

new areas for investigation and broaden the market. Neither the pure nor the applied aspects of any science can stand alone. Each contributes to the other more than some would care to admit. I have stressed the importance of mathematics; may I now say that we should make it interesting as well as fun to do.

At this point you may be wondering why a publisher continues. Well he has a dream, and he wants to be a part of the world of knowledge. He knows that a scientific book is a tool, and it must be made available, despite the limited audience to which it is addressed. He is also aware that the branching and twiggling effect that has occurred in science and technology is reflected in lower sales. The publisher needs to break even and to make a profit so that he will be there to publish your current book and your succeeding books.

JOHN WILEY AND SONS, 605 THIRD AVENUE, NEW YORK, NY 10016.

---

## REPRESENTATIONS OF $SL(2, p)$

J. E. HUMPHREYS

**1. Introduction.** The **special linear group**  $SL(2, p^n)$  consists of all  $2 \times 2$  matrices of determinant 1 with entries from the field of  $p^n$  elements, where  $p$  is a prime. (These matrices do form a group under matrix multiplication, thanks to the product rule for determinants). The matrices  $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  commute with all others, and thus form a normal subgroup  $Z$ , and the quotient groups  $PSL(2, p^n) = SL(2, p^n)/Z$  turn out to be **simple** when  $p^n \neq 2, 3$ , i.e., they have no proper normal subgroups (cf. Dornhoff [6, Part A, §35]). This is just the first of a number of infinite families of simple groups which arise from Lie theory by way of matrix groups over finite fields. In fact, if we add to the list so obtained, the alternating groups  $A_n$  ( $n \geq 5$ ), we get all but 22 or so of the presently known (nonabelian) simple groups. So it is a good idea for anyone interested in finite groups and their applications (cf. Waall [27]) to find out more about these remarkable families. Here we shall limit ourselves to the groups  $SL(2, p^n)$  when  $n = 1$ , to avoid some technical details involving tensor products. But most of the ideas carry over to the case of arbitrary  $n$  — and even to the other families of Lie type.

If  $G$  is any finite group,  $F$  any field, a **representation** of  $G$  is by definition a homomorphism  $\rho: G \rightarrow GL(n, F)$  (= group of all invertible  $n \times n$  matrices over  $F$ ).

The number  $n$  is called the **degree** of  $\rho$ . A representation of degree 1 is essentially just a homomorphism of  $G$  into the multiplicative group  $F^*$  of  $F$ . As the name implies, a representation provides a sort of picture of  $G$ : in place of abstract group elements, multiplied abstractly, we get concrete matrices, multiplied in a familiar way. But the picture may be a poor likeness of the original; for example, let  $\rho$  send all elements of  $G$  to 1 (this is called the **1-representation** of  $G$  and denoted  $1_G$ ). Even so, the study of *all* possible representations of  $G$  often yields a very good “composite” picture of  $G$  (cf. Klemm [17]). In the next three sections we shall survey some of the theory of representations for arbitrary  $G$  and then see what can be said about  $\mathbf{SL}(2, p)$ .

The reader may object that  $\mathbf{SL}(2, p)$  is already given concretely enough (in its “natural” representation of degree 2 over the field of  $p$  elements). But in fact the nicest results are obtained by studying representations of a group over the field  $\mathbf{C}$  of complex numbers.

**2. Group representations.** In §2–§4,  $G$  is an arbitrary finite group, and all representations are over  $\mathbf{C}$ . The theory to be summarized here was developed around 1900, largely by Frobenius, Schur, and Burnside. As general references we suggest Curtis and Reiner [5], Dornhoff [6, Part A].

In order to sort out the representations of  $G$ , it is necessary to decide first when two of them are to be viewed as essentially the same. Given  $\rho: G \rightarrow \mathbf{GL}(n, \mathbf{C})$ , each  $x \in G$  is represented by a matrix  $\rho(x)$ , which in turn describes a linear transformation of the vector space  $V = \mathbf{C}^n$  relative to the usual basis. So  $G$  acts (via  $\rho$ ) on  $V$ , which we express by saying that  $V$  is a **G-module**. This *action* of  $G$  on  $V$  really does not depend in any essential way on the basis chosen for  $V$ , although a change of basis would lead to different representing matrices. Indeed, if  $A \in \mathbf{GL}(n, \mathbf{C})$  describes a change of basis, then the new matrices are of the form  $A\rho(x)A^{-1}$  ( $x \in G$ ). This leads us to say that  $\rho$  is **equivalent** to another representation  $\rho': G \rightarrow \mathbf{GL}(n, \mathbf{C})$  (same degree  $n$ ) if there exists  $A \in \mathbf{GL}(n, \mathbf{C})$  such that  $\rho'(x) = A\rho(x)A^{-1}$  for all  $x \in G$ .

Consider, as the first nonabelian example, the symmetric group  $S_3$  of order  $6 = 3!$ .  $S_3$  is generated by the 2-cycle  $x = (12)$  and the 3-cycle  $y = (123)$ , subject only to the relations:  $x^2 = 1 = y^3$ ,  $yx = xy^2$ . To construct a representation of  $S_3$ , we just have to specify two matrices  $\rho(x)$ ,  $\rho(y)$  satisfying the same relations. If we identify  $1 \times 1$  matrices with scalars, we can write down a couple of obvious representations of degree 1: the 1-representation  $\rho(x) = 1 = \rho(y)$ , and the *sign*  $\rho'(x) = -1$ ,  $\rho'(y) = 1$  (+1 for an even permutation, -1 for an odd permutation). These two representations are *not* equivalent. (Exercise: They are the only possibilities of degree 1.)

Turning to degree 2, we propose

$$\rho(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \rho(y) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix},$$

where  $\omega$  is a primitive cube root of 1 in  $\mathbf{C}$ . It is easy to check that these matrices satisfy the required relations. On the other hand, we could take

$$\rho'(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \rho'(y) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

But  $\rho'$  is equivalent to  $\rho$ : choose  $A = \begin{pmatrix} \omega & 1 \\ 1 & \omega \end{pmatrix}$ .

What about degree 3? Here  $S_3$  has a "natural" representation: to a permutation of  $\{1, 2, 3\}$  corresponds the linear transformation which permutes the usual basis  $(e_1, e_2, e_3)$  of  $\mathbf{C}^3$  in the same way. For instance,

$$(123) \text{ goes to } \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

But notice that the vector  $e_1 + e_2 + e_3$  is fixed by all permutations of the subscripts, while the complementary subspace spanned by  $e_1 - e_3, e_2 - e_3$ , is stable under all the representing transformations. Changing the basis to  $(e_1 + e_2 + e_3, e_1 - e_3, e_2 - e_3)$ , we get an equivalent representation under which

$$(12) \text{ goes to } \left[ \begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & 1 \\ 0 & 1 & 0 \end{array} \right] \text{ and } (123) \text{ goes to } \left[ \begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & -1 & -1 \\ 0 & 1 & 0 \end{array} \right].$$

What we have here is the **direct sum** of the 1-representation and the representation of degree 2 constructed above. So nothing new has been obtained.

Conversely, we can build up representations of arbitrarily large degree by combining known ones in this way. The crucial thing is therefore to find those representations (called **indecomposable**) which cannot be broken down further into direct sums. The Krull-Schmidt Theorem (for  $G$ -modules) assures us in advance that each representation is a direct sum of indecomposable ones, the summands being unique up to ordering and equivalence. But it gives us no guidance in finding them!

