x \in M} \mu(x) .$$

The number of polynomials u_i of degree n_i which satisfy (1.8) is

$q^{n_i} - q^{n_i-1}$ if $n_i > 0$ (and is 1 if $n_i = 0$). Hence the number of conjugacy classes of type v in $GL_n(k)$ is

$$(1.11) \quad c_v = \prod_{n_i > 0} (q^{n_i} - q^{n_i-1})$$

and the total number of conjugacy classes in $GL_n(k)$ is

$$(1.12) \quad c_n = c(GL_n(k)) = \sum_{|v|=n} c_v .$$

Since $q^n - q^{n-1}$ is the coefficient of t^n in $(1-t)(1-qt)^{-1}$, if $n > 0$, it follows from (1.11) and (1.12) that the generating function for the numbers c_n is

$$(1.13) \quad C(t) = \sum_{n=0}^{\infty} c_n t^n = \prod_{r=1}^{\infty} \frac{1-t^r}{1-qt^r} .$$

This formula is due to Feit and Fine [1].

If we combine (1.13) with the well-known identity

$$\prod_{r=1}^{\infty} (1-qt^r)^{-1} = \sum_{r=0}^{\infty} q^r t^r \prod_{k=1}^r (1-t^k)^{-1} ,$$

we obtain

$$(1.14) \quad C(t) = \sum_{r=0}^{\infty} q^r t^r \prod_{k>r} (1-t^k) .$$

We can transform this further, as follows. From the identity

$$\prod_{k=1}^{\infty} (1+at^k) = \sum_{s \geq 0} a^s t^{s(s+1)/2} \prod_{j=1}^s (1-t^j)^{-1}$$

with $a = -t^r$, we obtain

$$\prod_{k>r} (1-t^k) = \sum_{s \geq 0} (-1)^s t^{rs+s(s+1)/2} \prod_{j=1}^s (1-t^j)^{-1}$$

and hence (1.14) becomes

$$\begin{aligned} C(t) &= \sum_{r=0}^{\infty} q^r \sum_{s=0}^{\infty} (-1)^s t^{(s+1)(r+s/2)} \prod_{j=1}^s (1-t^j)^{-1} \\ &= \sum_{r=0}^{\infty} \left(q^r t^r - \frac{q^r t^{2r+1}}{1-t} + \frac{q^r t^{3r+3}}{(1-t)(1-t^2)} - \dots \right) \end{aligned}$$

from which it follows that c_n is a polynomial in q of the form

$$c_n = q^n - (q^a + q^{a-1} + \dots + q^{b+1} + q^b) + \dots$$

where $a = [\frac{1}{2}(n-1)]$, $b = [\frac{1}{3}n]$, and the terms not written at the end have degree less than b . Also, from Euler's pentagonal number theorem, the constant term in c_n is 0 unless n is of the form $\frac{1}{2}m(3m+1)$ for some $m \in \mathbb{Z}$, in which case $c_n = (-1)^m$.

Finally, all the c_n ($n \geq 1$) are divisible by $q - 1$, as one sees by putting $q = 1$ in (1.13).

In Table 1 below we list the polynomials c_n for $0 \leq n \leq 12$, and in Table 2 the polynomials $c'_n = c_n/(q-1)$ for $1 \leq n \leq 12$.

TABLE 1

$$\begin{aligned} c_0 &= 1 \\ c_1 &= q - 1 \\ c_2 &= q^2 - 1 \\ c_3 &= q^3 - q \\ c_4 &= q^4 - q \\ c_5 &= q^5 - q^2 - q + 1 \\ c_6 &= q^6 - q^2 \\ c_7 &= q^7 - q^3 - q^2 + 1 \\ c_8 &= q^8 - q^3 - q^2 + q \\ c_9 &= q^9 - q^4 - q^3 + q \\ c_{10} &= q^{10} - q^4 - q^3 + q \\ c_{11} &= q^{11} - q^5 - q^4 - q^3 + q^2 + q \\ c_{12} &= q^{12} - q^5 - q^4 + q^2 + q - 1 \end{aligned}$$

TABLE 2

$$\begin{aligned}
 c'_1 &= 1 \\
 c'_2 &= q + 1 \\
 c'_3 &= q^2 + q \\
 c'_4 &= q^3 + q^2 + q \\
 c'_5 &= q^4 + q^3 + q^2 - 1 \\
 c'_6 &= q^5 + q^4 + q^3 + q^2 \\
 c'_7 &= q^6 + q^5 + q^4 + q^3 - q - 1 \\
 c'_8 &= q^7 + q^6 + q^5 + q^4 + q^3 - q \\
 c'_9 &= q^8 + q^7 + q^6 + q^5 + q^4 - q^2 - q \\
 c'_{10} &= q^9 + q^8 + q^7 + q^6 + q^5 + q^4 - q^2 - q \\
 c'_{11} &= q^{10} + q^9 + q^8 + q^7 + q^6 + q^5 - q^3 - 2q^2 - q \\
 c'_{12} &= q^{11} + q^{10} + q^9 + q^8 + q^7 + q^6 + q^5 - q^3 - q^2 + 1
 \end{aligned}$$

2. $PGL_n(k)$

The group k^* acts on $GL_n(k)$ by multiplication, and hence on the set of conjugacy classes in $GL_n(k)$. The conjugacy classes of $PGL_n(k)$ may be identified with the orbits of this action. If $\xi \in k^*$ is such that ξg is conjugate to g in $GL_n(k)$, then $\det(g) = \det(\xi g) = \xi^n \det(g)$, so that $\xi^n = 1$.

