REPRESENTATIONS OF ALGEBRAIC GROUPS

ROBERT STEINBERG*

To Professor RICHARD BRAUER on the occasion of his 60th birthday

§ 1. Introduction

Our purpose here is to study the irreducible representations of semisimple algebraic groups of characteristic $p \neq 0$, in particular the rational representations, and to determine all of the representations of corresponding finite simple groups. (Each algebraic group is assumed to be defined over a universal field which is algebraically closed and of infinite degree of transcendence over the prime field, and all of its representations are assumed to take place on vector spaces over this field.)

To state our first principal result, we observe that relative to a Cartan decomposition of a semisimple algebraic group, there is described in § 5 below (in a somewhat more general context) a standard way of converting an isomorphism on the universal field into one on the group, and that relative to a choice of a set S of simple roots, an irreducible rational projective representation of the group is characterized by a function from S to the nonnegative integers, to be called, together with the corresponding function on the Cartan subgroup of the decomposition, the high weight of the representation [13, Exp. 14 and 15].

1.1 THEOREM. *Let G be a semisimple algebraic group of characteristic $p \neq 0$ and rank l, and let $\mathfrak{R}$ denote the set of p^l irreducible rational projective representations of G in each of which the high weight λ satisfies $0 \leq \lambda(a) \leq (p-1)$ $(a \in S)$. Let α_i denote the automorphism $t \to t^{p^i}$ of the universal field as well as the corresponding automorphism (see § 5) of G, and for $R \in \mathfrak{R}$ let R^{α_i} denote the composition of α_i and R. Then every irreducible rational projective representation of G can be written uniquely as $\Pi_{i=0}^{\infty} R_i^{\alpha_i}$ (weak tensor product, $R_i \in \mathfrak{R}$).*

Received May 21, 1962.

* This research was supported by the Air Force Office of Scientific Research.

Conversely, every such product yields an irreducible rational projective representation of G.

This follows from 6.1 below. We need only remark here that there is no corresponding phenomenon for groups of characteristic 0, since then the identity is the only rational field automorphism and the tensor product of two rational representations is never irreducible unless one of them is one-dimensional. Related to 1.1 is the following conjecture for which there is much evidence and for which a proof for the group of type A_1 would go a long way.

1.2 CONJECTURE. *If G and $\mathfrak{R}$ are as in 1.1 and R is an irreducible, not necessarily rational, projective representation of G, there exist distinct isomorphisms β_i of the universal field into itself and corresponding representations R_i in $\mathfrak{R}$ such that $R = \prod R_i^{\beta_i}$ (see § 5 for the definition of $R_i^{\beta_i}$).*

That the above product is always irreducible follows from 5.1 below.

Our second main result applies to naturally defined finite simple subgroups of the groups considered above. These include all the "finite simple algebraic groups" (those made up of the rational points of simple algebraic groups suitably defined over finite fields), that is (see Hertzig [8]), the groups considered by Chevalley [3] and those considered by Hertzig [8], Tits [24, 25] and the author [19, 20], and also include the nonalgebraic groups considered by Suzuki [22] and Ree [11], all the known finite simple groups other than the cyclic, alternating and Mathieu groups.

1.3 THEOREM. *If G is a finite simple algebraic group and the rational field has $q = p^n$ elements, then every irreducible projective representation is the restriction of a rational representation of the corresponding infinite algebraic group. If the rank is l, the number of such representations is q^l. Each has a high weight λ for which $0 \leq \lambda(a) \leq q-1$ $(a \in S)$.*

Here we also have the product representation of 1.1 with the upper limit n in place of ∞ (see 7.4 and 9.3). For the nonalgebraic finite groups mentioned above there is a corresponding result (12.2 below), but the relevant representations of the containing infinite algebraic groups are those that satisfy the further condition: $\lambda(a) = 0$ if a is long; hence their number is $q^{l/2}$. A gap in our development is that for finite odd-dimensional unitary groups and finite

Ree groups of type G_2 we have established these results, and also the following (see 8.1, 8.2, 9.6 and 12.5) only for ordinary representations, not for projective representations.

1.4 THEOREM. *Each of the finite groups above, algebraic or not, has an irreducible (ordinary) representation of dimension equal to the order of a p-Sylow subgroup. No other irreducible (projective or ordinary) representation has as high a dimension.*

Among the subsidiary results below, we consider the character of this highest representation (8.4, 9.6, 11.3), and present in §§10 and 11 some results related to those rather special isogenies which give rise to the existence of the groups of Suzuki and Ree.

In addition to [13], to which frequent references will be made, earlier work related to our results is as follows. In [2] Brauer and Nesbitt determine the irreducible representations of finite groups of type $SL(2)$ and prove the appropriate tensor product theorem, while in [13, Exp. 20] Chevalley does the same for rational representations of the corresponding infinite groups. In [10] Mark considers the finite groups of type $SL(3)$, while in [27] Wong considers groups of type $SL(l+1)$ and $Sp(l)$ and proves 1.1, 1.3 and 1.4 for ordinary representations. His methods, however, are quite different from ours, and are not readily extendable to the other types of groups. Our methods are closely related to those of Curtis in [4] where the representations of $\mathfrak{R}$ in 1.1 are constructed by infinitesimal methods and in [5] where they are shown to remain irreducible on restriction to the corresponding finite Chevalley groups (under the assumption $p>7$, which can easily be removed).

§2. Classical Lie algebras

Let $\mathfrak{g}_C$ be a simple Lie algebra over the complex field C, $\mathfrak{h}_C$ a Cartan subalgebra, $\sum$ the (ordered) system of roots relative to $\mathfrak{h}_C$, S the set of simple positive roots, and for each pair r, s of roots, set $c_{rs}=2(r, s)/(s, s)$, and define p_{rs} to be 0 if $r+s$ is not a root, otherwise to be the least positive integer p for which $r-ps$ is not a root. Then Chevalley [3, p. 24] has shown that there exists a generating set $\{X_r, H_r \mid r\in\sum\}$ such that the equations of structure of $\mathfrak{g}_C$ are:

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

2.1. $H_{-r} = -H_r \qquad (r \in \sum)$.

2.2. $H_{r+is} = H_r + H_s$ *if* i *is a positive integer and* $r+is$ *and* r *have the maximum root length.*

2.3. $[H_r, H_s] = 0 \qquad (r, s \in \sum)$.

2.4. $[H_r, X_s] = c_{sr}X_s \qquad (r, s \in \sum)$.

2.5. $[X_r, X_{-r}] = H_r \qquad (r \in \sum)$.

2.6. $[X_r, X_s] = \pm p_{rs}X_{r+s} \qquad (r, s \in \sum, r+s \neq 0)$.

Let $\mathfrak{g}$ and $\mathfrak{h}$ denote the algebras obtained by shifting the coefficients to an arbitrary field K of characteristic p. Then X_r and H_r shall be considered to belong to $\mathfrak{g}$ but the subscript r shall continue to denote an element of $\sum$. For the algebras just constructed, Curtis [4] has developed a theory of irreducible representations quite analogous to the classical theory in characteristic 0. Although he states and proves his results under the assumption that K is algebraically closed and $p>7$, his proofs can be modified to apply to the present situation. We recall that a representation ρ of $\mathfrak{g}$ is restricted if $\rho(X_r)^p = 0$ and $\rho(H_r)^p = \rho(H_r)$ for each root r.

2.7 Curtis. *With* $\mathfrak{g}$ *as above, every irreducible restricted* $\mathfrak{g}$*-module* M *contains a nonzero element* v_+*, uniquely determined to within multiplication by a scalar, such that* $X_r v_+ = 0$ *if* r *is positive, and there exist integers* $\lambda(a)$*,* $0 \leq \lambda(a) \leq p-1$*, such that* $H_a v_+ = \lambda(a)v_+ (a \in S)$. *Inequivalent modules yield distinct sequences* $\lambda(a)$*, and all sequences are realized. Thus there are* p^l *modules for an algebra of rank* l.