Here a stronger condition comes into play:  $\rho: G \rightarrow \mathbf{GL}(n, \mathbf{C})$  is called **irreducible** if no proper subspace of  $\mathbf{C}^n$  is stable under all  $\rho(x), x \in G$ . (Irreducible implies indecomposable, but not vice versa.) The reader can verify, for example, that the above representation of degree 2 of  $S_3$  is irreducible, as is any representation of degree 1. Another basic result in algebra (Jordan-Hölder Theorem) assures us that each  $G$ -module has a "composition series" with irreducible "factors" which are essentially unique. In matrix language, this means that  $\rho$  is equivalent to some  $\rho'$ , where all  $\rho'(x)$  have the form:

$$\left[ \begin{array}{c|ccc} \rho_1(x) & & & \\ \hline & \rho_2(x) & & * \\ & & \cdot & \\ & & & \cdot \\ & & & \cdot \\ \hline 0 & & & \rho_k(x) \end{array} \right]$$

the  $\rho_i$  being irreducible representations and the  $*$  entries being unspecified.

Fortunately, we do not have to choose between the Krull-Schmidt approach and the Jordan-Hölder approach, thanks to

(2.1) MASCHKE'S THEOREM: *Every representation of  $G$  is equivalent to a direct sum of irreducible ones.*

The remaining task is to describe the irreducible representations of  $G$ . Again, we are fortunate, because there are not "too many" of them:

(2.2) *The number of (inequivalent) irreducible representations of  $G$  is equal to the number of conjugacy classes of  $G$ .*

This result is somewhat peculiar, because examples show that there is (in general) no natural 1-1 correspondence between the representations and the classes. In our example,  $S_3$  has three conjugacy classes:  $\{1\}$ ,  $\{(12), (13), (23)\}$ ,  $\{(123), (132)\}$ , one for each type of cycle structure. So the three irreducible representations already constructed must be the only ones, and we can fairly claim to have determined (up to equivalence) all possible representations of  $S_3$ . Notice that the degrees 1, 1, 2 obey the following general rule:

(2.3) *Let  $\rho_1, \dots, \rho_s$  be the distinct irreducible representations of  $G$ ,  $n_i = \text{degree of } \rho_i$ . Then  $\sum n_i^2 = |G|$  (the order of  $G$ ). Moreover,  $n_i$  divides  $|G|$ .*

The reason for  $|G|$  to appear here becomes plainer if we introduce the **regular representation** of  $G$ . The reader may recall Cayley's Theorem, which identifies an abstract group with a subgroup of the symmetric group  $S_{|G|}$  ( $x \in G$  permutes the elements of  $G$  by right multiplication). In turn,  $S_{|G|}$  may be represented by matrices obtained by permuting columns of the identity matrix (as was done above for  $S_3$ ). This yields the desired representation  $\rho_G$  of  $G$ , of degree  $|G|$ . The equality in (2.3) then comes from the more precise fact:

(2.4) *The regular representation  $\rho_G$  is the direct sum of the various  $\rho_i$ , each  $\rho_i$  occurring  $n_i$  times.*

**3. Characters.** So far, the theory looks very satisfactory. But when  $G$  is a large or "complicated" group (and simple groups tend to be quite complicated!), the

actual construction of irreducible representations is no routine matter. In fact, we usually have to settle for something less explicit.

Recall from linear algebra that the **trace**  $\text{tr } M$  of a square matrix  $M$  is the sum of its diagonal entries, and that this does not change if  $M$  is replaced by the similar matrix  $AMA^{-1}$  (thanks to the fact that  $\text{tr } XY = \text{tr } YX$ ). Given a representation  $\rho: G \rightarrow \mathbf{GL}(n, \mathbf{C})$ , the function  $\chi(x) = \text{tr } \rho(x)$  from  $G$  to  $\mathbf{C}$  is therefore the same for any representation equivalent to  $\rho$ . We call  $\chi$  the **character** of  $\rho$ . Note that the character of a direct sum is just the sum of the characters. If  $x$  is conjugate to  $y$  in  $G$  (say  $x = zyz^{-1}$ ), then  $\rho(x) = \rho(z)\rho(y)\rho(z)^{-1}$  is similar to  $\rho(y)$  and thus has the same trace. So  $\chi$  may also be thought of as a  $\mathbf{C}$ -valued function on the set of conjugacy classes of  $G$ . This suggests that we write down an  $s \times s$  **character table**, the rows indexed by the characters  $\chi_1, \dots, \chi_s$  of the irreducible representations  $\rho_1, \dots, \rho_s$ , and the columns by representatives  $x_1, \dots, x_s$  of the distinct conjugacy classes, with the value  $\chi_i(x_j)$  appearing in the  $(i, j)$  position. It is customary to put the class  $\{1\}$  first, so the first column contains the numbers  $\chi_i(1)$ , which are clearly just the degrees  $n_i$ . For  $S_3$ , see Table 1.

	1	(12)	(123)
$\chi_1$	1	1	1
$\chi_2$	1	-1	1
$\chi_3$	2	0	-1

TABLE 1. Character table of  $S_3$

$\mathbf{C}$ -valued functions on conjugacy classes of  $G$  may be added or multiplied by scalars, so they form an  $s$ -dimensional vector space  $CF(G)$  over  $\mathbf{C}$ . (What is the most obvious basis?) This vector space has a natural (unitary) inner product, the bar denoting complex conjugation:

$$(3.1) \quad (\chi, \phi)_G = |G|^{-1} \sum_{x \in G} \chi(x) \overline{\phi(x)} = |G|^{-1} \sum_j h_j \chi(x_j) \overline{\phi(x_j)}$$

( $x_j =$  class representative,  $h_j =$  number of conjugates of  $x_j$ ).

Remarkably enough:

(3.2) *The irreducible characters  $\chi_1, \dots, \chi_s$  form an orthonormal basis for  $CF(G)$ .*

This is one of the basic **orthogonality relations**. The other involves the columns of the character table:

$$(3.3) \quad \sum_{i=1}^s \chi_i(x_j) \chi_i(x_k) = \delta_{jk} |G|/h_k.$$

These relations are often used to get information about unknown characters from

information about known ones. (For instance, the reader should be able to fill in the third row of Table 1 once the first two rows are known.) Moreover, (3.2) shows that the character  $\chi$ , which at first sight seems to contain only partial information about  $\rho$ , actually determines  $\rho$  uniquely:

(3.4) *Two representations of  $G$  having the same character are equivalent. If  $\chi$  is a character of  $G$ , then  $\chi$  is irreducible if and only if  $(\chi, \chi)_G = 1$ .*

**4. How to construct characters.**  $G$  may have a subgroup  $H$  whose characters we already know. Say  $\phi$  is one of these. It is easy enough to extend  $\phi$  to a  $\mathbf{C}$ -valued function  $\phi$  on  $G$ , by decreeing that  $\phi(x) = 0$  if  $x \notin H$ . But  $\phi$  has little chance of being a character — for one thing,  $\phi$  may take distinct values at elements of  $H$  which are not conjugate in  $H$  but are conjugate in  $G$ . So we try something fancier:

$$(4.1) \quad \phi^G(x) = |H|^{-1} \sum_{y \in G} \phi(yxy^{-1}) \quad (x \in G).$$

A moment's scrutiny should make it clear that  $\phi^G$  is at least a class function on  $G$ . Indeed:

(4.2)  *$\phi^G$  is a character of  $G$  (called an **induced character**).*

The reason *why*  $\phi^G$  should be a character cannot be well understood without going into some technical details about tensor products. To see that some sort of “product” is involved, observe that:

(4.3) *The degree  $\phi^G(1)$  is the product of  $\phi(1)$  and the index  $[G:H]$ .*

If  $H$  has fairly small index in  $G$  (i.e., if  $H$  is big), and if  $\phi$  is irreducible, then there is at least a chance that  $\phi^G$  may also be irreducible. Take, for example,  $G = S_3$ ,  $H$  the cyclic subgroup generated by (123).  $H$  has an obvious representation of degree 1 sending (123) to  $\omega$  (= primitive cube root of 1). The induced character given by (4.1) then has degree 2 and in fact occupies the third row of Table 1.