If the conjugacy class of g in $GL_n(k)$ is represented by a sequence $u = (u_1(t), u_2(t), \dots)$ of polynomials as in §1, then the conjugacy class of ξg is represented by $\xi u = (u_1(\xi t), u_2(\xi t), \dots)$.

For each d dividing n , let $\mu_d(k)$ denote the group of d th roots of unity in k . The order of $\mu_d(k)$ is

$$h_d = (d, q-1)$$

(highest common factor). A sequence $u = (u_1(t), u_2(t), \dots)$ is fixed by $\mu_d(k)$ if and only if $\xi u = u$ for all $\xi \in k^*$ such that $\xi^d = 1$, that is to say if and only if $u_i(t) \in k[t^d]$ for all i . It follows that the number of conjugacy classes in $GL_n(k)$ fixed by $\mu_d(k)$ is $c_{n/d}$, and therefore the number for which the isotropy group is exactly $\mu_d(k)$ is

$$\sum_{d'} \mu(d') c_{n/dd'}$$

where μ is the Möbius function and the sum is over all divisors d' of n/d . But if the isotropy group is $\mu_d(k)$, the number of elements in the orbit is $(q-1)/h_d$. Hence the total number of orbits, that is, the number of conjugacy classes in $PGL_n(k)$, is

$$\begin{aligned} (2.1) \quad \bar{c}_n = c(PGL_n(k)) &= \sum_d \frac{h_d}{q-1} \sum_{d'} \mu(d') c_{n/dd'} \\ &= \sum_{d, d'} h_d \mu(d') c'_{n/dd'} \end{aligned}$$

where the sum is over all pairs of positive integers d, d' such that dd' divides n .

An alternative formula for \bar{c}_n is

$$(2.2) \quad \bar{c}_n = \sum_d \phi(d) c'_{n/d}$$

where ϕ is Euler's function and the sum is over the divisors d of $(q-1, n) = h_n$.

This is a consequence of the following lemma. For each positive integer k and positive integer n we define

$$(2.3) \quad \phi_r(n) = n^r \prod_{p|n} (1-p^{-r})$$

where the product on the right is over the prime factors of n ; $\phi_r(n)$

is the number of elements of order n in the abelian group $(\mathbb{Z}/n\mathbb{Z})^r$. When $r = 1$, $\phi_1 = \phi$ is Euler's function; when $r \geq 2$, ϕ_r is Jordan's generalization of Euler's function.

(2.4) Let N be a positive integer. Then

$$\begin{aligned} \sum_{d|n} (N, d)^r \mu(n/d) &= \phi_r(n) \text{ if } n|N, \\ &= 0 \text{ otherwise.} \end{aligned}$$

Proof. The function $d \rightarrow (N, d)^r$ is multiplicative, that is, $(N, dd')^r = (N, d)^r (N, d')^r$ if $(d, d') = 1$. Hence if $n = \prod_i p_i^{v_i}$ is the prime factorization of n we have

$$\sum_{d|n} (N, d)^r \mu(n/d) = \prod_i \left[\binom{v_i}{N, p_i}^r - \binom{v_i-1}{N, p_i}^r \right].$$

If n does not divide N , at least one of the factors on the right is zero. If n divides N , the product on the right is just $\phi_r(n)$. //

If we take $r = 1$ and $N = q - 1$ in (2.4), we have

$$\begin{aligned} \sum_{d|n} h_d \mu(n/d) &= \phi(n) \text{ if } n|q-1, \\ &= 0 \text{ otherwise.} \end{aligned}$$

Substitution of this result in (2.1) gives (2.2).

From (2.2), the generating function for the numbers \bar{c}_n is (with $\bar{c}_0 = 1$)

$$(2.5) \quad \bar{C}(t) = \sum_{n=0}^{\infty} \bar{c}_n t^n = \frac{1}{q-1} \sum_{d|q-1} \phi(d) C(t^d)$$

where $C(t)$ is the generating function (1.13).

In Table 3 we list the values of \bar{c}_n for $1 \leq n \leq 10$. They are easily computed from (2.1) and Table 2.

