Invent. math. 76, 469–514

Inventiones mathematicae

On the maximal subgroups of the finite classical groups

M. Aschbacher*

California Institute of Technology Pasadena, CA 91125, USA

Let G_0 be a finite simple classical group and G a group whose generalized Fitting subgroup $F^*(G)$ is isomorphic to G_0; equivalently $G_0 \leqq G \leqq \mathrm{Aut}(G_0)$. If $G_0 \cong P\Omega_8^+(q)$ assume no element of G induces a triality automorphism. A collection of subgroups $\mathscr{C}_G$ of G is defined, and it is shown that:

Theorem. Let G be a finite group whose generalized Fitting subgroup is a simple classical group G_0 over a finite field. If $G_0 \cong P\Omega_8^+(q)$ assume no element of G induces a triality automorphism on G_0. Let H be a proper subgroup of G such that $G = HG_0$. Then either H is contained in some member of $\mathscr{C}_G$ or the following hold:

1) $F^*(H)$ is a nonabelian simple group.

2) Let L be the covering group of $F^*(H)$ and V the natural projective module for G_0. Then V is an absolutely irreducible FL-module.

3) The representation of L on V is defined over no proper subfield of F.

4) If $a \in \mathrm{Aut}(F)$, V^* is the dual of V, and V is FL-isomorphic to V^{*a}, then either

i) $a = 1$ and G_0 is orthogonal or symplectic, or

ii) a is an involution and G_0 is unitary.

The definition of $\mathscr{C}_G$ appears in Sect. 1, 13 or 14, unless G_0 is $P\Omega_8^+(q)$ and G contains an element inducing an automorphism of order 3 on the Dynkin diagram of G_0, where no attempt is made to define a collection. Section 15 does contain some remarks relevant to this last case. The isomorphism type of the members of $\mathscr{C}_G$ and the action of G on $\mathscr{C}_G$ by conjugation is also (essentially) described in Sects. 1, 13, and 14. Presumably the members of $\mathscr{C}_G$ are maximal subgroups of G, with a few exceptions, but that question is not addressed here. The members of $\mathscr{C}_G$ are (essentially) the stabilizers of certain structures on the natural module for the classical group G_0.

The Main Theorem is intended to be one of the early pieces in a theory of permutation representations of finite groups based on the classification of the finite simple groups. The primitive permutation representations serve as the

* Partial support supplied by the National Science Foundation

irreducibles in this theory. The study of such representations is equivalent to the study of the maximal subgroups of finite groups. In [2] the primitive permutation representations of the general finite group are described in terms of:

(a) The 1-cohomology of finite simple groups on irreducible modules over fields of prime order, and

(b) The maximal subgroups M of groups G such that $F^*(G)$ is simple and $G = MF^*(G)$.

This focuses attention on the pairs (M^G, G) appearing in (b). If $F^*(G)$ is a sporadic simple group it seems certain that the conjugacy classes of maximal subgroups of G can be determined explicitly. This has already been accomplished for almost half of the 26 sporadic groups. If $F^*(G)$ is an exceptional group of Lie type it seems that it might be possible to achieve the same result. This leaves the alternating groups and classical groups. It is far from clear that the conjugacy classes of maximal subgroups of these groups can be explicitly determined; indeed it may not even be desirable to do so. However given the fundamental role of permutation representations in the theory of finite groups and in the applications of that theory, some systematic description of the maximal subgroups of these groups must be regarded as one of the most important goals of finite group theory.

The first step in such a theory is to describe the obvious maximal subgroups of our group. This was done when $F^*(G)$ is an alternating group by O'Nan and Scott, independently. Each discussed his work at the Santa Cruz conference in 1979; a statement of Scott's result appears in the appendix to [2]. The Main Theorem of this paper accomplishes the same goal when $F^*(G)$ is a classical group, modulo some more work when $F^*(G) \cong P\Omega_8^+(q)$ and some member of G induces a triality automorphism.