There is another useful technique, based in a different way on tensor products:

(4.4) *If  $\chi, \phi$  are characters of  $G$ , then so is their product:  $(\chi\phi)(x) = \chi(x)\phi(x)$ .*

The degree of  $\chi\phi$  being the product  $\chi(1)\phi(1)$ , there is usually little hope that the product will be irreducible even if  $\chi$  and  $\phi$  are. But  $\chi\phi$  *may* contain new irreducible constituents, and we *may* be able to sort them out.

**5. The groups  $\mathbf{SL}(2, p)$ .** From now on  $G = \mathbf{SL}(2, p)$  unless otherwise specified. Since we are dealing with a whole family of groups, not just a single group, the question arises at once: Why should we expect the representations of (say)  $\mathbf{SL}(2, 17)$  to have anything at all to do with those of (say)  $\mathbf{SL}(2, 71)$ ? The common origin of these groups in Lie theory does not at first seem to have any connection with their

representations over  $\mathbf{C}$ . One of our purposes, then, will be to explain what connection exists.

It is an observed fact that many phenomena surrounding these groups are (in some sense) independent of  $p$ , or else vary "smoothly" with  $p$ . For example:

$$(5.1) \text{ The order of } \mathbf{SL}(2, p) \text{ is } p^3 - p = p(p+1)(p-1).$$

This formula is easy to derive (cf. Dornhoff [6, Part A, Lemma 35.2]). It shows that the order of a  $p$ -sylog subgroup of  $G$  is  $p$ . One subgroup of this size consists of the matrices  $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ ; we denote it by  $U$ . Let  $T$  be the subgroup of all diagonal matrices  $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$  in  $G$ . This is cyclic of order  $p-1$  (being isomorphic to the multiplicative group of the field of  $p$  elements.) The product  $B = TU$  is the group of upper triangular matrices in  $G$ , and has order  $p(p-1)$ , hence index  $p+1$ .

From now on we shall always assume that  $p$  is an odd prime, to avoid a few awkward statements. The case  $p=2$  is essentially done, anyway, since  $\mathbf{SL}(2, 2)$  happens to be isomorphic to  $S_3$ . (To see this, notice that  $\mathbf{SL}(2, 2)$  has order 6, by (5.1), and permutes the three distinct subspaces of dimension 1 in 2-dimensional space over the field of 2 elements.)

The next two sections are based on the exposition in Dornhoff [6, Part A, §38], which in turn rests on Schur [19].

**6. Conjugacy classes of  $\mathbf{SL}(2, p)$ .** To find the irreducible representations of  $G$  (or at least their characters), we have to know how many to look for, i.e., how many classes  $G$  has (2.2). The answer is a polynomial in  $p$ , namely,  $p+4$ . (If 4 is interpreted as the square of the order of the center of  $G$ , the same formula will work for  $p=2$ .)

The best way to survey the classes is to introduce a factorization valid in any finite group (for a given prime  $p$ ). Call  $x \in G$   **$p$ -regular** if its order is relatively prime to  $p$ ,  **$p$ -singular** if its order is a power of  $p$ .

(6.1) Let  $x \in G$ . Then there exist unique elements  $y, z \in G$  satisfying the conditions:  $x = yz = zy$ ,  $y$   $p$ -regular,  $z$   $p$ -singular.

This boils down to an assertion about the cyclic group generated by  $x$ , which the reader can readily check.

In our case,  $G$  is given as a matrix group (over the field of  $p$  elements), so we can ask what meaning this factorization has in terms of *linear algebra*. A  $p$ -singular element of  $G$  is a matrix whose eigenvalues are both 1 (why?). On the other hand, a matrix has order prime to  $p$  if and only if it is diagonalizable (either over the prime field or over a quadratic extension). By adapting Jordan normal forms, one can show without much trouble that there are  $p$  classes of  $p$ -regular elements, including the class of 1, two other classes of  $p$ -singular elements, and two "mixed"

classes. There are essentially two types of  $p$ -regular elements: those conjugate already in  $G$  to a diagonal matrix and those which only become diagonal over a field of  $p^2$  elements.

In Table 2 we list class representatives, along with the number of elements in the class (= index in  $G$  of the centralizer in  $G$  of an element in the class). Here

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, z = -1, \quad c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, d = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}, a = \begin{pmatrix} v & 0 \\ 0 & v^{-1} \end{pmatrix},$$

Representative	1	$z$	$a^l$	$b^m$	$c$	$d$	$zc$	$zd$
$\#$ Conjugates	1	1	$p(p+1)$	$p(p-1)$	$\frac{1}{2}(p^2-1)$	$\frac{1}{2}(p^2-1)$	$\frac{1}{2}(p^2-1)$	$\frac{1}{2}(p^2-1)$

TABLE 2. Class representatives of  $SL(2, p)$

where  $v$  generates the multiplicative group of the field of  $p$  elements. Also,  $b$  denotes an element of order  $p + 1$  which is not diagonalizable over the prime field. The non-conjugate powers are:  $a^l$  ( $1 \leq l \leq (p - 3)/2$ ),  $b^m$  ( $1 \leq m \leq (p - 1)/2$ ), plus of course  $1 = a^0 = b^0$ ,  $z = a^{(p-1)/2} = b^{(p+1)/2}$ . As an exercise, the reader might verify that the number of classes exhibited is  $p + 4$  (as claimed) and that the total number of elements is  $p^3 - p$  (5.1).

A group of order 2, called the **Weyl group**, makes its appearance here. It brings about, for example, the conjugacy of  $a^k$  and  $a^{-k}$  (and similarly for powers of  $b$ ). *This group  $W$  is the same no matter what  $p$  is*, which turns out to be a key factor in the uniformity of the results which follow. Strictly speaking,  $W = N_G(T)/T$ , where the normalizer of the diagonal group  $T$  consists of all matrices with exactly one nonzero entry in each row and each column (check this).  $W$  should be thought of as the symmetric group  $S_2$ .

**7. Characters of  $SL(2, p)$ .** The character table of  $SL(2, p)$  was first obtained by Frobenius; shortly afterwards, Schur [19] and (independently) H. Jordan [16] found the characters of  $SL(2, p^n)$ . We are following Dornhoff's version of Schur's paper.