Here and elsewhere in the paper, "$\mathfrak{g}$-module" means vector space over the algebraic closure $\overline{K}$ of K on which $\overline{K}$ and $\mathfrak{g}$ act according to the usual rules, "irreducible" means absolutely irreducible, and $\mathfrak{M}$ denotes the p^l modules given by 2.7. As is easily seen, the modules of $\mathfrak{M}(\mathfrak{g}_{\overline{K}})$ may be viewed as extensions of those of $\mathfrak{M}(\mathfrak{g}_K)$, or equivalently, the latter as restrictions of the former. For each $M \in \mathfrak{M}$, v_+ is called a high vector and the linear function λ on $\mathfrak{h}$ defined by $\lambda(H_a) = \lambda(a)$ the high weight of M. Further for a positive root $r = \sum n(a)a \ (a \in S)$, we set $\operatorname{ht} r = \sum n(a)$, the height of r, then order the positive roots $r_1, r_2, \ldots, r_m$ in a manner consistent with heights (if $\operatorname{ht} r_i < \operatorname{ht} r_j$, then $i<j$), and for the monomial

$$v = X_{-r_m}^{i_m} \cdots X_{-r_2}^{i_2} X_{-r_1}^{i_1} v_+ \qquad (0 \leq i_k \leq p-1) \tag{2.8}$$

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

set ht $v = -\sum i_k$ ht r_k, and finally call w homogeneous of height n if it is a linear combination of monomials of height n. We recall that a basis for M can be selected from the monomials.

2.9 LEMMA. *Nonzero vectors of different heights are linearly independent.*

Proof. Given a relation $v_0 + v_1 + \cdots + v_d = 0$ with v_i of height $-i$, we prove by induction on d that each v_i is 0. If $d = 0$, this is clear.
Assume $d > 0$. If r is any positive root, $X_r v_0 + X_r v_1 + \cdots + X_r v_d = 0$, and since $X_r v_i$ is higher than v_i, the induction assumption yields $X_r v_d = 0$. Thus by 2.7, $v_d \in Kv_+$, and since the algebra generated by those X_{-r} for which $r > 0$ acts nilpotently on M because M is restricted, $v_d = 0$. Then each v_i is 0 by the induction assumption.

§ 3. Classical algebraic groups

Now set $x_r(t) = \exp \operatorname{ad} t X_r$ $(t \in K,\ r \in \sum)$, and let G (this is G' in [3]) denote the group generated by all of these automorphisms. With 4 exceptions [3, p. 63], which we henceforth exclude, G is simple. In G there are commutator relations [3, p. 36]:

3.1. $$(x_r(t),\ x_s(u)) = \prod x_{ir+js}(C_{ij,rs}\, t^i u^j) \qquad (r,\ s \in \sum,\ r + s \neq 0).$$

Here the product is taken over all positive integers i, j for which $ir + js$ is a root, the terms being arranged in some fixed, but arbitrary, order, and the $C_{ij,rs}$ are integers that depend on the order, but not on t, u or the field K. We also have from [3, p. 36]:

3.2. *For each positive root r there is a homomorphism φ_r of $SL(2, K)$ into G such that $\varphi_r\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = x_r(t)$ and $\varphi_r\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = x_{-r}(t)$.*

Together with G, we consider a covering group Γ, the abstract group generated by a set of elements $x_r(t)\,(t \in K,\ r \in \sum)$ subject to the relations 3.1 and those implied by 3.2 with Γ in place of G. That these relations define $SL(l+1, K)$ and $Sp(l, K)$ for $\sum$ of type A_l and C_l respectively was already known to Dickson [7]. The properities of Γ that we require, 3.3 to 3.6 below, are taken from [21].

3.3. *Each φ_r is an isomorphism.*

3.4. *Γ is equal to its commutator subgroup.*

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

3.5. *If* $h_a(t) = \varphi_a(\mathrm{diag}(t, t^{-1}))$ *and* $h_a = \{h_a(t) | t \in K^*\}$, *the* h_a ($a \in S$) *generate a subgroup* H *as a direct product.*

For each $r \in \sum$ the symbol r is also used to denote the root on H: $\prod h_a(t_a) \to \prod t_a^{c_{ra}}$ (see 2.4).

3.6. *The center* C *of* Γ *consists of those* $h \in H$ *for which all* $r(h)$ *are* 1; C *is the kernel of the natural projection of* Γ *on* G; Γ/C *is isomorphic to* G.

Thus Γ acts naturally on G-modules, in particular on $\mathfrak{g}$. Let $\Gamma(K)$, $G(K)$, etc. denote the dependence of Γ, G etc. on K.

3.7. *Let* K *be algebraically closed and of infinite degree of transcendence over the prime field. Then* G *and* Γ *may be identified, via isomorphisms, with a simple algebraic group and its simply connected covering group, and both may be defined over the prime field. It is then true that* (a) *the* pth *power automorphism of* Γ *is given by* $x_r(t) \to x_r(t^p)$, (b) *if* k *is a subfield of* K, Γ_k *is naturally isomorphic to* $\Gamma(k)$, *and* (c) H *is a Cartan subgroup of* Γ.

These results, which cover all simple algebraic groups because of the classification in [13], are proved at the end of § 4.

We use ω_a ($a \in S$) to denote the function (fundamental weight) on H defined by $\prod h_b(t_b) \to t_a$, and set $\omega = \prod \omega_a$.

3.8. $$\omega^2 = \prod_{r>0} r.$$

For a proof of the additive version of this result see [14, p. 19-01].

Finally to close this section we prove a result of fundamental importance in our later discussion of the representations of finite groups. We are indebted to T. A. Springer for the main ideas of the proof.

3.9 Lemma. *Assume that* K *is algebraically closed and of infinite transcendence degree over its prime field* F_p, *that* τ *is a rational automorphism of* Γ *such that* $H^\tau = H$, *that* σ *is the composition of* τ *with the* pth *power automorphism, and that* Γ_σ *is the subgroup of fixed points of* σ. *Then* (a) *the semisimple classes of conjugate elements of* Γ_σ *are in natural one-one correspondence with those orbits of* H *under* W, *the Weyl group, that are invariant under* σ, *and* (b) *if for each* $a \in S$, γ_a *is the sum of the distinct images of* ω_a *under* W, *the orbit space* H/W *is an affine variety with coordinates* γ_a ($a \in S$).

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

The proof proceeds in several steps.

(1) *Assume that B is a (connected) algebraic subgroup of Γ and that $B^\sigma = B$. Then for each x in B there is a y in B such that $x = y^{-1}y^\sigma$.* This result is quite close to one of Lang [9], and it does not depend on the simple-connectedness or semisimplicity of Γ. The proof, a straightforward modification of Lang's, is omitted.

(2) *The centralizer of a semisimple element of a simply-connected semisimple algebraic group is connected.* Here are the main steps in a proof due to Springer (unpublished). The semisimple element h is put in a Cartan subgroup H, and then by the Bruhat decomposition [13, p. 13-11], the problem is reduced to showing that an element of the Weyl group that leaves h fixed is a product of reflections (corresponding to roots) that also do. After the problem is shifted from H to an ordinary torus T and then to the covering space of T, the proof is completed by geometric means.

(3) *Two semisimple elements of Γ_σ which are conjugate in Γ are also conjugate in Γ_σ.* Assume $x = zwz^{-1}$ ($x, w \in \Gamma_\sigma$, $z \in \Gamma$). Then $x = z^\sigma wz^{-\sigma}$, whence $z^{-1}z^\sigma$ is in B, the centralizer of w. By 3.7 and (2), B is connected if w is semisimple, and because $w \in \Gamma_\sigma$, $B^\sigma = B$. Thus by (1) we can write $z^{-1}z^\sigma = y^{-1}y^\sigma$ ($y \in B$). Then $zy^{-1} \in \Gamma_\sigma$, and since $x = (zy^{-1})w(zy^{-1})^{-1}$, we have (3).

(4) *An element of Γ is conjugate to an element of Γ_σ if and only if it is conjugate to its image under σ.* For if $z \in \Gamma$, then $z = xz^\sigma x^{-1}$ for some $x \in \Gamma$ if and only if $z = y^{-1}y^\sigma z^\sigma y^{-\sigma}y$ for some $y \in \Gamma$, by (1) with $B = \Gamma$, that is, if and only if $yzy^{-1} \in \Gamma_\sigma$ for some $y \in \Gamma$.

(5) *Two elements of H are conjugate in Γ if and only if they are conjugate under W.* This easily comes from the uniqueness in the Bruhat decomposition.

Since an element of Γ is semisimple if and only if it is conjugate to an element of H [13, p. 6-13], we may combine (3), (4) and (5) to get (a). In [15, p. 57-8] it is proved that H/W is an affine algebraic variety whose coordinate ring is got from that of H by selecting the invariants under W. This means the polynomials in ω_a, ω_a^{-1} ($a \in S$) that are symmetric relative to W. Thus to complete the proof of (b) we need only establish the following result, which in case W is of type A_l reduces to the fundamental theorem for sym-

metric functions.