TABLE 3

$$\begin{aligned} \bar{c}_1 &= 1 \\ \bar{c}_2 &= q + h_2 \\ \bar{c}_3 &= q^2 + q + h_3 - 1 \\ \bar{c}_4 &= q^3 + q^2 + h_2q + h_4 - 1 \\ \bar{c}_5 &= q^4 + q^3 + q^2 + h_5 - 2 \\ \bar{c}_6 &= q^5 + q^4 + q^3 + h_2q^2 + (h_2+h_3-2)q + h_6 - h_2 \\ \bar{c}_7 &= q^6 + q^5 + q^4 + q^3 - q + h_7 - 2 \\ \bar{c}_8 &= q^7 + q^6 + q^5 + q^4 + h_2q^3 + (h_2-1)q^2 + (h_4-2)q + h_8 - h_2 \\ \bar{c}_9 &= q^8 + q^7 + q^6 + q^5 + q^4 + (h_3-2)(q^2+q) + h_9 - h_3 \\ \bar{c}_{10} &= q^9 + q^8 + q^7 + q^6 + q^5 + h_2q^4 + (h_2-1)q^3 + (h_2-2)q^2 \\ &\quad + (h_5-2)q + (h_{10}-2h_2+1) \end{aligned}$$

3. $SL_n(k)$

For each partition $\nu = (\nu_1, \dots, \nu_r)$ of n , let h_ν denote the highest common factor of $q - 1$ and $\nu_1, \nu_2, \dots, \nu_r$.

(3.1) *The number of $GL_n(k)$ -conjugacy classes of type ν contained in $SL_n(k)$ is $h_\nu c'_\nu = h_\nu c_\nu / (q-1)$.*

Proof. Consider a conjugacy class c of type ν represented as in §1 by a sequence of polynomials $u = (u_1(t), u_2(t), \dots)$, where

$u_i = a_i t^{n_i} + \dots + 1$ ($a_i \in k^*$, $n_i = m_i(\nu)$). From (1.7), the class c is contained in $SL_n(k)$ (that is, its elements have determinant 1) if and only if $\prod_{i=1}^r a_i^{n_i} = (-1)^n$.

Let S be the set of positive integers i such that $n_i > 0$, so

that $s = |S|$ is the number of different parts of ν . Consider the homomorphism $\phi : (k^*)^S \rightarrow k^*$ defined by

$$(a_i)_{i \in S} \rightarrow (-1)^n \prod a_i^i .$$

If C and K are the cokernel and kernel of ϕ , the exact sequence

$$1 \rightarrow K \rightarrow (k^*)^S \rightarrow k^* \rightarrow C \rightarrow 1$$

shows that $|K| = (q-1)^{s-1} |C|$. Also C is the quotient of k^* by the subgroup generated by the i th powers for all $i \in S$, that is to say by the ν_j th powers ($1 \leq j \leq r$). Hence C is a cyclic group of order

h_ν , and so $|K| = (q-1)^{s-1} h_\nu$. It follows that the number of $GL_n(k)$ -conjugacy classes of type ν contained in $SL_n(k)$ is

$$(q-1)^{s-1} h_\nu \prod_{i \in S} q^{n_i-1} = h_\nu c_\nu / (q-1) . \quad //$$

Next we need to know how many $SL_n(k)$ -conjugacy classes are contained in a $GL_n(k)$ -class. For this purpose we shall use the following lemma:

(3.2) *Let G, H be finite groups, $\delta : G \rightarrow H$ a surjective homomorphism, K the kernel of δ . Let X be a set on which G acts. Then for each $x \in X$, the G -orbit of x in X splits up into*

$$n_x = |\text{Coker}(\delta|_{G_x})|$$

K -orbits, where G_x is the subgroup of G which fixes x .

Proof. Since K is a normal subgroup of G , the K -orbits contained in $G.x$ are permuted transitively by G , and therefore the number of them is

$$n_x = \frac{|G.x|}{|K.x|} = \frac{|G/G_x|}{|K/K_x|} = \frac{|G/K|}{|G_x/K_x|} = \frac{|H|}{|\delta(G_x)|} = |\text{Coker}(\delta|_{G_x})| ,$$

since $K_x = K \cap G_x$ is the kernel of $\delta|_{G_x}$. //

We shall apply (3.2) with $G = GL_n(k)$, $H = k^*$ and δ the determinant homomorphism (so that $K = SL_n(k)$) and $X = SL_n(k)$ with G

acting by inner automorphisms.

(3.3) Let $g \in \text{SL}_n(k)$ and let $Z(g)$ be the centralizer of g in $\text{GL}_n(k)$. If $v = (v_1, \dots, v_r)$ is the type of g , then $\det(Z(g))$ is the subgroup P_v of k^* generated by the v_1 th, ..., v_r th powers.

Proof. As in §1, let $\bar{V} = \bar{V}_g$ be the $\bar{k}[t]$ -module defined by g . We have

$$\bar{V} = \bigoplus_{x \in M} \bar{V}(x),$$

where

$$(1) \quad \bar{V}(x) \cong \bigoplus_{i \geq 1} \bar{k}[t]/(t-x)^{\mu_i(x)}$$

is the characteristic submodule of \bar{V} consisting of the elements of \bar{V} killed by some power of $t - x$.