It turns out that the irreducible characters of  $G$  occur in two "series." The first of these is very easy to construct by the induced character technique sketched in Section 4. (In this case one easily gets the *representations*, not just the characters.) Begin with  $T$ , the cyclic group of order  $p - 1$  generated by  $a$ . There are  $p - 1$  distinct characters of  $T$  having degree 1 (cf. (2.2) and (2.3)), given as follows: Let  $\tau \in \mathbb{C}$  be a primitive  $(p - 1)$ -th root of 1, and define  $\lambda_i(a^l) = \tau^{il}$ . We could induce these characters to  $G$ , but since  $T$  has rather large index in  $G$  this would be unwise. Instead, we extend  $\lambda_i$  first to a character (again called  $\lambda_i$ ) of the triangular group  $B = TU$  by requiring that  $\lambda_i(x) = 1$  for  $x \in U$ . (Why is this legitimate?) Now  $[G : B] = p + 1$ ,



so the induced character  $\zeta_i = \lambda_i^G$  has degree  $p + 1$  (4.3). From (4.1) the values of  $\zeta_i$  on class representatives can be computed without much labor (Table 3).

1	$z$	$a^l$	$b^m$	$c$	$d$	$zc$	$zd$
$p + 1$	$(-1)^i(p+1)$	$\tau^{il} + \tau^{-il}$	0	1	1	$(-1)^i$	$(-1)^i$

TABLE 3. Values of  $\zeta_i$

A glance at Table 3 shows that not all  $\zeta_i$  are distinct; so we can limit our attention to the indices  $0 \leq i \leq (p - 1)/2$ . The next question is: Which (if any) of the  $\zeta_i$  are irreducible? A straightforward calculation using (3.1) shows that if  $1 \leq i \leq (p - 3)/2$ , then  $(\zeta_i, \zeta_i)_G = 1$ , so (3.4) says that these  $\zeta_i$  are indeed irreducible. (Since we are looking for a total of  $p + 4$ , our task is roughly half completed.) On the other hand,  $(\zeta_0, \zeta_0)_G = 2$ . This means (cf. (3.2)) that  $\zeta_0$  is the sum of *two* irreducible characters. It can be shown that one of these is  $1_G$ , so the other one (denoted  $\psi$  and called the **Steinberg character**) has degree  $p =$  highest power of  $p$  dividing  $G$  (cf. Steinberg [23]). Finally, when  $i = (p - 1)/2$ , we again get  $(\zeta_i, \zeta_i)_G = 2$ . In this case  $\zeta_i$  can be shown to split into a sum  $\zeta_1 + \zeta_2$ , where each  $\zeta_i$  has degree  $(p + 1)/2$ . (But the values of these characters are a bit tricky to compute.)

The series of characters just constructed “corresponds” in some sense to the family of  $p$ -regular classes represented by powers of  $a$  (this in spite of our remark following (2.2)!). So it is natural to turn to the cyclic group  $S$  of order  $p + 1$  generated by  $b$  for another series. Let  $\sigma \in \mathbf{C}$  be a primitive  $(p + 1)$ -th root of 1, and define characters of  $S$  by  $\phi_i(b^j) = \sigma^{ij}$ . So far, so good. Unfortunately,  $S$  (like  $T$ ) has large index in  $G$  but fails (unlike  $T$ ) to sit inside a larger group to which we can trivially extend  $\phi_i$ . The induced character  $\phi_i^G$  has degree  $p(p - 1)$ , and therefore could not be irreducible (cf. (2.3)).

At this point, the second technique in Section 4 for constructing characters is invoked. Consider the class function:

$$(7.1) \quad \theta_i = \zeta_i \psi - \zeta_i - \phi_i^G \quad (1 \leq i \leq (p + 1)/2).$$

The values of  $\theta_i$  are not hard to compute (Table 4). But the reason for picking  $\theta_i$  in the first place is certainly obscure; for now, just note the presence of the Steinberg character  $\psi$ . At any rate, when  $1 \leq i \leq (p - 1)/2$ ,  $(\theta_i, \theta_i)_G = 1$  (and  $\theta_i(1) > 0$ ),

1	$z$	$a^l$	$b^m$	$c$	$d$	$zc$	$zd$
$p - 1$	$(-1)^i(p-1)$	0	$-(\sigma^{im} + \sigma^{-im})$	-1	-1	$(-1)^{i+1}$	$(-1)^{i+1}$

TABLE 4. Values of  $\theta_i$

which guarantees that  $\theta_i$  is a bona fide irreducible character of  $G$ . As to  $\theta_{(p+1)/2}$ , it splits into a sum  $\eta_1 + \eta_2$  of two irreducible characters of degree  $(p-1)/2$ . Once the values of  $\eta_1, \eta_2$  are pinned down (with the aid of the orthogonality relations (3.2), (3.3)), we are in possession of  $p+4$  distinct irreducible characters, so our task is done (2.2). The results are shown in Table 5, where  $\varepsilon = (-1)^{(p-1)/2}$ . For

	1	$z$	$a^l$	$b^m$	$c$	$d$
$1_G$	1	1	1	1	1	1
$\psi$	$p$	$p$	1	-1	0	0
$\zeta_i$	$p+1$	$(-1)^l(p+1)$	$\tau^{il} + \tau^{-il}$	0	1	1
$\xi_1$	$\frac{1}{2}(p+1)$	$\frac{1}{2}\varepsilon(p+1)$	$(-1)^l$	0	$\frac{1}{2}(1 + \sqrt{\varepsilon p})$	$\frac{1}{2}(1 - \sqrt{\varepsilon p})$
$\xi_2$	$\frac{1}{2}(p+1)$	$\frac{1}{2}\varepsilon(p+1)$	$(-1)^l$	0	$\frac{1}{2}(1 - \sqrt{\varepsilon p})$	$\frac{1}{2}(1 + \sqrt{\varepsilon p})$
$\theta_1$	$p-1$	$(-1)^l(p-1)$	0	$-(\sigma^{im} + \sigma^{-im})$	-1	-1
$\eta_1$	$\frac{1}{2}(p-1)$	$-\frac{1}{2}\varepsilon(p-1)$	0	$(-1)^{m+1}$	$\frac{1}{2}(-1 + \sqrt{\varepsilon p})$	$\frac{1}{2}(-1 - \sqrt{\varepsilon p})$
$\eta_2$	$\frac{1}{2}(p-1)$	$-\frac{1}{2}\varepsilon(p-1)$	0	$(-1)^{m+1}$	$\frac{1}{2}(-1 - \sqrt{\varepsilon p})$	$\frac{1}{2}(-1 + \sqrt{\varepsilon p})$

TABLE 5. Characters of  $SL(2, p)$  (classes of  $zc, zd$  omitted)

brevity, the classes of  $zc$  and  $zd$  are omitted: for any character  $\chi$ ,  $\chi(zc) = \chi(z)\chi(1)^{-1}\chi(c)$ , and similarly for  $zd$ . It is an amusing exercise to verify directly from this table the formula (2.3) for  $|G|$ .

The characters  $\theta_i$  are rather mysterious, having been constructed in a roundabout and seemingly arbitrary way. Moreover, the *representations* to which they belong are nowhere in sight. (It is a difficult matter to construct them explicitly, cf. Tanaka [25], Silberger [20], Gel'fand [7].) In recent years a more systematic approach to the characters of groups of Lie type has been formulated by Harish-Chandra [9] (see Springer [21]), making clear why two series are to be expected here. On the other hand, Green [8] was already able around 1955 to compute explicitly the characters of the finite "general linear" groups, thus going well beyond  $SL(2, p)$ . But there are still a lot of unanswered questions.