In summary if (M^G, G) is a pair appearing in (b), then we can hope to determine the class M^G explicitly if $F^*G)$ is a sporadic group or an exceptional group of Lie type. If $F^*(G)$ is an alternating group or a classical group, then the Main Theorem together with the O'Nan-Scott theorem reduces the problem to the case where $F^*(M)$ is a nonabelian simple group and the restriction of the natural representation of $F^*(G)$ to $F^*(M)$ is a well behaved irreducible in the appropriate category. The hardest part of the problem is untouched: Develop a useful description of the nonobvious classes of maximal subgroups of the alternating groups and classical groups.

The author would like to thank Richard Lyons, Steve Smith, and particularly David Wales for useful conversations on representation theory.

Section 1. The definition of $\mathscr{C}_G$

In this section F is a finite field of characteristic p and V is an n-dimensional vector space over F. f is either an F-bilinear form on V or an F-sesquilinear form on V with respect to an automorphism of F of order 2. We are primarily interested in four cases:

I. f trivial,
II. f symplectic,
III. f orthogonal with quadratic form Q,
IV. f unitary.

f is trivial if $V=V^{\perp}$ is self radical. In the remaining cases by definition f is nondegenerate (i.e. $V^{\perp}=0$), with f bilinear and skew symmetric in case II, f bilinear and symmetric in case III, and f sesquilinear and hermitian symmetric in case IV. In case III we also require that V admit a quadratic form Q.

If p is odd then Q is determined by f up to a scalar multiple, and we usually normalize and take $Q(x)=f(x,x)$. If $p=2$ there are many quadratic forms Q on V satisfying $Q(x+y)+Q(x)+Q(y)=f(x,y)$, in which case we say f is the bilinear form associated to Q.

Recall that a subspace U of V is *totally singular* if the restriction of f to U is trivial, and in case III also the restriction of Q to U is trivial. U is *nondegenerate* if the restriction of f to U is nondegenerate. The *Witt index* of V is the dimension of a maximal totally singular subspace of V. In case III if n is even then V has Witt index $n/2$ or $(n/2)-1$, and we define the *sign* of f (or Q) to be $+1$ or -1 in the respective case. Write $\mathrm{sgn}(f)$ (or $\mathrm{sgn}(Q)$) for the sign.

Recall that n is even in case II and also in case III when $p=2$. If f is bilinear let $\mathrm{sym}(f)=+1$ if f is symmetric and $\mathrm{sym}(f)=-1$ if f is skew symmetric. Of course if $p=2$ then symmetry and skew symmetry are the same, so $\mathrm{sym}(f)$ should be read modulo p.

An *isometry* of spaces (V,f) and (V',f') (or (V,Q) and (V',Q')) is a vector space isomorphism α: $V\to V'$ such that $f(x,y)=f'(x\alpha,y\alpha)$ (or $Q(x)=Q'(x\alpha)$) for all x, $y\in V$. A *similarity* of the spaces is a vector space isomorphism α such that $\tau(\alpha)f(x,y)=f'(x\alpha,y\alpha)$ (or $\tau(\alpha)Q(x)=Q'(x\alpha)$) for all x, $y\in V$ and some $\tau(\alpha)\in F^{\#}$ depending on α but not x and y.

It turns out spaces (V_i,f_i) (or (V_i,Q_i)), $i=1,2$, are similar if and only if $\dim(V_1)=\dim(V_2)$, the type of the spaces are the same (i.e. of the same type I–IV), and $\mathrm{sgn}(Q_1)=\mathrm{sgn}(Q_2)$ if case III holds and $\dim(V_1)$ is even. Further it happens that similar spaces are isometric, except in case III in odd dimension where there are two isometry types which can be differentiated by whether $Q(v)$ is a residue or nonresidue in F, for $\langle v\rangle=U^{\perp}$ and U a nondegenerate hyperplane of V of sign $+1$. We use these remarks, often without comment, throughout the paper.