If $h \in Z(g)$, each submodule $\bar{V}(x)$ is stable under h and therefore decomposes relative to the action of h : say

$$(2) \quad \bar{V}(x) = \bigoplus_{y \in M} \bar{V}(x, y)$$

where $\bar{V}(x, y)$ is the subspace of elements of $\bar{V}(x)$ killed by some power of $h - y$, and is a submodule of $\bar{V}(x)$ because h is a module automorphism of \bar{V} . Let $\pi(x, y)$ be the type of $\bar{V}(x, y)$, so that

$$(3) \quad \bar{V}(x, y) \cong \bigoplus_{i \geq 1} \bar{k}[t]/(t-x)^{\pi_i(x,y)}.$$

From (1), (2) and (3) it follows that

$$\mu(x) = \bigcup_{y \in M} \pi(x, y)$$

and therefore

$$(4) \quad v = \bigcup_{x \in M} \mu(x) = \bigcup_{x,y} \pi(x, y).$$

On the other hand, the determinant of $h|_{\bar{V}(x, y)}$ is

$$y^{\dim \bar{V}(x,y)} = y^{|\pi(x,y)|},$$

and therefore

$$(5) \quad \det(h) = \prod_{x,y} y^{|\pi(x,y)|} .$$

From (4) and (5) it is clear that $\det(h) \in P_\nu$, for all $h \in Z(g)$.

To show that $\det(Z(g))$ is the whole of P_ν , it is enough to show that we can choose $h \in Z(g)$ so that $\det(h) = \xi^{\nu_j}$ for any $\xi \in k^*$ and any $j \geq 1$. Suppose that $\nu_j = \lambda_i(f)$ in the notation of §1. Then V_g has a direct summand isomorphic to $k[t]/(f)^{\nu_j}$, and it is enough to produce an automorphism of this cyclic module with determinant ξ^{ν_j} . In the field $k_f = k[t]/(f)$, choose an element ζ whose norm (from k_f to k) is ξ ; if ζ is the image in k_f of a polynomial $z(t) \in k[t]$, then multiplication by $z(t)$ will induce an automorphism of $k[t]/(f)^{\nu_j}$ with the required determinant. //

From (3.2) and (3.3) it follows that each $GL_n(k)$ -conjugacy class of type ν contained in $SL_n(k)$ is the union of

$$(k^* : P_\nu) = h_\nu$$

$SL_n(k)$ -conjugacy classes. Hence from (3.1) the total number of conjugacy classes in $SL_n(k)$ is

$$(3.4) \quad \tilde{c}_n = c(SL_n(k)) = \sum_{|\nu|=n} h_\nu^2 c'_\nu .$$

Now it is clear from (1.11) that if k divides each part ν_i of ν we have $c'_\nu = c'_{\nu/k}$, where ν/k is the partition $(\nu_1/k, \nu_2/k, \dots)$. Hence if we define

$$c''_n = \sum_\nu c'_\nu$$

summed over all partitions ν of n such that the highest common factor

of v_1, v_2, \dots is 1, we have

$$c'_n = \sum_{|v|=n} c'_v = \sum_{d|n} c''_d,$$

and therefore by Möbius inversion

$$c''_n = \sum_{d|n} \mu(d) c'_{n/d}.$$

Now in (3.4) the possible values of h_v are h_d , for d dividing n , and hence (3.4) takes the form

$$\tilde{c}_n = \sum_{d|n} h_d^2 c''_{n/d};$$

that is,

$$(3.5) \quad \tilde{c}_n = \sum_{d,d'} h_d^2 \mu(d') c'_{n/dd'}.$$

Comparison of (3.5) with (2.1) shows that \tilde{c}_n is derived from \bar{c}_n by replacing each coefficient h_d by h_d^2 . Hence \tilde{c}_n for $1 \leq n \leq 10$ can be read off from Table 3.

From (3.5) and (2.4) we deduce an alternative formula for \tilde{c}_n :

$$(3.6) \quad c_n = \sum_d \phi_2(d) c'_{n/d}$$

summed over all divisors d of $(q-1, n) = h_n$. Hence the generating function for the \tilde{c}_n (with $\tilde{c}_0 = 1$) is

$$(3.7) \quad \tilde{c}(t) = \sum_{n=0}^{\infty} \tilde{c}_n t^n = \frac{1}{q-1} \sum_{d|q-1} \phi_2(d) c(t^d) - q + 2$$

(since $\sum_{d|q-1} \phi_2(d) = (q-1)^2$).

REMARKS. 1. From (3.1) it follows that the number of $GL_n(k)$ -classes contained in $SL_n(k)$ is

$$\sum_{|v|=n} h_v c'_v$$

which by the same argument that led from (3.4) to (3.5) is equal to

$$\sum_{d,d'} h_d \mu(d') c'_{n/dd'}$$

and hence is equal to \bar{c}_n : in other words, the number of $GL_n(k)$ -classes contained in $SL_n(k)$ is equal to the number of conjugacy classes in $PGL_n(k)$. This fact was first observed by Lehrer [2].

2. Instead of counting conjugacy classes we could instead have counted the irreducible representations of $SL_n(k)$, using the parametrization of [3], §5. The details are rather similar to those of this section and lead (fortunately) to the same result (3.5) or (3.6).

4. Other groups isogenous to SL_n

Let e, f be positive integers such that $ef = n$. Let A_e be the kernel of the homomorphism $\delta : GL_n \times GL_1 \rightarrow GL_1$ defined by

$$\delta(g, x) = x^{-e} \det(g) ,$$

and let B_e be the image of the homomorphism $\epsilon : GL_1 \rightarrow GL_n \times GL_1$ defined by

$$\epsilon(x) = \left(x1_n, x^f \right) .$$

Then B_e is isomorphic to GL_1 , and is a closed normal subgroup of A_e . Let $G_e = A_e/B_e$.