One striking fact about Table 5 is that most of the irreducible characters have degree either  $p+1$  or  $p-1$ , these being polynomials in  $p$  with highest term  $p$  (= highest power of  $p$  dividing  $|G|$ ). Equally striking is the fact that the actual character values on  $p$ -regular classes (which account for most classes) are so simple and involve numbers such as  $\tau^{il} + \tau^{-il}$  which are in some sense "symmetric" relative to the Weyl group  $W$  discussed in Section 6. These phenomena occur for other groups of Lie type as well, so it is reasonable to look for some further explanation of them in Lie theory. This we do next.

**8. Irreducible modular representations.** For the moment let  $G$  be any finite group,  $p$  any prime dividing  $|G|$ , and  $K$  an algebraically closed field of characteristic  $p$ . As alleged in Section 1, the representations of  $G$  over  $K$  are not so well-behaved as those over  $\mathbb{C}$ . Indeed, the main results listed in Sections 2 and 3 break down com-

pletely. The “modular” theory therefore seems at first very unpromising. But since the late 1930’s Brauer and others (cf. Brauer and Nesbitt [2]), have made it a valuable tool in the study of “ordinary” representations (i.e., those over  $\mathbf{C}$ ). General references for the modular theory are Curtis and Reiner [5], Dornhoff [6, Part B].

The first interesting fact, which generalizes (2.2), is:

(8.1) *The number of (inequivalent) irreducible representations of  $G$  over  $K$  is equal to the number of  $p$ -regular conjugacy classes of  $G$ .*

However, (2.3) fails to hold over  $K$ , and the characters are not very useful: e.g., the first part of (3.4) fails, and we cannot make sense of the inner product (3.1) when  $p$  and hence  $|G|$  is 0 in  $K$ . To get around this, Brauer associated with an irreducible representation  $\rho: G \rightarrow \mathbf{GL}(n, K)$  a  $\mathbf{C}$ -valued function  $\phi$  on  $G_{\text{reg}}$  (= set of  $p$ -regular elements of  $G$ ), nowadays called the **Brauer character**. To define  $\phi$ , notice that for  $x \in G_{\text{reg}}$ , the eigenvalues of  $\rho(x)$  are certain roots of unity in  $K$ , of order relatively prime to  $p$ , and their sum is the trace of  $\rho(x)$  (the usual character). We just replace these eigenvalues by corresponding complex roots of unity and call the sum  $\phi(x)$ . If  $r$  = number of  $p$ -regular classes, denote by  $\phi_1, \dots, \phi_r$  the corresponding irreducible Brauer characters. The usefulness of these functions is indicated by:

(8.2)  *$\phi_1, \dots, \phi_r$  form a basis of the vector space (over  $\mathbf{C}$ ) of  $\mathbf{C}$ -valued class functions on  $G_{\text{reg}}$ . An (ordinary) character of  $G$ , restricted to  $G_{\text{reg}}$ , is a nonnegative integral linear combination of the  $\phi_i$ .*

In particular, the restrictions to  $G_{\text{reg}}$  of the (ordinary) irreducible characters  $\chi_1, \dots, \chi_s$  of  $G$  can be expressed as:

$$(8.3) \quad \chi_i = \sum_{j=1}^r d_{ij} \phi_j \quad (d_{ij} \in \mathbf{Z}^+).$$

The integers  $d_{ij}$  form an  $s \times r$  matrix  $D$ , called the **decomposition matrix** of  $G$  (relative to  $p$ ). In terms of actual representations, (8.3) reflects the fact that the representation with character  $\chi_i$  may be “reduced modulo  $p$ ” to obtain a representation over  $K$  whose composition factors have the indicated Brauer characters with multiplicities  $d_{ij}$ .

The point of all this is that a knowledge of  $D$  and of the  $\phi_j$  would enable us to write down that portion of the character table of  $G$  corresponding to  $G_{\text{reg}}$ . When  $G = \mathbf{SL}(2, p)$ , virtually all classes are  $p$ -regular, so this would be a very large portion. Of course, it seems at this stage no easier to find  $D$  and the Brauer characters than to find the  $\chi_i$ . (We mention, in passing, that in principle  $D$  itself can be found if all  $\chi_i$  and  $\phi_j$  are known. This is quite hard to do in practice — cf. Srinivasan [22]. And, of course, it tends to defeat the purpose of the theory!)

Now let  $G = \mathbf{SL}(2, p)$  again (and let the prime in question be  $p$ ). Lie theory actually provides a systematic procedure for constructing all the irreducible modular

representations of  $G$ . We view  $G$  as acting on a 2-dimensional vector space over  $K$ , with basis  $(e_1, e_2)$ , and we extend that action in a natural way to the space of homogeneous polynomials of degree  $\lambda \geq 0$  in  $e_1$  and  $e_2$  (viewed as indeterminates). This space of polynomials has dimension  $\lambda + 1$ , with basis  $(e_1^\lambda, e_1^{\lambda-1}e_2, \dots, e_2^\lambda)$ , and is denoted  $M_\lambda$ . For instance,

$$a = \begin{pmatrix} v & 0 \\ 0 & v^{-1} \end{pmatrix}$$

sends  $e_1$  to  $ve_1$  and  $e_2$  to  $v^{-1}e_2$ , so it must send  $e_1^3e_2$  to  $(ve_1)^3(v^{-1}e_2) = v^2(e_1^3e_2)$ . It is not too hard to verify that the resulting  $G$ -module is irreducible provided  $0 \leq \lambda < p$ . (For  $\lambda = 0$ , we just get  $1_G$ .) So we obtain irreducible Brauer characters of degrees  $1, 2, \dots, p$ . Since there are just  $p$   $p$ -regular classes (Section 6), (8.1) insures that we need look no further.

The case  $\lambda = p - 1$  is especially interesting. Here the reader can verify that the Brauer character agrees on  $G_{\text{reg}}$  with the *Steinberg character*  $\psi$  constructed in Section 7. In fact, the representation  $M_{p-1}$  is precisely the “reduction modulo  $p$ ” of the ordinary representation whose character is  $\psi$ .

**9. Lie algebra representations.** The construction of  $G$ -modules in Section 8 is straightforward, but does not fully reveal the influence of Lie theory. So we shall give a slightly more abstract version, based on the **Lie algebra**  $\mathfrak{g} = \mathfrak{sl}(2, K)$ , which is by definition the set of all  $2 \times 2$  matrices over  $K$  having trace 0.  $\mathfrak{g}$  is closed under addition and scalar multiplication, so it is a vector space over  $K$ . One basis consists of

$$h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

$\mathfrak{g}$  is also closed under a bilinear (but not associative) “product” operation:  $[u, v] = uv - vu$ .

A **representation** of  $\mathfrak{g}$  is just a linear transformation  $\rho: \mathfrak{g} \rightarrow \mathbf{M}(n, K)$  (= space of all  $n \times n$  matrices over  $K$ ) such that  $\rho[u, v] = \rho(u)\rho(v) - \rho(v)\rho(u)$ . As for group representations, there is a natural notion of “equivalence,” and  $K^n$  can be viewed as a “ $\mathfrak{g}$ -module.”