Denote by $O(V,f)$ (or $O(V,Q)$) the group of all isometries of the space (V,f) (or (V,Q)) and write $\Delta(V,f)$ (or $\Delta(V,Q)$) for the group of all similarities of the space. Let $\Gamma(V)$ denote the group of all semilinear transformations of V: That is the group of invertible maps α from V to V preserving addition and with $(av)\alpha=a^{\sigma(\alpha)}(v\alpha)$ for all $v\in V$ and $a\in F$, and for some $\sigma(\alpha)\in\mathrm{Aut}(F)$ depending on α but not a and v. $\Gamma(V,f)$ (or $\Gamma(V,Q)$) denotes those α with $f(x\alpha,y\alpha)=\tau(\alpha)f(x,y)^{\sigma(\alpha)}$ (or $Q(x\alpha)=\tau(\alpha)Q(x)^{\sigma(\alpha)}$) for all $x,y\in V$ and some $\tau(\alpha)\in F^{\#}$. Finally let $\Omega(V,f)$ be the commutator group of $O(V,f)$. Then $\Omega(V,f)\leqq O(V,f)\leqq\Delta(V,f)\leqq\Gamma(V,f)$ is a $\Gamma(V,f)$-invariant sequence of groups.

If we wish to emphasize the role of F we write (V,F), (V,f,F), $O(V,f,F)$, etc. This is necessary as we will often regard V as a vectorspace over some extension field or subfield of F. Notice in case I that $O(V,f)=GL(V)$ is the general linear group on V.

Let $P\Omega(V,f)=\Omega(V,f)/Z(\Omega(V,f))$. Usually $P\Omega(V,f)$ is simple. The finite simple classical groups are the groups $P\Omega(V,f)$.

Given spaces (V_i,f_i), $1\leqq i\leqq m$, define $f_1\otimes\ldots\otimes f_m$ to be the unique form on $V_1\otimes\ldots\otimes V_m$ such that

$$(f_1\otimes\ldots\otimes f_m)(v_1\otimes\ldots\otimes v_m, u_1\otimes\ldots\otimes u_m)=\prod_{i=1}^{m} f_i(v_i,u_i)$$

for all $u_i, v_i\in V_i$.

We are now in a position to define eight collections C_i, $1\leqq i\leqq 8$, of subgroups of $\Gamma=\Gamma(V,f)$ (or $\Gamma(V,Q)$). Let $\Delta=\Delta(V,f)$, $O=O(V,f)$, and $\Omega=\Omega(V,f)$ (or $\Delta(V,Q)$, $O(V,Q)$ and $\Omega(V,Q)$).

C_1 consists of the stabilizers of nontrivial proper subspaces U of V such that U is nondegenerate or totally singular, or U is a nonsingular point of V in case III with $p=2$. We also require that U is not isometric to $U^\perp$ if U is nondegenerate.

C_2 consists of the stabilizers of sets S of subspaces of V such that $V=\bigoplus_{U\in S} U$ and one of the following holds:

$(C_2 1)$ The sum is orthogonal and each member of S is of the same isometry type.

$(C_2 2)$ $S=\{U,U^\perp\}$, p is odd, case III holds, $\dim(U)$ is odd, and U and $U^\perp$ are similar.

$C_2 3)$ $S=\{U,W\}$ and U and W are totally singular of dimension $n/2$. In case II if $n=4$ then p is odd.

C_3 consists of the groups $N_\Gamma(K)$, where K varies over the extension fields of F of prime index dividing n such that the F-space structure on V extends to a K-structure, and such that $C_0(K)$ is irreducible on V.

C_4 consists of the groups $\Gamma(\mathscr{D})\pi$ (in the notation of 9.2) as $\mathscr{D}$ varies over the families $((V_1,f_1),(V_2,f_2))$ of nonisometric F-spaces such that (V,f) is isometric to $(V_1\otimes V_2, f_1\otimes f_2)$. In case II we require p to be odd.

C_5 consists of the groups $N_\Gamma(U)F$ as K varies over the subfields of F of prime index r and U varies over the n-dimensional K-subspaces of V such that U is an absolutely irreducible $KN_0(U)$-module.

C_6 consists of the groups $N_\Gamma(R)$, where $n=r^m$ is a power of a prime $r\neq p$ and R varies over the r-groups of symplectic type such that $|R:Z(R)|=r^{2m}$, R is of exponent r if r is odd and of exponent 4 if $r=2$, R acts irreducibly on V, and one of:

$(C_6 1)$ $|Z(R)|>2$, $|F|=p^e$ where e is the order of p in the group of units of the integers modulo $|Z(R)|$, case I holds if e is odd, and case IV holds if e is even.