(6) *Every polynomial in* ω_a, ω_a^{-1} $(a \in S)$ *that is symmetric relative to* W *is a polynomial in the elementary symmetric polynomials* γ_a $(a \in S)$. Partially order the monomials $\prod \omega_a^{n_a}$ so that each is higher than those obtained by multiplying it by a product of negative (multiplicative) roots. Thus if β is a nonzero symmetric polynomial and $c\prod \omega_a^{n_a}$ is one of its highest terms, each $n_a \geq 0$ because β is symmetric. Then $\beta - c\prod \gamma_a^{n_a}$ does not contain this term, and the proof of (6) may be completed by induction.

§ 4. Lifting representations from algebras to groups

The notations $\mathfrak{p}$, K, $\sum$, S, H, ω_a, etc. introduced in §§ 2 and 3 in connection with the algebra $\mathfrak{g}$ and corresponding groups G and Γ will be used throughout the paper. By a module (or representation) for these groups we mean one over $\overline{K}$, the algebraic closure of K. Following Curtis [4], we first convert each $M \in \mathfrak{M}$ into a projective Γ-module. For $x \in \Gamma$, let M^x be the irreducible $\mathfrak{g}$-module obtained by defining the action of $\mathfrak{g}$ on M by the rule:

4.1 $$(M^x) \quad X.v = X^x v \qquad (X \in \mathfrak{g},\ v \in M).$$

Here X^x is the image of X under x and we use the convention $(X^x)^y = X^{yx}$. The module M^x is equivalent to M [4]. Thus there is a $\mathfrak{g}$-module isomorphism $T(x)$, uniquely determined to within a scalar multiple by Schur's lemma, of M on M^x. This satisfies:

4.2 $$T(x)Xv = X^x T(x)v \qquad (x \in \Gamma,\ X \in \mathfrak{g},\ v \in M).$$

The map $x \to T(x)$ is a projective representation of Γ (or G) on M, again by Schur's lemma. For each positive root r we may (and do) normalize all $T(x_r(t))$ to keep v_+ fixed (see 2.7); since 4.1 and 4.2 imply that $T(x_r(t))v = v + \textit{higher terms}$, for each monomial v, this amounts to making each $T(x_r(t))$ unipotent. After treating negative roots in a similar way, we want to show that the normalization can be extended to yield an ordinary (not just a projective) representation of Γ. When it is convenient, we write xv for $T(x)v$.

4.3 Lemma. *Let* $M \in \mathfrak{M}$ *have high weight* $\lambda(a)$ $(a \in S)$, *fix* $a \in S$ *and set* $\lambda(a) = n$. *Then* (a) $v_+, X_{-a}v_+, \ldots, X_{-a}^n v_+$ *are linearly independent and* $X_{-a}^{n+1} v_+ = 0$; (b) *the normalized action of the* $x_a(t)$ *and* $x_{-a}(t)$ *on* M *can be*

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

extended to an ordinary representation of Z_a, the group generated by these elements; we then have (c) $h_a(t)v_+ = t^n v_+$.

Proof. By induction, $X_a X_{-a}^i v_+ = i(n-i+1)X_{-a}^{i-1}v_+$ $(i \geq 1)$, whence the vectors $X_{-a}^i v_+$ $(0 \leq i \leq n)$ are nonzero and then linearly independent by 2.9. Further $X_a X_{-a}^{n+1} v_+ = 0$, and clearly $X_r X_{-a}^{n+1} v_+ = 0$ for $r > 0$, $r \neq a$. Thus $X_{-a}^{n+1} v_+ = 0$ by 2.7 and 2.9. Now set $v_0 = v_+$, $iv_i = X_{-a} v_{i-1}$ $(1 \leq i \leq n)$, so that also $(n-i)v_i = X_a v_{i+1}$. From $x_a(t)v_+ = v_+$, $x_a(t)X_{-a} = X_{-a} + tH_a - t^2 X_a$ and 4.2, we see by induction that $x_a(t)v_i = \sum_{j=0}^{i} \binom{n-j}{n-i} t^{i-j} v_j$. Now interchanging the roles of X_a and X_{-a}, and also of v_0 and v_n, that is, replacing M by M^w with w an element of Z_a corresponding to the Weyl reflection relative to a, we get $x_{-a}(t)v_i = \sum_{j=i}^{n} \binom{j}{i} t^{j-i} v_j$. Introducing a space with coordinates x and y and setting $v_i' = x^{n-i} y^i$, we see that in the space of polynomials of degree n exactly the same equations hold for the transformations $x_a'(t)$: $x, y \to x, y + tx$ and $x_{-a}'(t)$: $x, y \to x + ty, y$. We thus see that the relations on the $x_a(t)$ and $x_{-a}(t)$ $(a \in S)$ implied by 3.2 also hold for the $T(x_a(t))$ and $T(x_{-a}(t))$. Further the relations 3.1 with $r, s > 0$ are also preserved, as we see by applying both sides to v_+ and noting that every term leaves v_+ fixed. Since we may choose an element w in Γ corresponding to an arbitrary element of the Weyl group and apply the above considerations to M^w, we see that all of the relations of 3.1 and 3.2 are preserved. We thus get 4.3(b), 4.3(c) and also:

4.4. *The projective representation of Γ on M can be lifted in a unique way to an ordinary representation.*

The uniqueness comes from 3.4, which implies that Γ has no nontrivial one-dimensional representation.

From the definitions we see that if v has height n in M then

4.5 $\qquad (x_r(t) - 1)v = tX_r v + \textit{higher (lower) terms, when } r > 0 \ (r < 0).$

By 2.7 this yields:

4.6. *The vectors $\bar{K}v_+$ are the only ones fixed by all $x_r(t)$ $(r > 0)$.*

From this and 4.3, we see that the Γ-module M determines $\bar{K}v_+$, which in turn determines $\lambda(a)$ $(a \in S)$ since $\lambda(a) + 1$ is the dimension of the subspace generated by the elements $x_{-a}(t)$ $(t \in K)$ acting on $\bar{K}v_+$. Thus using also 4.3(c),

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

4.7. *If M_1 and M_2 in $\mathfrak{M}$ are distinct as $\mathfrak{g}$-modules, they are distinct as Γ-modules. If M_1 has high weight λ as $\mathfrak{g}$-module, it has high weight $\prod\omega_a^{\lambda(a)}$ as Γ-module.*

In order to pass to projective G-modules, we use:

4.8. *Under the natural projection from Γ to G, each irreducible Γ-module leads to an irreducible projective G-module. Distinct Γ-modules yield distinct G-modules.*

We need only observe that the center C of Γ must act via scalars in any irreducible representation of Γ, and then use 3.4.

Now Γ acts faithfully on $\mathfrak{M}$ as a set: since Γ/C is simple, the kernel is contained in C and consists of those h for which all $\omega_a(h)$ $(a\in S)$ are 1. Further, relative to monomial bases, the group $\{x_r(t),\ t\in K\}$ acts via matrices that are polynomials in t with coefficients in F_p, thus acts as an algebraic group defined over F_p with the pth power map given by $x_r(t)\to x_r(t^p)$. The same is thus true of the group Γ. Comparing the structure just put on Γ with the one put on G by T. Ono [J. Math. Soc. Japan 10 (1958)], and using his results and methods and those of [13, Exp. 23], we easily get the assertions of 3.7 and also

4.9. *Γ (hence also G) acts rationally on each M in $\mathfrak{M}$.*

§ 5. Tensor product theorem

Each isomorphism α of K into $\overline{K}$ gives rise to an isomorphism of $\Gamma(K)$ into $\Gamma(\overline{K})$, defined by $x_r(t)\to x_r(t^\alpha)$, and can thus be used to convert each Γ-module $M\in\mathfrak{M}$ into another Γ-module, denoted M^α, by the rule $x\cdot v=x^\alpha v$ $(x\in\Gamma(K),\ v\in M)$.

5.1 THEOREM. (a) *If $M_1, M_2, \ldots, M_k$ are in $\mathfrak{M}$ and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are distinct isomorphisms of K into $\overline{K}$, then $M=M_1^{\alpha_1}M_2^{\alpha_2}\cdots M_k^{\alpha_k}$ (tensor product) is an irreducible Γ-module.* (b) *For a fixed sequence of α's, two Γ-modules M constructed in this way are equivalent if and only if the sequences of M_i's are the same. Or, equivalently, if $N=N_1^{\beta_1}N_2^{\beta_2}\cdots N_l^{\beta_l}$ with the N_j in $\mathfrak{M}$ and the β_j distinct isomorphisms of K into $\overline{K}$, then M is equivalent to N if and only if, after the deletion of all one-dimensional factors, $k=l$ and, for some permutation π of $1, 2, \ldots, k$, M_i is equivalent to $N_{\pi i}$ and $\alpha_i=\beta_{\pi i}$ for $i=1, 2, \ldots, k$.*

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

(c) *If the modules in* (a) *and* (b) *are taken to be projective G-modules, the modified statements are also true.*

Proof. Let $X_r^{(i)}$ be the transformation that is X_r on $M_i^{a_i}$ and the identity on the other components of M, let $v_+ = \prod v_+^{(i)}$ be the product of the high vectors in the separate components, and let the height of a product of monomials be defined as the sum of the heights of its terms.