The mapping $g \mapsto (g, 1)$ embeds SL_n in A_e , hence defines a homomorphism $SL_n \rightarrow A_e \rightarrow G_e$, which is easily seen to be surjective, with kernel $\mu_f \cdot 1_n$, where μ_f is the group of f th roots of unity. Hence G_e is a connected algebraic group isogenous to SL_n . In particular, $G_1 = PGL_n$ and $G_n = SL_n$.

Now let k be a finite field, and consider the group $A_e(k)$ of k -rational points of the algebraic group A_e . We define the *type* of an element (g, x) in $GL_n(k) \times k^*$ (or of its conjugacy class) to be the type of g (hence a partition of n).

(4.1) For each partition $\nu = (\nu_1, \dots, \nu_r)$ of n , the number of conjugacy classes of type ν in $A_e(k)$ is

$$h_{e,\nu}^2 c_\nu,$$

where $h_{e,\nu}$ is the highest common factor of $q - 1, e$, and ν_1, \dots, ν_r .

Proof. The same argument as in (3.1) shows that the number of $GL_n(k) \times k^*$ -conjugacy classes of type ν contained in $A_e(k)$ is $h_{e,\nu} c_\nu$.

Next, by applying the lemma (3.2) to the homomorphism

$\delta : GL_n(k) \times k^* \rightarrow k^*$, we see that the $GL_n(k) \times k^*$ -conjugacy class of an element $(g, e) \in A_e(k)$ of type ν splits up into $|\text{Coker}(\delta|Z(g) \times k^*)|$ $A_e(k)$ -conjugacy classes. By (3.3), the group $\delta(Z(g) \times k^*)$ is the subgroup $P_{e,\nu}$ of k^* generated by the ν_1 th, ..., ν_r th and e th powers, and therefore

$$|\text{Coker}(\delta|Z(g) \times k^*)| = (k^* : P_{e,\nu}) = h_{e,\nu}. \quad //$$

We have now to pass from $A_e(k)$ to the group $G_e(k)$. Since B_e is connected, it follows from Lang's theorem ([5], §10) that

$G_e(k) \cong A_e(k)/B_e(k) \cong A_e(k)/k^*$. The conjugacy classes of $G_e(k)$ may

therefore be identified with the orbits of k^* acting on the set of conjugacy classes of $A_e(k)$, the action of k^* on $A_e(k)$ being given by

$$\xi.(g, x) = (\xi g, \xi^f x).$$

If $\xi \in k^*$ fixes the class of (g, x) in $A_e(k)$, we must have

$x = \xi^f x$, so that $\xi \in \mu_f(k)$. As in §2, if the conjugacy class of g in $GL_n(k)$ is represented by a sequence $u = (u_1(t), u_2(t), \dots)$ of

polynomials $u_i \in k[t]$, then the conjugacy class of ξg is represented by

$\xi u = (u_1(\xi t), u_2(\xi t), \dots)$; also $\deg u_i = m_i(v)$ where v is the type of g .

Suppose that $\mu_d(k)$, where d is a divisor of f , fixes the conjugacy class of (g, x) in $A_e(k)$. Then each u_i must be a polynomial in t^d , and therefore d divides each $m_i(v)$. Let $d \setminus v$ denote the partition of n/d such that $m_i(d \setminus v) = m_i(v)/d$. Since v and $d \setminus v$ have the same parts (with different multiplicities), we have $h_{e,v} = h_{e,d \setminus v}$. Hence the number of $A_e(k)$ -conjugacy classes of type v for which the isotropy group is exactly $\mu_d(k)$ is, by (4.1),

$$h_{e,v}^2 \sum_{d'} \mu(d') c_{dd' \setminus v}$$

summed over all divisors d' of f/d such that dd' divides each $m_i(v)$ (so that the partition $dd' \setminus v$ is defined). Since $|\mu_d(k)| = h_d$, there are $(q-1)/h_d$ elements in each orbit, and hence the total number of conjugacy classes in the group $G_e(k)$ is

$$(4.2) \quad c(G_e(k)) = \sum_{|v|=n} h_{e,v}^2 \sum_{d,d'} h_d \mu(d') c'_{dd' \setminus v} ,$$

in which the first sum is over all partitions v of n , and the second is over all pairs of positive integers d, d' such that dd' divides f and each $m_i(v)$. By (2.4), the expression (4.2) is equal to

$$(4.3) \quad \sum_{|v|=n} h_{e,v}^2 \sum_{d_1} \phi(d_1) c'_{d_1 \setminus v}$$

where d_1 runs through the common divisors of $f, q - 1$ and the $m_i(v)$. Since $h_{e,v} = h_{e,d_1 \setminus v}$, (4.3) can be rewritten in the form

$$\sum_{d_1} \phi(d_1) \sum_v h_{e,v}^2 c'_v$$

where d_1 runs through the divisors of h_f and v through the partitions

of n/d_1 . As in §3, the inner sum is equal to

$$\sum_{d_2} \phi_2(d_2) c'_{n/d_1 d_2}$$

where d_2 runs through the divisors of h_e . Hence

(4.4) *The number of conjugacy classes in the group $G_e(k)$ is*

$$c(G_e(k)) = \sum_{d_1, d_2} \phi(d_1) \phi_2(d_2) c'_{n/d_1 d_2}$$

summed over pairs of positive integers d_1, d_2 such that d_1 divides h_f and d_2 divides h_e .