$(C_6 2)$ Case II holds, $|Z(R)|=2$, $|F|=p$, and $R\cong(D_8)^{m-1}Q_8$.

$(C_6 3)$ Case III holds with $\mathrm{sgn}(Q)=+1$, $|Z(R)|=2$, $|F|=p$, and $R\cong(D_8)^m$.

C_7 consists of the groups $\Delta(\mathscr{D},\mathscr{F})\pi$ (in the notation of 9.2) as $\mathscr{D}$ varies over the families $(V_i,f_i)\colon 1\leqq i\leqq m)$ of F-spaces and $\mathscr{F}$ over the families $(\alpha_i\colon 1\leqq i\leqq m)$ of similarities α_i: $(V_1,f_1)\to(V_i,f_i)$ with $\alpha_i=1$ such that (V,f) is isometric to $(V_1\otimes\ldots\otimes V_m, f_1\otimes\ldots\otimes f_m)$. In case II we require p to be odd. We also require that $\Omega(V_1,f_1)$ be quasisimple.

C_8 consists of the subgroups $\Gamma(V,g)$ as g varies over the F-forms on V subject to one of the following:

($C_8$1) Case I holds and g is unitary or symplectic, or p is odd and g is orthogonal.

($C_8$2) Case II holds, $p=2$, and g is a quadratic form with associated bilinear form f.

Let C be the union of the collections C_i, $1\leqq i\leqq 8$. If $\Omega\leqq G\leqq\Gamma$ define $\mathscr{C}_G$ to consist of the groups $G\cap H$ as H varies over C. If $P\Omega\leqq G\leqq P\Gamma$, where P denotes the projection map $\Gamma\to\Gamma/C_\Gamma(\Omega)$, then define $\mathscr{C}_G$ to consist of the groups $P\tilde{M}$, where $\tilde{G}$ is the preimage in Γ of G under the projection map P, and $\tilde{M}$ varies over $\mathscr{C}_{\tilde{G}}$.

Recall that either $P\Gamma=\mathrm{Aut}(P\Omega)$ or $P\Omega\cong L_n(q)$, $PSp_4(q)$ or $P\Omega_8^+(q)$ and $|\mathrm{Aut}(P\Omega): P\Gamma|=2$, 2, or 3, respectively. In the first two cases $\mathscr{C}_G$ is defined and discussed in Sects. 13 and 14, respectively. If $P\Omega\cong P\Omega_8^+(q)$ and $P\Omega\leqq G\leqq\mathrm{Aut}(P\Omega)$, then either there is an injective homomorphism of G into $P\Gamma$ or G contains an element inducing an automorphism of order 3 on the Dynkin diagram of $P\Omega$. In the first instance we may take $G\leqq P\Gamma$, so that $\mathscr{C}_G$ is defined (subject to this representation); in the second we make no attempt to define $\mathscr{C}_G$, although Sect. 15 contains some relevant remarks.

The next result describes the structure of the members of C.

Theorem A. (1) *If $H\in C_3$ then there exists a K-form g on V, and in case* III *if g is bilinear, a K-quadratic form P on V associated to g, such that* $g\mathrm{Tr}_F^K=f$, $P\mathrm{Tr}_F^K=Q$, *and if g is unitary and case* III *holds, also* $g\mathrm{Tr}_F^K=Q$, *where E is the subfield of K of index* 2. *Moreover either $H=\Gamma_F(V,g,K)$ or P is defined and $H=\Gamma_F(V,P,K)$. Finally one of the following holds:*

i) f and g are trivial.

ii) *f and g are unitary and r is odd.*

iii) *f and g are nondegenerate bilinear*, $\mathrm{sym}(f)=\mathrm{sym}(g)$, *and in case* III $\mathrm{sgn}(Q)=\mathrm{sgn}(P)$ *if* $\dim_K(V)$ *is even.*

iv) *Case* II *or* III *holds, g is unitary, $r=2$, and in* III $\mathrm{sgn}(Q)=(-1)^{\dim_K(V)}$.