(1) *The set of vectors of M annihilated by all $X_r^{(i)}$ ($r>0$, $i=1, 2, \ldots, k$) is $\overline{K}v_+$. Nonzero vectors of distinct heights are linearly independent.* For $k=1$, this follows from 2.7 and 2.9. If $k>1$, we can write any v in M as $v=\sum u_j w_j$ ($u_j \in M_1^{a_1}\cdots M_{k-1}^{a_{k-1}}$, $w_j \in M_k^{a_k}$) with the u_j and also the w_j linearly independent. Then $X_r^{(k)}v = \sum u_j(X_r w_j)$, which is 0 only if all $X_r w_j$ are 0, because the u_j are linearly independent. Thus $X_r^{(k)}v=0$ for all $r>0$ only if all w_j are in $\overline{K}v_+^{(k)}$, whence the first part of (1) follows by induction. This implies the second part (see the proof of 2.9) and also:

(2) *If v is a homogeneous vector of M and $r>0$ (resp. $r<0$), then $(x_r(t)-1)v = \sum t^{\alpha_i} X_r^{(i)} v +$ higher (resp. lower) terms.*

(3) *Irreducibility.* Let M' be a Γ-submodule of M and v a nonzero vector of M'. Write $v=v_0+v_1+\cdots+v_d$, $v_d \neq 0$, height $v_j=-j$. The α_i are distinct, thus linearly independent. By (2) this implies that for every $r>0$ and every $i=1, 2, \ldots, k$ there is a vector $X_r^{(i)}v_d +$ *higher terms* in M', whence by (1) and induction on d the vector v_+ is also in M'. Then using negative roots, we see by (downward) induction on the height that for every monomial v of M there is a vector $v +$ *lower terms* in M'. By induction on the height this implies that M' contains all monomials, that $M'=M$, that M is irreducible.

(4) *Uniqueness.* Let λ_i be the high weight of M_i as $\mathfrak{g}$-module. We must show that M as Γ-module intrinsically determines the numbers $\lambda_i(a)$ ($i=1, 2, \ldots, k$; $a \in S$). First note that M determines $\overline{K}v_+$ by (1). Fix a and set $\lambda_i(a)=a_i$. If all $x_{-a}(t)$ ($t \in K$) fix v_+, then the a_i are certainly determined by M—they must all be 0 by 4.3(a) and 4.5. Assume henceforth that this is not the case. Then $h_a(t)$ acts on $\overline{K}v_+$ with the characteristic value t^α, $\alpha=\sum a_i\alpha_i$, some $a_i \neq 0$, by 4.3(c). Assuming that M does not determine the a_i uniquely, we are thus led to the existence of a nontrivial identical relation $t^\alpha = t^\beta$ ($\beta = \sum b_i\alpha_i$, some $b_i \neq 0$, some $b_j \neq a_j$, $t \in K$). Among all such relations on the

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

monomials t^γ ($\gamma = \sum c_i \alpha_i$, $0 \leq c_i \leq p-1$), ordered lexicographically, we choose one of minimum degree. The substitution $t \to tu$ shows that this relation has the form $t^\delta = t^\varepsilon$ ($\delta > \varepsilon$, $\delta = \sum d_i \alpha_i$, $\varepsilon = \sum e_i \alpha_i$). Then using the minimality of the degree and the substitution $t \to t+u$, we get in turn $d_k = 0$ (whence we may assume $e_k \neq 0$ since otherwise the proof is completed by induction), $k > 1$, $\delta = \alpha_1$, $\varepsilon = \alpha_k$, and $\alpha_1 = \alpha_k$, a contradiction. This proves the first statement of (b). The second follows immediately.

(5) *G-modules.* By 4.8 the results we have proved for Γ-modules are equally valid for G-modules, which is (c).

We remark that considering $\mathfrak{g}$ as Lie ring rather than Lie algebra we can interpret $M_i^{a_i}$ above as $\mathfrak{g}$-module and then prove a theorem entirely analogous to 5.1 with $\mathfrak{g}$ in place of Γ.

§ 6. Rational representations

As a first application of 5.1 we have:

6.1 THEOREM. *If K is infinite and perfect and α_i denotes the automorphism $t \to t^{p^i}$ of K, then every irreducible rational Γ-module or irreducible rational projective G-module can be expressed uniquely as a tensor product $M = \prod_{i=0}^{\infty} M_i^{a_i}$ ($M_i \in \mathfrak{M}$, almost all M_i trivial).*

Proof. By 4.8 we need only consider Γ-modules, and by the density theorem of Rosenlicht [12, p. 44] we may assume that K is algebraically closed and of infinite transcendence degree over its prime field. For given, but arbitrary, nonnegative integers $\lambda(a)$ ($a \in S$), we can uniquely write $\lambda(a) = \sum p^i \lambda_i(a)$ ($0 \leq \lambda_i(a) \leq p-1$), choose M_i in $\mathfrak{M}$ as the Γ-module with high weight $\prod \omega_a^{\lambda_i(a)}$ (see 4.7), and thus construct a Γ-module $\prod M_i^{a_i}$ which is rational by 4.9, irreducible by 5.1, and has high weight $\prod \omega_a^{\lambda(a)}$. Using the classification [13, Exp. 14 and 15] of irreducible representations of semisimple algebraic groups in terms of high weights, we see that this construction yields a complete set of irreducible rational Γ-modules, whence 6.1.

By now we have also shown that if K is infinite and perfect every irreducible rational projective representation of Γ or G comes in a unique way from an ordinary representation of Γ.

§ 7. Finite groups, normal forms

If K is finite with q elements, we write Γ_q, G_q for Γ, G. The following fact, not used here, is proved in [21].

7.1. *If the rank is at least* 2, *the relations* 3.1 *alone are enough to define* Γ_q.

What is required here from [21] is:

7.2. *Every irreducible projective* G_q*-module can be lifted uniquely to a* Γ_q*-module.*

Now by 3.9 with σ the qth power mapping, the semisimple classes of conjugate elements of Γ_q are characterized by coordinates $\gamma(a)$ subject to the condition $\gamma(a)^q = \gamma(a)$ (see also 3.7(a)). This yields:

7.3 Lemma. *If the rank is* l, *the number of semisimple classes of conjugate elements of* Γ_q *is* q^l.

We can now prove one of the main results of this paper. Observe that the modules considered are not assumed to be rational, throughout this section.

7.4 Theorem. *Let* $q = p^n$ *and let* α_i *denote the field automorphism* $t \to t^{p^i}$. *Then every irreducible* Γ_q*-module, also every irreducible projective* G_q*-module, can be expressed uniquely as a tensor product* $M = \prod_{i=0}^{\mu-1} M_i^{\alpha_i}$ $(M_i \in \mathfrak{M})$. *If the rank of* Γ_q *is* l, *there are* q^l *such modules.*

Proof. Again we need only consider Γ_q-modules, this time by 7.2. By 7.3 and a theorem of Brauer and Nesbitt [1, p. 14] the number of inequivalent irreducible Γ_q-modules is q^l. Since the q^l modules $\prod M_i^{\alpha_i}$ are inequivalent and irreducible by 5.1, they thus form a complete set, as required.

7.5 Corollary. *If* L *is an infinite field containing the finite field* K, *every irreducible representation of* $\Gamma(K)$ *can be extended to* $\Gamma(L)$. *Every irreducible representation of* $\Gamma(K)$ *can be realized over* K. *The corresponding statements for projective representations of* G *are also true.*

The first statement is clear. For the second we need only observe that relative to a monomial basis 2.8 for $M_i \in \mathfrak{M}$ each generator $x_r(t)$ is represented by a matrix which is a polynomial in t with coefficients in the prime field.