The analogous Lie algebra over  $\mathbf{C}$  has a well-known series of irreducible representations, which in dimensions  $\leq p$  adapt at once to  $\mathfrak{g}$ . Letting  $(e_0, \dots, e_\lambda)$  be a basis for  $K^{\lambda+1}$ , we simply prescribe:

$$(9.1) \quad \begin{aligned} \rho(h)e_i &= (\lambda - 2i)e_i, \\ \rho(x)e_i &= (\lambda - i + 1)e_{i-1} \quad (e_{-1} = 0), \\ \rho(y)e_i &= (i + 1)e_{i+1} \quad (e_{\lambda+1} = 0). \end{aligned}$$

The reader can check that this recipe yields a representation of  $\mathfrak{g}$  (of degree

$\lambda + 1$ ). What is more, the  $G$ -module  $M_\lambda$  of Section 8 can in a sense be identified with this  $\mathfrak{g}$ -module, via "exponentiation." We give a rough idea of how this works. If  $A$  is any square matrix, then  $\exp A = 1 + A + A^2/2! + A^3/3! + \dots$  may or may not be a well-defined matrix over  $K$ . Since division by  $p$  is impossible in  $K$ , one clearly has to require that  $A^p = 0$ . For instance,  $\exp \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}$  is defined and equals  $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ . It turns out that we can exponentiate the matrix  $\rho(x)$  or  $\rho(y)$  given by (9.1) and thereby get matrices representing elements of  $G$  on  $M_\lambda$ .

This needs to be made more precise, of course, but it will suffice to indicate how  $\mathfrak{g}$  is brought into the picture. For more details, consult Curtis [4], Steinberg [24].

**10. Principal indecomposable modules.** In Section 8 we pointed out the desirability of finding the decomposition matrix  $D$  (without first knowing  $\chi_1, \dots, \chi_s$ ). It happens that  $D$  is related in a remarkable way to another matrix of integers, which we now explain.

Consider briefly the case of an arbitrary finite group  $G$ . Maschke's Theorem (2.1) breaks down rather badly in characteristic  $p$ , when  $p$  divides  $|G|$ , leaving us with a vast assortment of indecomposable representations other than the irreducible ones. (Since  $SL(2, p)$  has cyclic  $p$ -syllow subgroups, it is actually possible in this case to classify them to some extent, cf. Janusz [14]. But this seems beyond reach for other groups of Lie type.) Fortunately, some of these are both useful and manageable. As in Section 2, we can construct the regular representation of  $G$  (over  $K$ ) and decompose it via the Krull-Schmidt Theorem into a direct sum of indecomposables. These are called the **principal indecomposable modules** (PIM's for short). Two pleasant facts emerge:

(10.1) *There is a natural 1-1 correspondence between PIM's and irreducible modular representations of  $G$ , each of the latter occurring as unique "top" composition factor of its PIM. Moreover, a PIM occurs as many times in the regular representation as the degree of the associated irreducible representation.*

(10.2) *The degree of a PIM is divisible by the highest power of  $p$  dividing  $|G|$ .*

Denoting by  $\eta_i$  the Brauer character of the PIM corresponding to  $\phi_i$  ( $1 \leq i \leq r$ ), we can write (thanks to (8.2)):

$$(10.3) \quad \eta_i = \sum_{j=1}^r c_{ij} \phi_j \quad (c_{ij} \in \mathbf{Z}^+).$$

The  $r \times r$  matrix  $C = (c_{ij})$  is called the **Cartan matrix** of  $G$  (relative to  $p$ ). It satisfies:

(10.4)  $C = D^t D$  ( $D^t =$  transpose of  $D$ ); in particular,  $C$  is symmetric.

(10.5) *The determinant of  $C$  is a certain (predictable) power of  $p$ .*

$C$  can therefore be found once  $D$  is known. (Brauer also showed how to compute  $C$  — in principle, but rarely in practice — if only  $\phi_1, \dots, \phi_r$  are known.) Conversely,  $D$  can sometimes be reconstructed from a knowledge of  $C$  and this turns out to be the case for  $\mathbf{SL}(2, p)$ !

An example may help to fix the ideas. Take  $G = S_3, p = 2$ . There are two  $p$ -regular classes (those of 1 and (123)), hence two irreducible representations over  $K$ : the 1-representation and the (reduction modulo 2 of the) degree 2 representation constructed in Section 2. Table 6 gives the Brauer characters. Comparison with Table 1 shows that

	1	(123)
$\phi_1$	1	1
$\phi_2$	2	-1

TABLE 6. Brauer characters of  $S_3, p = 2$

$$D^t = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore,  $C = D^t D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$  (and  $\det C = 2$ ).

The general set-up may still seem to be hopelessly complicated (perhaps the reader wishes we had quit while we were ahead, at the end of Section 7). But the strategy is a simple one: to “trap” the ordinary characters  $\chi_i$  of a group  $G$  between the  $\eta_i$  and the  $\phi_i$ . Indeed, (10.4) comes essentially from the fact that each  $\eta_i$  is a sum of certain  $\chi_j$  (or their restrictions to  $G_{\text{reg}}$ ), while each  $\chi_j$  is a sum of certain  $\phi_i$  in a reciprocal fashion.

Henceforth,  $G = \mathbf{SL}(2, p)$ . Denote by  $R_\lambda$  the PIM corresponding to  $M_\lambda$  ( $0 \leq \lambda < p$ ), as in (10.1). Since  $\dim M_\lambda = \lambda + 1$ , (10.2) makes it clear that  $M_\lambda$  is strictly smaller than  $R_\lambda$  except possibly when  $\lambda = p - 1$ . In fact:

(10.6)  $R_{p-1} = M_{p-1}$  (Steinberg representation).

**11. PIM’s for the Lie algebra.** Now the Lie algebra  $\mathfrak{g} = \mathfrak{sl}(2, K)$  re-enters the picture. It happens that  $\mathfrak{g}$  too has PIM’s. The “regular representation” here involves the so-called “restricted universal enveloping algebra,” an algebra of dimension  $p^3$  over  $K$  which we shall not attempt to describe further. (10.1) carries over verbatim:

(11.1) *There is a natural 1-1 correspondence between PIM’s  $Q_\lambda$  and irreducible modular representations  $M_\lambda$  ( $0 \leq \lambda < p$ ),  $Q_\lambda$  occurring as often as the degree of  $M_\lambda$ .*

Pollack [18] studied these PIM’s in detail and found (cf. (10.2), (10.6)):

(11.2)  $Q_{p-1} = M_{p-1}$  (Steinberg representation). *If  $0 \leq \lambda < p - 1$ , then  $Q_\lambda$  has degree  $2p$ ; its composition factors are  $M_\lambda$  and  $M_{p+2-\lambda}$ , each repeated twice.*

These results were explained (and generalized) by Humphreys [10] (cf. Verma [26]), in a way which makes plain the role of the *Weyl group*. (For example, the 2 in  $2p$  results from the fact that  $W$  has order 2.) Here  $W$  appears as a group of order 2 acting on the subspace  $\mathfrak{h}$  of diagonal matrices in  $\mathfrak{g}$ : the nontrivial element of  $W$  sends  $h$  to  $-h$ .  $W$  acts equally on the numbers  $\lambda$ , which in Lie theory are viewed as linear functions on  $\mathfrak{h}$  and called **weights**:  $\lambda$  is sent to  $\pm \lambda$ . The weight 1 plays a special role and gets the special name  $\delta$ . Now define weights  $\lambda, \mu$  to be **linked** if  $w(\lambda + \delta) \equiv (\mu + \delta) \pmod{p}$  for some  $w \in W$ . This is an equivalence relation, with equivalence classes:

$$(11.3) \quad \{0, p-2\}, \{1, p-3\}, \dots, \{p-1\}.$$

It is no accident that these pairs (or the single weight  $p-1$ ) also occur in (11.2):

(11.4) *If  $M_\lambda$  and  $M_\mu$  occur as composition factors of any indecomposable representation of  $\mathfrak{g}$ , then  $\lambda$  and  $\mu$  must be linked.*

In effect, then, each PIM  $Q_\lambda$  ( $\lambda \neq p-1$ ) involves a single linkage class, repeated twice. And in each such case,  $\dim M_\lambda + \dim M_{p-2-\lambda} = p$ .