REMARKS. 1. When $f = 1$ and $e = n$ (respectively $e = 1$ and $f = n$) the group $G_e(k)$ is $SL_n(k)$ (respectively $PGL_n(k)$), and the expression (4.4) reduces to (3.6) (respectively (2.2)).

2. From (4.4) and (2.4) we deduce an alternative formula for $c(G_e(k))$:

$$(4.5) \quad c(G_e(k)) = \sum_{a_1, a_2, b_1, b_2} \mu(a_1) \mu(a_2) h_{b_1, f} h_{b_2, e}^2 c'_{n/a_1 a_2 b_1 b_2}$$

summed over all quadruples a_1, a_2, b_1, b_2 of positive integers such that $a_1 a_2 b_1 b_2$ divides n , where $h_{b_1, f}$ (respectively $h_{b_2, e}$) is the highest common factor of b_1, f and $q - 1$ (respectively b_2, e and $q - 1$). When $e = n$ and $f = 1$ (respectively $e = 1$ and $f = n$), the formula (4.5) reduces to (3.5) (respectively (2.1)).

3. The group $GL_n(k)$ acts by inner automorphisms on $A_e(k)$:

$h.(g, x) = (hgh^{-1}, x)$. This action fixes $B_e(k)$ pointwise, and hence defines an action of $GL_n(k)$ on the group $G_e(k)$. The method used to prove (4.4) shows that the number of $GL_n(k)$ -orbits in $G_e(k)$ is

$$(4.6) \quad \sum_{d_1, d_2} \phi(d_1) \phi(d_2) c'_{n/d_1 d_2}$$

summed over pairs of positive integers d_1, d_2 such that d_1 divides h_f and d_2 divides h_e . Since (4.6) is unaltered by interchange of e and f , it follows that the number of $GL_n(k)$ -orbits is the same in $G_e(k)$ and $G_f(k)$. This result generalizes Remark 1 of §3.

For a related result, see Lehrer [2].

5. $PSL_n(k)$

Let $PSL_n(k)$ denote the quotient of $SL_n(k)$ by its centre $\mu_n(k).1_n$. The conjugacy classes of $PSL_n(k)$ may be identified with the orbits of $\mu_n(k)$ acting on the set of conjugacy classes of $SL_n(k)$. From §3, the number of conjugacy classes of type ν in $SL_n(k)$ is $h_\nu^2 c'_\nu$, for each partition ν of n . It follows as in §4 that the number of $SL_n(k)$ -classes for which the isotropy group is $\mu_d(k)$, where d is a divisor of n , is

$$h_\nu^2 \sum_{d'} \mu(d') c'_{dd' \setminus \nu}$$

summed over all divisors d' of n/d such that dd' divides each $m_i(\nu)$. The number of elements in each orbit is $(\mu_n(k) : \mu_d(k)) = h_n/h_d$, and hence we obtain the total number of conjugacy classes in $PSL_n(k)$:

$$\hat{c}_n \doteq c(PSL_n(k)) = \frac{1}{h_n} \sum_{|\nu|=n} h_\nu^2 \sum_{d, d'} h_d^{\mu(d')} c'_{dd' \setminus \nu}$$

in which the first sum is over all partitions ν of n , and the second is over all pairs of positive integers d, d' such that dd' divides n and each $m_i(\nu)$. This formula can be turned around in the same way as in §4 to give

$$(5.1) \quad \hat{c}_n = \frac{1}{h_n} \sum_{d_1, d_2} \phi(d_1) \phi(d_2) c'_{n/d_1 d_2}$$

summed over all pairs of divisors d_1, d_2 of $q-1$ such that $d_1 d_2$ divides n ; and equivalently

$$(5.2) \quad \hat{c}_n = \frac{1}{h_n} \sum_{a_1, a_2, b_1, b_2} \mu(a_1)\mu(a_2)h_{b_1}h_{b_2}^2 \frac{c'_n}{a_1 a_2 b_1 b_2},$$

summed over all quadruples a_1, a_2, b_1, b_2 of positive integers such that $a_1 a_2 b_1 b_2$ divides n .

In Table 4 below we list the values of \hat{c}_n for $1 \leq n \leq 8$; these are straightforward to calculate from (5.2) and Table 2.