The modules of 7.4 have high weights $\prod \omega_a^{\lambda(a)}$ with $0 \leq \lambda(a) \leq q-1$. Those in which the center C of Γ (see 3.6) acts trivially, or what is equivalent, fixes

v_+, yield all of the irreducible G_q-modules. Thus

7.6 COROLLARY. *Every irreducible G_q-module is obtained from a Γ_q-module for which the high weight $\prod\omega_a^{\lambda(a)}$ is* 1 *on the center of Γ.*

In individual cases, when the root system $\sum$ is specfied, more detailed results can be given. Thus if $\sum$ is of type E_8, F_4 or G_2 (and K is arbitrary), $\Gamma = G$, so that 7.6 is superfluous, while, for example, if $\sum$ is of type A_l (so that Γ_q and G_q are respectively isomorphic to $SL(l+1, q)$ and $PSL(l+1, q)$), the irreducible G_q-modules correspond to the sequences $(\lambda_1, \lambda, \ldots, \lambda_l)$ for which $0 \leq \lambda_i \leq q-1$ and $\sum i\lambda_i$ is divisible by the greates common divisor of $l+1$ and $q-1$.

Dually, one can make similar statements concerning the classes of conjugate elements of G in terms of those of Γ.

Finally, we remark that there are results analogous to 7.4 and 7.5 with the finite Lie ring $\mathfrak{g}_q$ in place of Γ_q. The proof of completenteness of the modified 7.4 can be given along the lines of [14; p. 22-11, 22-12].

§ 8. Prime power representations

A general formula in characteristic p, comparable to Weyl's formula in characteristic 0 (cf. [6]), for the characters or dimensions of the above modules does not yet exist (except for groups of type A_1 and A_2 [13, p. 588], [14]). However, for the irreducible Γ_q-module with the greatest of all possible high weights, ω^{q-1} (recall that $\omega = \prod\omega_a$), that is, the module $M_q = \prod M_i^{q_i}$ of 7.4 in which each M_i is equivalent to the module M_p of $\mathfrak{M}$ with high weight $\lambda(a) = p-1$ ($a \in S$) as $\mathfrak{g}$-module, the situation can be described rather completely and is very much as in characteristic 0. The following result is proved in [17].

8.1 LEMMA. *If m is the number of positive roots in $\sum$, there is an irreducible Γ_q-module $\overline{M}_q$ of dimension q^m, that is, the order of a p-Sylow subgroup of Γ_q.*

8.2 THEOREM. *The Γ_q-modules $\overline{M}_q$ of* 8.1 *and M_q of high weight ω^{q-1} are eqnivalent. All other irreducible Γ_q-modules have smaller dimensions than M_q.*

Proof. Because each module of $\mathfrak{M}$ is spanned by the monomials 2.8, the only one that could have a dimension as large as p^m is M_p by 4.3(a), and hence by 7.4 the only possible irreducible Γ-module of dimension as large as

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

q^m is M_q. From the existence of the module $\overline{M}_q$ with dimension q^m, it follows that M_q is equivalent to $\overline{M}_q$ and that the other irreducible Γ_q-modules have smaller dimensions.

In the course of the argument, we have proved:

8.3 COROLLARY. *The irreducible module M_p with high weight ω^{p-1} has dimension p^m and a basis consisting of all the monomials* 2.8.

A direct proof of this result, within the framework of $\mathfrak{g}$-modules, also exists. Using 8.3 we can compute the (Brauer) character of M_q. To define this we write the order g of Γ_q as $g=p^e g'$, $(p, g')=1$, choose an isomorphism θ of the group of g'th roots of 1 in $\overline{K}$ onto the corresponding group in the complex field, and then for any semisimple element x of Γ_q and any module M for Γ_q, define $\chi(x)$, the character of x on M, to be $\sum\theta(c_i)$, the sum to be taken over the characteristic roots c_i of x on M. Generally χ depends on the choice of θ, but not on M_q where it turns out to be rational.

The following result has been proved previously only for groups of type A_l [16, p. 281] and in somewhat different terms.

8.4 THEOREM. *If Γ_q is of rank l, and x is a semisimple element whose centralizer in the correpsonding algebraic group has dimension $l+2d(x)$, or equivalently, whose action on $\mathfrak{g}$ has fixed point set of dimension $l+2d(x)$, the character of x on M_q is given by $\chi(x)=\pm q^{d(x)}$.*

Proof. In $\Gamma(\overline{K})$, x is conjugate to an h in $H(\overline{K})$. Now since h acts on the monomial 2.8 of M_p by multiplication by $\omega^{p-1}(h)\prod r_k(h)^{-i_k}$, we see by 8.3 that the character of h on M_p is

$$\psi(h)=\theta(\omega^{p-1}(h))\prod_{r>0}\sum_{i=0}^{p-1}\theta(r(h)^{-i}), \tag{8.5}$$

and then using 3.8, that the character $\chi(h)$ on M_q satisfies $\chi(h)^2=\prod_r\sum_{i=0}^{q-1}\theta(r(h)^{(q-1-2i)/2})$, the product over all roots. Since h is conjugate to an element of Γ_q and the roots are permuted by the Weyl group, it follows from (4) and (5) of the proof of 3.9 that the numbers $\theta(r(h))^q$ form a permutation of the numbers $\theta(r(h))$. Thus the roots can be arranged in cycles (of various lengths) $(r_1 r_2 \cdots r_k)$ such that $\theta(r_i(h))^q=\theta(r_{i+1}(h))$, $\theta(r_k(h))^q=\theta(r_1(h))$. If $r(h)\neq 1$, the cycle containing r telescopically contributes 1 to the product for $\chi(h)^2$, since the term for r may be written, subject to a consistent choice of square roots,

as $(c^{q/2}-c^{-q/2})/(c^{1/2}-c^{-1/2})$ with $c=\theta(r(h))$. The terms for which $r(h)=1$ contribute q each to the product, $q^{2d(h)}$ together. Thus $\chi(h)^2=q^{2d(h)}$. Since h is conjugate to x, we have 8.4.

8.6 COROLLARY. *If Γ_q is replaced by G_q, 8.2 and 8.4 remain valid.*

We need only remark that M_p, hence M_q, is an ordinary (not just projective) G_q-module: if c is in the center of Γ, $\omega^2(c)=\prod r(c)=1$ by 3.6 and 3.8, whence $\omega^{p-1}(c)=1$, even if p is 2.

Finally we remark that for semisimple algebraic groups over an algebraically closed field of characteristic 0, results analogous to 8.3 to 8.6, in which p need not be a prime nor q a prime power are true. Here we content ourselves with showing that the formula 8.5 for the character on the irreducible module with high weight ω^{p-1} is essentially unchanged. With $\Delta(j)=\sum(\det w)(w\omega)^j$, the sum over the Weyl group, Weyl's formula for the character [26, p. 389] yields $\Delta(p)/\Delta(1)$, that is, 8.5 with $\theta=1$ because of the basic factorization $\Delta(j)=\omega^j\prod_{r>0}(1-r^{-j})$ [26, p. 386].

§ 9. Finite groups, nonnormal forms

In this section we treat the simple groups denoted as A_l^1 (a projective unitary group in $l+1$ dimensions), D_l^1 (a second projective orthogonal group in $2l$ dimensions), E_6^1 (a nonnormal "real" form of E_6) and D_4^2 (a "triality" form of D_4) in [19], and their covering groups. Each of the latter groups can be defined in terms of generators and relations derived from the structure of the corresponding simple group, just as Γ is in terms of G in § 3; however, it is more convenient to define them directly as subgroups of the groups Γ. Starting with an automorphism σ, other than the identity, of the root system $\sum$ such that $\sigma S=S$, and an automorphism σ of the same period on the field K, we can construct an automorphism, also called σ, of the corresponding group Γ such that $x_a(t)^\sigma=x_{\sigma a}(t^\sigma)$ for all $a\in\pm S$ and all $t\in K$, and then define Γ^1 to be the group of fixed points of σ. Comparing this definition with the one given in [19] for the corresponding simple groups, and using 3.6, we easily get:

9.1. *Let C^1 be the center of Γ^1. Then $C^1=C\cap\Gamma^1$, and Γ^1/C^1 is naturally isomorphic to the corresponding simple group of* [19].

We write G^1 for Γ^1/C^1, K_0 for the fixed field under σ, and Γ_q^1, etc. when K_0

has q elements. As a subgroup of Γ, Γ^1 acts naturally on each Γ-module.

9.2 THEOREM. *If the M_i are in $\mathfrak{M}$, and the α_i are isomorphisms of K into $\overline{K}$ which are distinct on K_0, then $M = M_1^{\alpha_1} M_2^{\alpha_2} \cdots M_k^{\alpha_k}$ is an irreducible Γ^1-module, and there is uniqueness in this product representation in the sense of the second sentence of* 5.1(b).