**12. Comparison of PIM's.** The results of Section 11 are pleasant, but of course one has to ask what bearing they have on  $G$ . Recent work of Jeyakumar [15], Humphreys [11, 12], Humphreys and Verma [13], reveals the following pattern:  $G$  and  $\mathfrak{g}$  share the same irreducible representations  $M_\lambda$ . They *almost* share the same PIM's — but not quite, since the regular representation of  $G$  has degree  $p^3 - p$  while that of  $\mathfrak{g}$  has degree  $p^3$  (cf. (10.1), (11.1)). In fact  $Q_\lambda$  may be constructed as a summand of a suitable "tensor product"  $M_\mu \otimes M_{p-1}$ ; the latter is also a representation of  $G$ , and it turns out that  $Q_\lambda$  is stable under the action of  $G$ . What is more:

(12.1)  *$Q_\lambda$  (viewed as a representation of  $G$ ) involves  $R_\lambda$  as a summand. In particular,  $\dim R_\lambda \leq \dim Q_\lambda \leq 2p$ .*

By counting dimensions and using the last assertion of (10.1), the reader will see quickly that all but one  $R_\lambda$  must coincide with  $Q_\lambda$  (viewed as a representation of  $G$ ). The odd case turns out to be:  $Q_0 = R_0 + R_{p-1}$ .

The tensor product involved here begins to shed light on the mysterious formula (7.1), and points up the pivotal role of the Steinberg representation (which is unique in being both irreducible and a PIM). On a more practical level, the tensor product construction yields precise information about  $R_\lambda$ , obtained earlier only by resort to Brauer's theory or a knowledge of ordinary characters (cf. [11], [15]):

(12.2) *The composition factors of  $R_\lambda$  ( $0 \leq \lambda < p-1$ ) are:  $M_\lambda, M_{p-1-\lambda}, M_\lambda, M_{p-3-\lambda}$  (the last omitted if  $p-3-\lambda < 0$ ).*

In particular, the matrix  $C$  can now be written down explicitly (for any given  $p$ ). Evidently  $p$  plays no essential role in the general pattern: there are three diagonal

blocks, one the  $1 \times 1$  matrix (1) corresponding to the Steinberg representation, the other two of the form illustrated in Table 7 (entries not shown being 0).

$$\left[ \begin{array}{cccccccc} 2 & 1 & & & & & & \\ 1 & 2 & 1 & & & & & \\ & 1 & 2 & 1 & & & & \\ & & 1 & 2 & & & & \\ & & & & \cdot & \cdot & \cdot & \\ & & & & & & & 1 \\ & & & & & & & \cdot \\ & & & & & & & 2 & 1 \\ & & & & & & & 1 & 2 & 1 \\ & & & & & & & & & 1 & 3 \end{array} \right]$$

TABLE 7. A block of  $C$

With a little effort, the reader can use the equation (10.4) to reconstruct the matrix  $D$ , whose entries are all 0 or 1 (cf. Brauer and Nesbitt [2, p. 590]). The fact that  $D$  can be recovered in one and only one way from  $C$  is a special fact about  $\mathrm{SL}(2, p)$ , which fails for most groups (but does seem to persist for some other groups of Lie type). At any rate, without using the results of Section 7, most of the character table of  $G$  for a given  $p$  can in principle be written down using just the modular theory! We shall see below how well it can be done in practice.

It has to be added that Brauer, Dade, and others have been able to derive these results about the modular theory of  $\mathrm{SL}(2, p)$  in another (very different) way, by means of a deep general theory (cf. Dornhoff [6, Part B, §71], Alperin and Janusz [1]). But this general theory does *not* apply to other groups of Lie type, so we avoid discussing it here.

**13. The role of the Weyl group.** The calculation of  $C$  (and then  $D$ ) sketched in Section 12 does not yet explain adequately the regularities encountered earlier.

A closer look at  $D$  (cf. (12.2)) reveals that  $M_\lambda, M_{p+1-\lambda}$  (resp.  $M_\lambda, M_{p+3-\lambda}$ ) occur together in the decomposition of some ordinary character of degree  $p+1$  (resp.  $p-1$ ). It is suggestive to view each pair of weights  $\{\lambda, p-1-\lambda\}$  or  $\{\lambda, p-3-\lambda\}$  as a **deformation** of the linkage class  $\{\lambda, p-2-\lambda\}$ . These two deformations can be assigned in a precise way, *independent of  $p$* , to the two elements (or conjugacy classes) of  $W$ , as follows. Say  $W = \{e, w\}$ ,  $w^2 = e$ . Set  $\delta_e = 0$ ,  $\delta_w = \delta (= 1)$ . Then:



(13.1) *The element  $e$  deforms the linkage class  $\{\lambda, p-2-\lambda\}$  by adding  $e(\delta_e) = 0$  to  $\lambda$  and  $e(\delta_w) = 1$  to  $p-2-\lambda$ . The element  $w$  deforms this class by adding  $w(\delta_e) = 0$  to  $\lambda$  and  $w(\delta_w) = -1$  to  $p-2-\lambda$ .*

From this perspective, the dimension polynomial  $p = \dim M_\lambda + \dim M_{p-2-\lambda}$  is being "deformed" to yield either  $p+1$  or  $p-1$ . In defense of this formulation, which appears at first sight artificial and overly elaborate, we remark that (a) it describes the observed facts, (b) it generalizes to some other groups of Lie type, (c) it ties in with the suspicion on other grounds that the "series" of ordinary characters found in Section 7 are somehow connected with the conjugacy classes of  $W$ . (The classes of  $W$  are known in any case to lead to the two families of  $p$ -regular classes described in Section 6.)

The above pairs of weights also tie in neatly with the simple form taken by the actual *character values* on  $p$ -regular classes (Table 5). An example should make this clear. Take  $p = 13$ ,  $\lambda = 8$ . Then

$$a = \begin{pmatrix} v & 0 \\ 0 & v^{-1} \end{pmatrix}$$

is represented on  $M_\lambda$  by a diagonal matrix whose diagonal entries are the following powers of  $v$ : 8, 6, 4, 2, 0, -2, -4, -6, -8. Replacing  $v$  by  $\tau$ , a primitive  $(p-1)$ -th root of 1 in  $\mathbf{C}$ , we see that the Brauer character of  $M_\lambda$  assigns to  $a$  the number:  $\tau^8 + \tau^6 + \dots + \tau^{-8}$ . Since  $\tau^{12} = 1$ , the exponents here can equally well be thought of as: 8, 6, 4, 2, 0, 10, 8, 6, 4. Now the other weight in the pair  $\{\lambda, p-1-\lambda\}$  is 4, and similar reasoning leads to the exponents: 4, 2, 0, 10, 8. So the Brauer character of  $M_8 + M_4$  assigns to  $a$  the corresponding sum of powers of  $\tau$ . But each even exponent from 0 to 10 occurs in the combined list exactly twice, except that 8 and 4 each occur three times. Since  $\tau$  is a root of  $X^{12} - 1$ , but not of  $X^2 - 1$ ,  $\tau$  is also a root of

$$(X^{12} - 1)/(X^2 - 1) = X^{10} + X^8 + X^6 + X^4 + X^2 + 1.$$

So most terms in the Brauer character add up to 0, leaving just:  $\tau^8 + \tau^4 (= \tau^{-4} + \tau^4)$ .