TABLE 4

$$\begin{aligned} \hat{c}_1 &= 1 \\ \hat{c}_2 &= \frac{1}{h_2} (q+4h_2-3) \\ \hat{c}_3 &= \frac{1}{h_3} (q^2+q+5h_3-5) \\ \hat{c}_4 &= \frac{1}{h_4} (q^3+q^2+q(4h_2-3)+h_4^2+h_4+3h_2-5) \\ \hat{c}_5 &= \frac{1}{h_5} (q^4+q^3+q^2+7h_5-8) \\ \hat{c}_6 &= \frac{1}{h_2 h_3} (q^5+q^4+q^3+q^2(4h_2-3)+q(4h_2+5h_3-9)+5(4h_2-3)(h_3-1)) \\ \hat{c}_7 &= \frac{1}{h_7} (q^6+q^5+q^4+q^3-q+9h_7-10) \\ \hat{c}_8 &= \frac{1}{h_8} (q^7+q^6+q^5+q^4+q^3(4h_2-3)+q^2(4h_2-4)+q(h_4^2+h_4+3h_2-6) \\ &\quad +h_2 h_4^2+h_8^2-h_4^2+3h_2 h_4+h_8-3h_4-11h_2+9). \end{aligned}$$

6. Unitary groups

Let k_2 be the unique quadratic extension of k contained in \bar{k} . The unitary group $U_n(k_2)$ is the subgroup of all $g \in GL_n(k_2)$ such that $Fg = {}^t g^{-1}$, where $(Fg)_{ij} = g_{ij}^q$.

(6.1) Every conjugacy class of $G = GL_n(k)$ which intersects $U = U_n(k_2)$ does so in a single conjugacy class of U .

Proof. Let σ be the endomorphism of G defined by $g^\sigma = {}^t(Fg)^{-1}$, so that U is the group of fixed points of σ . Suppose that $u \in U$ and $g \in G$ are such that $gug^{-1} \in U$; we have to show that u and gug^{-1} are conjugate in U .

Since $gug^{-1} \in U$, we have $gug^{-1} = g^\sigma ug^{-\sigma}$, so that $g^{-1}g^\sigma \in G_u$, the centralizer of u in G . Now centralizers in G are connected ([4], III, 3.22), and $\sigma(G_u) \subset G_u$ because $u = u^\sigma$; since the kernel of σ is finite it follows that $\sigma|_{G_u}$ is surjective, and hence by Lang's theorem ([5], §10) the mapping $h \rightarrow h^{-1}h^\sigma$ from G_u to G_u is surjective. Hence we have $g^{-1}g^\sigma = h^{-1}h^\sigma$ for some $h \in G_u$, which shows that $v = gh^{-1} \in U$ and therefore $gug^{-1} = gh^{-1}uhg^{-1} = vuv^{-1}$. Hence u and gug^{-1} are conjugate in U . //

In particular, if two elements of $U_n(k_2)$ are conjugate in $GL_n(k_2)$, they are conjugate in $U_n(k_2)$. It follows that the conjugacy classes of $U_n(k_2)$ are parametrized bijectively by the partition-valued functions μ on $M = \bar{k}^*$ which satisfy (1.3) and $\mu(x^{-q}) = \mu(x)$ for all $x \in M$ in place of (1.4). Equivalently, as in §1, each conjugacy class of $U_n(k_2)$ may be represented by a sequence of polynomials $u = (u_1(t), u_2(t), \dots)$ with coefficients in k_2 which satisfy (1.9) and are such that $u_i(0) = 1$ and the set of roots of each u_i is stable under $x \rightarrow x^{-q}$ (in place of (1.8)). We define the *type* ν of a conjugacy class in $U_n(k_2)$ as in §1 to be the partition $(1^{n_1} 2^{n_2} \dots)$ of n , where $n_i = \deg u_i$. It is easily seen that the number of possibilities for u_i of degree n_i is $q^{n_i} + q^{n_i-1}$ if $n_i > 0$ (and 1 if $n_i = 0$), so that the number of conjugacy classes of type ν in $U_n(k_2)$ is

$$(6.2) \quad \gamma_v = \prod_{n_i > 0} (q^{n_i + q} q^{n_i - 1})$$

or equivalently

$$(6.2') \quad \gamma_v = q^{l(v) - p(v)} (q+1)^{p(v)}$$

where $l(v)$ is the number of parts of v and $p(v)$ is the number of unequal parts. Hence the total number of conjugacy classes in $U_n(k_2)$ is

$$(6.3) \quad \gamma_n = c(U_n(k_2)) = \sum_{|v|=n} \gamma_v .$$

Since $q^n + q^{n-1}$ is the coefficient of t^n in $(1+t)/(1-qt)^{-1}$, if $n > 0$, it follows from (6.2) and (6.3) that the generating function for the numbers γ_n is

$$(6.4) \quad \Gamma(t) = \sum_{n=0}^{\infty} \gamma_n t^n = \prod_{r=1}^{\infty} \frac{1+t^r}{1-qt^r} .$$

This formula is due to Wall [6].

Each γ_n ($n \geq 1$) is a polynomial in q , divisible by $(q+1)$, as one sees for example by putting $q = -1$ in (6.4). Let $\gamma'_n = \gamma_n / (q+1)$, so that from (6.2') and (6.3) we have

$$(6.5) \quad \gamma'_n = \sum_{|v|=n} q^{l(v) - p(v)} (q+1)^{p(v) - 1} .$$

In Table 5 (p. 46) we list the polynomials γ'_n for $1 \leq n \leq 10$. They are easily calculated from the formula (6.5).

The formulas of §§2-5 all have their analogues for the unitary groups. Since the proofs are the same, we shall merely state the results.

For any positive integer d , let η_d denote the highest common factor of d and $q + 1$.