Proof. We use the notations of the proof of 5.1 and assume that σ above has period 2. If the period is 3, as it is for one of the groups of type D_4, the argument is similar. If r is a root such that $\sigma r = r$ and there is no root s such that $r = s + \sigma s$, then we may assume $x_r(t) \in \Gamma^1$ for all $t \in K_0$ [19, *p.* 879], and we have 5.1(2) holding. If r is such that $\sigma r \neq r$ and $r + \sigma r$ is not a root, then (see [19]) $x_r(t)x_{\sigma r}(t^\sigma) \in \Gamma^1$ for all t in K, and we have instead $(x_r(t)x_{\sigma r}(t^\sigma) - 1)v = \sum t^{\alpha_i} X_r^{(i)} v + \sum t^{\sigma\alpha_i} X_{\sigma r}^{(i)} v + \cdots$. If r, σr and $r + \sigma r$ are all roots, the situation is similar. Since the α_i act distinctly on K_0 and the α_i and $\sigma\alpha_i$ together act distinctly on K, the proofs of irreducibility and uniqueness in 9.2 are from this point on straightforward modifications of those in 5.1.

For finite groups, we have:

9.3 THEOREM. *If K_0 has $q = p^n$ elements and α_i denotes the field automorphism $t \to t^{p^i}$, then every irreducible Γ_q^1-module can be written uniquely as a tensor product $M = \prod_{i=0}^{n-1} M_i^{\alpha_i}$ ($M_i \in \mathfrak{M}$). If the rank is l, the number of such modules is q^l.*

Thus every irreducible Γ_q^1-module is the restriction of some $\Gamma(\overline{K})$-module, and the largest high weight that occurs is ω^{q-1}. Again, by 9.2, we are reduced to showing that the number of semisimple classes of conjugate elements is q^l. By 3.9, these are characterized by coordinates $\gamma(a)$ ($a \in S$) subject to the condition $\gamma(a)^q = \gamma(\sigma a)$. Whatever permutation σ effects on S, the number of solutions is q^l (the contribution for each cycle of length d is q^d), as required.

Turning again to [21], we have:

9.4. *If the type A_l (l even) is excluded, every irreducible projective G_q^1-module can be lifted uniquely to a Γ_q^1-module.*

Quite likely this exclusion is unnecessary, but we have not yet shown this. From 9.3 and 9.4 we get:

9.5 COROLLARY. *If the type A_l (l even) is excluded,* 9.3 *also holds for*

projective G_q^1-modules.

Here also one can get the irreducible G_q^1-modules as those of Γ_q^1 in which the center acts trivially. Since 8.1 is true with Γ_q^1 in place of Γ_q [17, 19], the same is true of 8.2. Also if h in $H(\overline{K})$ is conjugate to an element of Γ_q^1, then by (4) and (5) of the proof of 3.9, it is conjugate under the Weyl group to h^σ, so that the numbers $r(h)^q$ again form a permutation of the numbers $r(h)$ (see the definition of σ at the beginning of this section). Thus the proof 8.4 carries over as is.

9.6 THEOREM. *The statements* 8.1, 8.2 *and* 8.4 *are true with Γ_q^1 in place of Γ_q.*

§ 10. Special isogenies, infinitesimal and global

In this section we present a discussion of the rather special isogenies that exist for simple groups of type B_l, C_l and F_4 and characteristic 2, and type G_2 and characteristic 3 (cf. [23, p. 282], [13, Exp. 21-24]). The results will be used in the next sections, where we return to group representations.

In what follows we identify two root systems that are related by a scalar multiplication. Associated with each system $\sum$, there is a dual system $\sum^*$ and a map of $\sum$ onto $\sum^*$ such that $r^* = 2r/(r, r)$ $(r \in \sum)$. When roots of unequal lengths occur, this map preserves angles, sends short roots to long roots and vice versa, maps the simple set S onto another, and puts types B_l and C_l in duality with each other and types C_2, F_4 and G_2 with copies of themselves.

The pair $(\sum, p)$ will be called special if $\sum$ contains roots r and s such that $(s, s)/(r, r) = p$. The possibilities are those listed in the first paragraph of this section. In the corresponding algebra $\mathfrak{g}$ of § 2, those X_r and H_r for which r is short span an ideal, denoted $\mathfrak{g}_1$ in what follows. To see this, observe that if r is short and s is long $c_{sr} = pc_{rs}$, and that if r, s and $r+s$ are roots with r short and $r+s$ long then s is short and $p_{rs} = p$ (check for $\sum$ of type C_2 and G_2). Observe also that in the present case $\Gamma = G$, Γ maps $\mathfrak{g}_1$ onto itself (because each $x_r(t)$ does), and, being simple, Γ acts faithfully on each of $\mathfrak{g}_1$ and $\mathfrak{g}/\mathfrak{g}_1$. To indicate the dependence of $\mathfrak{g}$, etc. on $\sum$ we write $\mathfrak{g}(\sum)$, etc.

10.1 (Existence of isogenies). *If $(\sum, p)$ is special, it is possible to normalize*

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

equations 2.6 *for* $\mathfrak{g}(\sum)$ *and* $\mathfrak{g}(\sum^*)$ *so that the following hold.* (a) *There exists a homomorphism* $\bar{\theta}$ *of* $\mathfrak{g}(\sum)$ *into* $\mathfrak{g}(\sum^*)$ *such that* $\bar{\theta}X_r = X_{r^*}$ *if* r *is long,* $\bar{\theta}X_r = pX_{r^*} = 0$ *if* r *is short, and similar equations hold for* $\bar{\theta}H_r$. (b) *The kernel of* $\bar{\theta}$ *in* (a) *is* $\mathfrak{g}_1(\sum)$. *Thus* $\bar{\theta}$ *induces an isomorphism, also dented* $\bar{\theta}$, *of* $(\mathfrak{g}/\mathfrak{g}_1)(\sum)$ *onto* $\mathfrak{g}_1(\sum^*)$. (c) *If* $\Gamma(\sum)$ *acts on* $(\mathfrak{g}/\mathfrak{g}_1)(\sum)$ *and* $\Gamma(\sum^*)$ *on* $\mathfrak{g}_1(\sum^*)$, *the map* θ: $x^\theta = \bar{\theta}x\bar{\theta}^{-1}$ $(x \in \Gamma(\sum))$ *is an isomorphism of* $\Gamma(\sum)$ *into* $\Gamma(\sum^*)$ *such that* $x_r(t)^\theta = x_{r^*}(t)$ *if* r *is long,* $x_r(t)^\theta = x_{r^*}(t^p)$ *if* r *is short, and similar equations hold for* $h_r(t)^\theta$.

The proof that we have in mind for $(\sum, p)$ of type $(G_2, 3)$ involves many details and will not be given here. When $p = 2$, however, the situation is quite simple since $-1 \equiv 1 \pmod 2$, and no normalization is required.

Proof of 10.1 *for* $p = 2$. To show that the equations of (a) define a homomorphism, we must verify that the relations 2.1 to 2.6 are preserved. For this the relations 2.2 and 2.6 will suffice since they together with the relations $[H_r, X_r] = 2X_r = 0$ and $[X_r, X_{-r}] = H_r$, which are clearly preserved, imply all of the others (cf. [21]). We give details only for 2.6. Now if either r or s is short, then 2.6 is preserved (both sides go to 0) because $g_1(\sum)$ is an ideal, while if r and s are long and linearly independent, then either $(r, s) < 0$, whence $p_{rs} = 1 = p_{r^*s^*}$, or $(r, s) \geq 0$, whence $p_{rs} = 0$ and $p_{r^*s^*} = 0$ or 2. Since $p = 2$, we have (a), and then (b). For the proof of (c), we fix a long root $s \in \sum$. If r is long, $r \in \sum$, then either $r = -s$ and $x_r(t)^\theta X_{s^*} = \bar{\theta}x_r(t)X_{-r} = \bar{\theta}(X_{-r} + tH_r - t^2X_r) = X_{-r^*} + tH_{r^*} - t^2X_{r^*} = x_{r^*}(t)X_{-r^*} = x_{r^*}(t)X_{s^*}$, or $r \neq -s$ and $x_r(t)^\theta X_{s^*} = \bar{\theta}x_r(t)X_s = \bar{\theta}(X_s + p_{rs}tX_{r+s}) = X_{s^*} + p_{r^*s^*}tX_{r^*+s^*} = x_{r^*}(t)X_{s^*}$; whereas if r is short, $r \in \sum$, then either $r + s \notin \sum$ in which case $r^* + s^* \notin \sum^*$ and $x_r(t)^\theta X_{s^*} = X_{s^*} = x_{r^*}(t^p)X_{s^*}$, or $r + s \in \sum$ in which case $2r + s \in \sum$, $(2r + s)^* = r^* + s^*$ and $x_r(t)^\theta X_{s^*} = \bar{\theta}x_r(t)X_s = \bar{\theta}(X_s + tX_{r+s} + t^2X_{2r+s}) = X_{s^*} + t^2X_{r^*+s^*} = x_{r^*}(t^2)X_{s^*}$. Since the X_{s^*} (s long) generate $\mathfrak{g}_1(\sum^*)$, we have (c).