On the other hand, the Brauer character of  $M_8$  assigns to the element  $b$  a sum of powers of  $\sigma$ , a primitive  $(p+1)$ -th root of 1, the exponents (modulo 14) being: 8, 6, 4, 2, 0, 12, 10, 8, 6. For  $M_4$  the exponents are: 4, 2, 0, 12, 10. Here the combined list contains each even exponent from 0 to 12 exactly twice. But  $\sigma$  is a root of  $X^{12} + X^{10} + \dots + 1$ , so the Brauer character assigns to  $b$  the value 0. This is not unexpected (if we know Table 5), since the preceding paragraph already showed that the *ordinary character* in question must be  $\zeta_4$ .

The other pair to which the weight 8 belongs is  $\{8, 2\}$ . Here  $a$  is assigned the list of exponents (modulo 12): 8, 6, 4, 2, 0, 10, 8, 6, 4 and 2, 0, 10. So the Brauer character has value 0 at  $a$ . On the other hand,  $b$  is assigned exponents (modulo 14): 8, 6, 4, 2, 0

12, 10, 8, 6 and 2, 0, 12. Here each even exponent occurs twice, except that 10 and 4 only occur once. So the Brauer character assigns to  $b$  the value  $-(\sigma^{10} + \sigma^4)$ . We recognize the ordinary character in question as  $\theta_4$ .

**14. Conclusion.** The reader who has persisted this far might want to look at some of the cited references in order to see how the actual *proofs* go, and how to treat the groups  $\mathrm{SL}(2, p^n)$  as well. Admittedly, there is a lot of general theory mixed into the study of these particular representations. But, in compensation, there are still many fascinating open questions about the other groups of Lie type, posed within this same framework. The reader may want to have a hand in settling them.

#### References

1. J. L. Alperin, G. J. Janusz, Resolutions and periodicity, *Proc. Amer. Math. Soc.*, 37 (1973) 403–406.
2. R. Brauer, C. Nesbitt, On the modular characters of groups, *Ann. of Math.*, 42 (1941) 556–590.
3. R. W. Carter, *Simple Groups of Lie Type*, Interscience, New York, 1972.
4. C. W. Curtis, Representations of Lie algebras of classical type with application to linear groups, *J. Math. Mech.*, 9 (1960) 307–326.
5. C. W. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras* Interscience, New York, 1962.
6. L. Dornhoff, *Group Representation Theory*, M. Dekker, New York, 1971 (Part A): 1972 (Part B).
7. S. I. Gel'fand, Representations of the full linear group over a finite field, *Math. USSR-Sb.*, 12 (1970) 13–39.
8. J. A. Green, The characters of the finite general linear groups, *Trans. Amer. Math. Soc.*, 80 (1955) 402–447.
9. Harish-Chandra, Eisenstein series over finite fields, in: *Functional Analysis and Related Fields*, ed. F. E. Browder, Springer, New York, 1970.
10. J. E. Humphreys, Modular representations of classical Lie algebras and semisimple groups, *J. Algebra*, 19 (1971) 51–79.
11. ———, Projective modules for  $\mathrm{SL}(2, q)$ , *J. Algebra*, 25 (1973) 513–518.
12. ———, Some computations of Cartan invariants for finite groups of Lie type, *Comm. Pure Appl. Math.*, 26 (1973) 745–755.
13. J. E. Humphreys, D.-N. Verma, Projective modules for finite Chevalley groups, *Bull. Amer. Math. Soc.* 79 (1973) 467–468.
14. G. J. Janusz, Indecomposable modules for finite groups, *Ann. of Math.*, 89 (1969) 209–241.
15. A. V. Jeyakumar, Principle indecomposable representations for the group  $\mathrm{SL}(2, q)$ , *J. Algebra*, 30 (1974) 444–458.
16. H. Jordan, Group characters of various types of linear groups, *Amer. J. Math.*, 29 (1907) 387–405.
17. M. Klemm, Charakterisierung der Gruppen  $\mathrm{PSL}(2, p^f)$  und  $\mathrm{PSU}(3, p^{2f})$  durch ihre Charaktertafel, *J. Algebra*, 24 (1973) 127–153.
18. R. D. Pollack, Restricted Lie algebras of bounded type, *Bull. Amer. Math. Soc.*, 74 (1968) 326–331.
19. I. Schur, Untersuchungen über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. Reine Angew. Math.*, 132 (1907) 85–137.
20. A. J. Silberger, An elementary construction of the representations of  $\mathrm{SL}(2, GF(q))$ , *Osaka J. Math.*, 6 (1969) 329–338.

21. T. A. Springer, Cusp forms for finite groups; Characters of special groups; in: Seminar on Algebraic Groups and Related Finite Groups, Lect. Notes in Math. 131, Springer, New York, 1970.
22. B. Srinivasan, On the modular characters of the special linear group  $SL(2, p^n)$ , Proc. London Math. Soc. (3), 14 (1964) 101–114.
23. R. Steinberg, Prime power representations of finite linear groups II, Canad. J. Math., 9 (1957) 347–351.
24. ———, Representations of algebraic groups, Nagoya Math. J., 22 (1963) 33–56.
25. S. Tanaka, Construction and classification of irreducible representations of the special linear group of the second order over a finite field, Osaka J. Math., 4 (1967) 65–84.
26. D.-N. Verma, Role of affine Weyl groups in the representation theory of algebraic Chevalley groups and their Lie algebras, in: Proc. 1971 Summer School on Group Representations, ed. I.M. Gel'fand, to appear.
27. R. W. van der Waall, Remarks on the Artin  $L$ -functions of the groups  $GL_2(F_3)$  and  $SL_2(F_3)$ , Indag. Math., 35 (1973) 41–48.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MASSACHUSETTS, AMHERST, MA 01002.

---

## QUERIES

EDITED BY A. C. ZITRONENBAUM

*This Department welcomes queries from readers about mathematics at the collegiate level, such as sources for exposition of a particular topic from a special point of view, references to vaguely remembered articles, descriptions of special kinds of courses or teaching methods, and methods constructing illustrative examples for exercises of particular kinds (questions on research topics should, in general, be addressed to the "Queries Department" of the Notices of the American Mathematical Society). Replies will be forwarded to the questioner and may be edited into a composite answer for publication in this Department. Consequently all items submitted for consideration for possible publication should include the name and complete mailing address of the person who is to receive the reply. Queries and answer should be sent to A. C. Zitronenbaum, Department of Mathematics, Cornell University, Ithaca, NY 14853.*

17. Can anyone supply the Monthly with a complete list of programmed or individualized self-instruction texts in arithmetic, algebra, geometry and calculus for use in developmental classes in two or four-year colleges?

18. **A. B. Willcox.** Can anyone supply the name and address of a firm that manufactures mathematical models for educational use in university courses? Until the middle 60's such models were available from a German firm, Rudolf Stoll KG, but this firm seems to have gone out of business.