(i) $PU_n(k_2)$. Corresponding to (2.1) we have

$$(6.6) \quad \bar{\gamma}_n = c(PU_n(k_2)) = \sum_{d, d'} \eta_d^{\mu(d')} \gamma'_{n/dd'}$$

summed over all pairs of positive integers d, d' such that dd' divides n , or alternatively

$$(6.7) \quad \bar{\gamma}_n = \sum_d \phi(d) \gamma'_{n/d}$$

summed over the divisors d of $\eta_n = (n, q+1)$. Hence the generating function for the $\bar{\gamma}_n$ is (with $\bar{\gamma}_0 = 1$)

$$(6.8) \quad \bar{\Gamma}(t) = \sum_{n=0}^{\infty} \bar{\gamma}_n t^n = \frac{1}{q+1} \sum_{d|q+1} \phi(d) \Gamma(t^d),$$

where $\Gamma(t)$ is the generating function (6.4).

TABLE 5

$$\gamma'_1 = 1$$

$$\gamma'_2 = q + 1$$

$$\gamma'_3 = q^2 + q + 2$$

$$\gamma'_4 = q^3 + q^2 + 3q + 2$$

$$\gamma'_5 = q^4 + q^3 + 3q^2 + 4q + 3$$

$$\gamma'_6 = q^5 + q^4 + 3q^3 + 5q^2 + 6q + 4$$

$$\gamma'_7 = q^6 + q^5 + 3q^4 + 5q^3 + 8q^2 + 9q + 5$$

$$\gamma'_8 = q^7 + q^6 + 3q^5 + 5q^4 + 9q^3 + 12q^2 + 13q + 6$$

$$\gamma'_9 = q^8 + q^7 + 3q^6 + 5q^5 + 9q^4 + 14q^3 + 19q^2 + 17q + 8$$

$$\gamma'_{10} = q^9 + q^8 + 3q^7 + 5q^6 + 9q^5 + 15q^4 + 22q^3 + 27q^2 + 23q + 10$$

(ii) $SU_n(k_2)$. In place of (3.5) and (3.6) we obtain

$$(6.9) \quad \tilde{\gamma}_n = c(SU_n(k_2)) = \sum_{d,d'} \eta_d^{2\mu(d')} \gamma'_{n/dd'}$$

so that $\tilde{\gamma}_n$ is obtained from $\bar{\gamma}_n$ by replacing each η_d by η_d^2 , and equivalently

$$(6.10) \quad \tilde{\gamma}_n = \sum_d \phi_2(d) \gamma'_n/d$$

summed over the divisors d of η_n . Consequently the generating function for the $\tilde{\gamma}_n$ is (with $\tilde{\gamma}_0 = 1$)

$$(6.11) \quad \tilde{\Gamma}(t) = \sum_{n=0}^{\infty} \tilde{\gamma}_n t^n = \frac{1}{q+1} \sum_{d|q+1} \phi_2(d) \Gamma(t^d) - q.$$

(iii) Groups isogenous to SU_n . If Γ_e is the quotient of SU_n by its central subgroup isomorphic to μ_f (where $ef = n$ as in §4) then in place of (4.4) we find

$$(6.12) \quad d(\Gamma_e(k_2)) = \sum_{d_1, d_2} \phi(d_1) \phi_2(d_2) \gamma'_n/d_1 d_2$$

summed over pairs of positive integers d_1, d_2 such that d_1 divides η_f and d_2 divides η_e .

(iv) $PSU_n(k_2)$. This is the quotient of $SU_n(k_2)$ by its centre, and in place of (5.1) the number of its conjugacy classes is

$$(6.13) \quad \tilde{\gamma}_n = c(PSU_n(k_2)) = \frac{1}{\eta_n} \sum_{d_1, d_2} \phi(d_1) \phi_2(d_2) \gamma'_n/d_1 d_2$$

summed over all pairs of divisors d_1, d_2 of $q + 1$ such that $d_1 d_2$ divides n .

References

- [1] Walter Feit and N.J. Fine, "Pairs of commuting matrices over a finite field", *Duke Math. J.* 27 (1960), 91-94.
- [2] G.I. Lehrer, "Characters, classes, and duality in isogenous groups", *J. Algebra* 36 (1975), 278-286.
- [3] I.G. Macdonald, "Zeta functions attached to finite general linear groups", *Math. Ann.* 249 (1980), 1-15.

- [4] T.A. Springer and R. Steinberg, "Conjugacy classes", *Seminar on algebraic groups and related finite groups*, Princeton, 1968/69, 167-226 (Lecture Notes in Mathematics, 131. Springer-Verlag, Berlin, Heidelberg, New York, 1970).
- [5] Robert Steinberg, *Endomorphisms of linear algebraic groups* (Memoirs of the American Mathematical Society, 80. American Mathematical Society, Providence, Rhode Island, 1968).
- [6] G.E. Wall, "On the conjugacy classes in the unitary, symplectic and orthogonal groups", *J. Austral. Math. Soc.* 3 (1963), 1-62.
- [7] G.E. Wall, "Conjugacy classes in projective and special linear groups", *Bull. Austral. Math. Soc.* 22 (1980), 339-364.

Department of Pure Mathematics,
Queen Mary College,
University of London,
Mile End Road,
London E14NS,
England.