10.2 Corollary (well known). *Over a perfect field of characteristic* 2 *the groups* Γ *of type* B_l *and* C_l *are isomorphic.*

§ 11. Special algebraic groups

In case $(\sum, p)$ is special our previous results on representations can be refind. In $\mathfrak{M}$ let $\mathfrak{M}'$ ($\mathfrak{M}''$) be the subset each of whose elements has, as

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

$\mathfrak{g}$-module, high weight λ vanishing on all long (short) roots of S.

11.1 THEOREM. *Assume that* $(\sum, p)$ *is special and regard the elements of* $\mathfrak{M}$ *either as* $\mathfrak{g}$*-modules or as* Γ*-modules. If* $M' \in \mathfrak{M}'$ *and* $M'' \in \mathfrak{M}''$, *then* $M'M'' \in \mathfrak{M}$, *and conversely every element of* $\mathfrak{M}$ *can be expressed, uniquely, as such a product.*

Proof. Assume $M' \in \mathfrak{M}'$ and $M'' \in \mathfrak{M}''$.

(1) M' *restricted to* $\mathfrak{g}_1$ *is irreducible.* If M_0 is the space spanned by those monomials 2.8 for which all r_i are short, we show first that $M_0 = M'$. Let r be a long positive root. Then $X_r M_0 \subseteq M_0$ because $\mathfrak{g}_1$ is an ideal and $X_r v_+ = 0$. We use induction on the height of r to show that $X_{-r} M_0 \subseteq M_0$. This is so if r is simple since then $X_{-r} v_+ = 0$ because $\lambda(r) = 0$. If r is not simple, there is a simple root a such that $(r, a) < 0$. If a is long, we may write $X_{-r} = \pm [X_{-a}, X_{-(r-a)}]$ and use induction. If a is short, and w denotes the corresponding Weyl reflection and also a corresponding element of Γ, we may apply the induction hypothesis to the module M'^w (see 4.1) with high vector $X_{-a}^{\lambda(a)} v_+$ (see 4.3(a)) and with M_0^w defined accordingly to get $X_{-wr} \cdot M_0^w \subseteq M_0^w$, that is, $X_{-r} M_0^w \subseteq M_0^w$. By 4.3(a) we have $M_0^w = M_0$. Thus $X_{-r} M_0 \subseteq M_0$, M_0 is a $\mathfrak{g}$-submodule of M', and since M' is irreducible, $M_0 = M'$. Next if $v = v_0 + v_1 + \cdots + v_d$ with v_i of height $-i$ and $v_d \neq 0$, we prove by induction on d that the $\mathfrak{g}_1$-module generated by v contains v_+. If $d > 0$, $X_r v \neq 0$ for some $r > 0$ by 2.7. By the induction hypothesis, $X_{r_1} \cdots X_{r_k} X_r v = c v_+$, $c \neq 0$, for a sequence $r_1, r_2, \ldots, r_k$ of short roots. Thus $\sum_{i=1}^{k} X_{r_1} \cdots [X_{r_i}, X_r] \cdots X_{r_k} v + X_r X_{r_1} \cdots X_{r_k} v = c v_+$. If a term in the sum is nonzero we are done, while if the last term on the left is nonzero we may finish by imitating the last part of the proof that $M_0 = M'$ to show that if $r > 0$ and $X_r v' = v_+$ then v_+ is in the $\mathfrak{g}_1$-module generated by v'. By the two parts above, an arbitrary nonzero element of M' generates M' as $\mathfrak{g}_1$-module, which is (1).

(2) M'' *restricted to* $\mathfrak{g}_1$ *is* 0. Let M^* be the $\mathfrak{g}(\sum^*)$-module in $\mathfrak{M}'(\sum^*)$ with high weight λ^* given in terms of the high weight λ of M'' by $\lambda^*(a^*) = \lambda(a)$. We may convert M^* into a $\mathfrak{g}(\sum)$-module by the rule $X.v = (\bar{\theta} X) v$ $(X \in \mathfrak{g}(\sum), v \in M^*)$. As such it is irreducible by (1) and the definition of $\bar{\theta}$, is restricted, and has high weight λ. Thus by 2.7 it is equivalent to M''. From the definition of $\bar{\theta}$, $X_r.v = 0$ if r is short, which is (2).

(3) *Proof of* 11.1 *for* $\mathfrak{g}$*-modules.* Choose a nonzero $u = \sum u_i' u_i''$ with the u_i' linearly independent in M' and the u_i'' in M''. By (1) and (2) we can multiply u by a sequence of X_r (r short, $r>0$) to get a nonzero $v = v_+' v''$, and then v by a sequence of X_r (r long, $r>0$) to get a nonzero multiple of $v_+' v_+''$. Using negative roots instead, first short ones and then long ones, we see that this last vector generates $M'M''$: we first get all $v'v_+''$ (v' monomial in M'), and then using induction on the height of v', all $v'M''$, hence $M'M''$, which is thus irreducible. Since it is also restricted, it is in $\mathfrak{M}$. Since the high weight of $M'M''$ is the sum of those of M' and M'', the uniqueness and completeness in 11.1 follow immediately.

(4) *Proof of* 11.1 *for* Γ*-modules.* As is easily verified, the process 4.2 of lifting the modules of $\mathfrak{M}$ from $\mathfrak{g}$ to Γ is consistent with the two types of tensor products—for algebras and for groups. Thus (4) follows from (3).

11.2 Corollary. *If* $(\sum, p)$ *is special, the map* $\bar{\theta}$ *(resp.* θ*) puts the algebra modules (resp. group modules) of* $\mathfrak{M}''(\sum)$ *in one-one correspondence with those of* $\mathfrak{M}'(\sum^*)$.

In case $(\sum, p)$ is special, 11.1 and 11.2 lead to corresponding refinements of 5.1, 6.1 and 7.4 with $\mathfrak{M}$ replaced by $\mathfrak{M}'$ and $\mathfrak{M}''$. However, there does not seem to be a refinement of the semisimple classes of elements in 7.3. Passing on to 8.2, 8.3 and 8.4, we have:

11.3 Corollary. *Assume that* $(\sum, p)$ *is special. Let* ω' $(\omega'') = \prod \omega_a$, *the product over the short (long) simple roots, let* l' (l'') *be the number of short (long) simple roots, and let* m' (m'') *be the uumber of short (long) positive roots. Then* (a) *the* Γ_q*-module* M_q' (M_q'') *with high weight* ω'^{q-1} (ω''^{q-1}) *has dimension* $q^{m'}$ $(q^{m''})$ *and character at a semisimple element* h *given by* $\chi(h) = \pm q^{d(x)}$ *with* $2d(x) + l'$ (l'') *the dimension of the set of fixed points of* x *on* $\mathfrak{g}_1$ $(\mathfrak{g}/\mathfrak{g}_1)$. (b) *The* Γ_q*-module* M_p' (M_p'') *has dimension* $p^{m'}$ $(p^{m''})$ *and a basis consisting of all monomials* 2.8 *corresponding to short (long) roots* r_i.

The proofs are as in § 8 and will be omitted. To supplement 11.3 we remark that $M_q = M_q' M_q''$, that M_q' is quite similar to the corresponding module for the group Γ of characteristic 0 (it is of the same dimension, by Weyl's formula), that M_q'' in contrast has lower dimension, that M_q' for $\sum$ of type B_l

and $q=2$ is just the spin module [13, p. 20-04] of dimension 2^l, and that $m'/m''=l'/l''$ in all cases [18, p. 501].

§ 12. Twisted groups

In this, the last, section we extend our results to the finite simple groups associated with the names of Suzuki [22] and Ree [11]. These are defined as follows. A system $\sum$ of type C_2, F_4 or G_2 may be identified with its dual $\sum^*$ in such a way that the map $r\to r^*$ of $\sum$ on $\sum^*$ (see § 10) yields an involutary map, σ, on $\sum$ such that positivity and simplicity of roots is preserved, angles are preserved, but short and long roots are interchanged. If also $(\sum, p)$ is special, K is algebraically closed, and $k\geq 1$, the isomorphism θ of 10.1(c) accordingly yields an automorphism of Γ which combines with the p^kth power map to produce an automorphism, also denoted σ, such that

12.1 $$x_r(t)^\sigma = x_{\sigma r}(t^{ps}),\ x_{\sigma r}(t)^\sigma = x_r(t^s) \qquad (r \text{ short},\ s=p^k).$$

If now $n=2k+1$ and $q=p^n$, the fixed points of σ form the sought simple group, to be denoted Γ_q^1, a subgroup of Γ_q. Observe (see 11.3) that $l'=l''$ and $m'=m''$ here.

12.2 Theorem. *If α_i denotes the p^ith power map, every irreducible Γ_q^1-module can be written uniquely as $\prod_{i=0}^{n-1} M_i^{\alpha_i}$ $(M_i\in\mathfrak{M}')$. If the rank of $\sum$ is l, there are $q^{l/2}$ such modules. Each can be realized over F_q.*

Proof. If $r>0$ and $t\in F_q$, Γ_q^1 contains an element of the form $x=x_r(t)x_{\sigma r}(t^{ps})\prod x_{r'}(t')$, the product over roots r' which are positive integral linear combinations of r and σr (proof by downward induction on the height of r). Thus if $v\in M\in\mathfrak{M}'$ and v is homogeneous,

12.3 $$(x-1)v = tX_r v + t^{ps}X_{\sigma r}v + \text{higher terms}.$$

If we refine the notion of height so that a positive linear combination of simple roots is taken to be lower than another one of the same height as previously defined if fewer short simple roots are used, then r is lower than σr. In fact, if $r=\sum[c(a)a+d(a)\sigma a]$, the sum over the short simple roots a, then $\sigma r=\sum[pd(a)a+c(a)\sigma a]$: since σ preserves angles, the map $r'\to p^{-1/2}\sigma r'$, $\sigma r'\to p^{1/2}r'$ (r' short) comes from an isometry, which maps r to $\sum[p^{-1/2}c(a)\sigma a+p^{1/2}d(a)a]=p^{-1/2}\sum[pd(a)a+c(a)\sigma a]$. With a corresponding refinement in the

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

notion of homogeneity, we thus get 12.3 with the second term of the right missing, and a similar equation for negative roots. Combining these equations with the key fact, proved as 11.1(1), that each $M \in \mathfrak{M}'$ is irreducible as $\mathfrak{g}_1$-module, we can now prove, almost exactly as in 5.1, that $\prod M_i^{a_i}$ $(M \in \mathfrak{M}')$ is irreducible. The proof that this product determines its components M_i can also be taken from 5.1. As for completeness of the set of $q^{l/2}$ product modules, the semisimple classes of Γ_q^1 are characterized by coordinates $\gamma(a)$ and $\gamma(\sigma a)$ $(a \in S, a$ short) for which $\gamma(a)^{p^s} = \gamma(\sigma a)$ and $\gamma(\sigma a)^s = \gamma(a)$ (see 3.9 and 12.1); their number is thus $q^{l/2}$, as required. Finally, as the restriction of a Γ_q-module, each irreducible Γ_q^1-module can be realized over F_q by 7.5.

As a supplement to 12.2 we have:

12.4. *For $\sum$ of type C_2 or F_4 and $p = 2$, every irreducible projective representation of Γ_q^1 can be lifted to an ordinary one.*

This result, proved in [21], quite likely also holds for the remaining case, $\sum$ of type G_2 and $p = 3$.

Also since the axioms of [17] are easily verified for the groups Γ_q^1 there is an analogue of 8.1, and modifying the development of § 8, we have no trouble in proving:

12.5 THEOREM. (a) *Γ_q^1 has an irreducible module M_q', constructed by the methods of* [17], *of dimension $q^{m/2}$, the order of a Sylow group in Γ_q^1 (here m is the number of positive roots in $\sum$).* (b) *M_q' is equivalent to the restriction to Γ_q^1 of the Γ_q-module M_q' of* 11.3. (c) *All other irreducible Γ_q^1-modules have lower dimensions than M_q'.*

From 12.2 we know all irreducible Γ_q^1-modules (in fact all Γ_q-modules also by 7.4, 11.1 and 11.2) once we know those in $\mathfrak{M}'$. We consider the individual cases. For $\sum$ of type C_2, $p^{l/2} = 2$, so that the trivial 1-dimensional module and the 4-dimensional module M_2' of 11.3(b), on which Γ_q acts as the symplectic group, exhaust $\mathfrak{M}'$. For $\sum$ of type G_2, $p^{l/2} = 3$, we have in $\mathfrak{M}'$ the trivial module, the module $\mathfrak{g}_1$, of dimension 7, and the module M_3' of 11.3(b), of dimension $3^3 = 27$. Finally, for $\sum$ of type F_4, $p^{l/2} = 4$, there are the trivial module, the module $\mathfrak{g}_1$, of dimension 26, and the module M_2', of dimension $2^{12} = 4096$, leaving one module yet to be described.

https://doi.org/10.1017/S0027763000011016 Published online by Cambridge University Press

References

[1] Brauer, R. and Nesbitt, C., On the modular representations of groups of finite order, U. of Toronto Studies (1937), 1-21.

[2] Brauer, R. and Nesbitt, C., On the modular characters of groups, Ann. of Math. **42** (1941), 556-590.

[3] Chevalley C., Sur certains groupes simples, Tôhoku Math. J. **7** (1955), 14-66.

[4] Curtis, C. W., Representations of Lie algebras of classical type with applications to linear groups, J. Math. and Mech. **9** (1960), 307-326.

[5] Curtis, C. W., On projective representations of certain finite groups, Proc. Amer. Math. Soc. **11** (1960), 852-860.

[6] Curtis, C. W., On the dimensions of the irreducible modules of Lie algebras of classical type, Trans. Amer. Math. Soc. **96** (1960), 135-142.

[7] Dickson, L. E., The abstract form (two papers), Quart. J. Math. **38** (1907), 141-158.

[8] Hertzig, D., Forms of algebraic groups, Proc. Amer. Math. Soc. **12** (1961), 657-660.

[9] Lang, S., Algebraic groups over finite fields, Amer. J. Math. **78** (1956), 555-563.

[10] Mark, C., Thesis, U. of Toronto.

[11] Ree, R., A family of simple groups associated with the simple Lie algebra of type (F_4), second paper: (G_2), Amer. J. Math. **83** (1961), 401-420, 432-462.

[12] Rosenlicht, M., Some rationality questions on algebraic groups, Ann. di Mat. **43** (1957), 25-50.

[13] Séminaire C. Chevalley, Classification des Groupes de Lie Algébriques (two volumes), Paris (1956-8).

[14] Séminaire "Sophus Lie," Paris (1954-5).

[15] Serre, J. P., Groupes algébtiques et corps de classes, Hermann, Paris (1959).

[16] Steinberg, R., A geometric approach, Trans. Amer. Math. Soc. **71** (1951), 274-282.

[17] Steinberg, R., Prime power representations of finite linear groups II, Can. J. Math. **9** (1957), 347-351.

[18] Steinberg, R., Finite reflection groups, Trans. Amer. Math. Soc. **91** (1959), 493-504.

[19] Steinberg, R., Variations on a theme of Chevalley, Pacific J. Math. **9** (1959), 875-891.

[20] Steinberg, R., The simplicity of certain groups, Pacific J. Math. **10** (1960), 1039-1041.

[21] Steinberg, R., Générateurs, relations et revêtements de groupes algébriques, Colloque sur la théorie des groupes algébriques, Bruxelles (1961).

[22] Suzuki, M., On a class of doubly transitive groups, Ann. of Math. **75** (1962), 105-145.

[23] Tits, J., Sur les analogues algébriques des groupes semisimple complexes, Colloque d'algèbre supérieure, Bruxelles (1956), 261-289.

[24] Tits, J., Les "formes réelles" des groupes de type E_6, Séminaire Bourbaki 162, Paris (1958).

[25] Tits, J., Sur la trialité et certains groupes qui s'en déduisent, Paris Inst. Hautes Etudes Sci. Publ. Math. **2** (1959), 37-84.

[26] Weyl, H., Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformationen III, Math. Zeit (1926), 377-395.

[27] Wong, W. J., Thesis, Harvard U.

Institute for Advanced Study, Princeton
University of California, Los Angeles