(2) *If $H\in C_4$ then $H=\Gamma(\mathscr{D})\pi$ and its action on V are described in Lemmas* 9.2 *and* 3.12. *Moreover one of the following holds:*

i) *f, f_1, and f_2 are trivial.*

ii) *f, f_1, and f_2 are unitary.*

iii) *f, f_1, and f_2 are orthogonal or symplectic with* $\mathrm{sym}(f)=\mathrm{sym}(f_1)\,\mathrm{sym}(f_2)$. *In case* III *if $p=2$ then* $\mathrm{sgn}(Q)=+1$, *while if p is odd then one of the following holds:*

(a) *n is even and* $\mathrm{sgn}(f)=+1$.

(b) *For some* $i\in\{1,2\}$, $\dim(V_i)$ *and n are even*, $\mathrm{sym}(f_1)=\mathrm{sym}(f_2)=+1$, $\dim(V_{3-i})$ *is odd, and* $\mathrm{sgn}(f_i)=\mathrm{sgn}(f)=-1$.

(3) *if $H\in C_5$ then there exists a K-form g on V, and in case* III *a K-quadratic form P on V associated to g, such that f and Q are obtained from g and P via a tensoring process described in Sect.* 8, $N_\Gamma(U)=A\Delta(U,g)$ (*or* $A\Delta(U,P)$) *where A is described in* 3.2.2 *and* 6.5, *and one of the following holds:*

i) *f and g are trivial.*

ii) *Case* II *holds and g is symplectic.*

iii) *Case* III *holds, g is orthogonal, P exists, and* $\mathrm{sgn}(Q)=\mathrm{sgn}(P)^r$ *if n is even.*

iv) *Case* IV *holds as does one of:*

(a) *g is unitary and r is odd.*

(b) *g is nondegenerate and symmetric and* $r=2$.

(c) *g is symplectic,* $r=2$, *and p is odd.*

4) *If* $H\in C_6$ *then* H/F *is isomorphic to* $C_{\mathrm{Aut}(R)}(Z(R))$ *extended by the group of field automorphisms of F.*

(5) *If* $H\in C_7$ *then* $H=\Lambda(\mathcal{D},\mathcal{F})\pi$ *and its action on V are described in Lemma* 3.12 *and* 9.2. *Moreover one of the following holds:*

i) *f and* f_1 *are trivial.*

ii) *f and* f_1 *are unitary.*

iii) *f and* f_1 *are orthogonal or symplectic with* $\mathrm{sym}(f)=\mathrm{sym}(f_1)^m$. *In case* III *if* $p=2$ *then* $\mathrm{sgn}(Q)=+1$, *while if p is odd then either*

(a) *n is even and* $\mathrm{sgn}(f)=+1$, *or*

(b) *n and* $\dim(V_1)$ *are odd and* f_1 *is orthogonal.*

It is assumed that the structure of the groups in C_1, C_2, and C_8 are well known; the structure of the groups in case $(C_2 3)$ is described in Lemma 5.4. In (1), $\alpha=\mathrm{Tr}_F^K$ is the trace of K to F and $g\alpha$ and $P\alpha$ are the corresponding compositions. $\Gamma_F(V,g,K)$ is the subgroup of $\Gamma(V,g,K)$ consisting of those x with $\tau(x)\in F$. For $G\leqq\Gamma$ and $H\in C$, the index of $H\cap G$ in H is small, so the structure of the members of $\mathscr{C}_G$ can be retrieved from Theorem A and from Theorem B, which can be used to determine $|H:H\cap G|$.

We next state Theorem *B* which can be used to determine the action of G on $\mathscr{C}_G$. Theorem *B* comes in four parts dealing with the cases $G=\Gamma,\Delta,O$, and Ω.

Theorem $B\Gamma$. *The orbits of* Δ *and* Γ *on C are the same.*

Theorem $B\Delta$. *The action of* Δ *on* C_i *is described below in case* (i) *for* $1\leqq i\leqq 8$:

(1) Δ *is transitive on subspaces of V of the same isometry type, except in case* III *when p is odd and n is even, where* Δ *is transitive on subspaces of the same similarity type. Hence* Δ *is transitive on the corresponding stabilizers.*

(2) Δ *is transitive on the stabilizers in* $(C_2 2)$ *and* $(C_2 3)$. *Stabilizers of collections S and S′ in* $(C_2 1)$ *are conjugate in* Δ *if and only if either*

(a) *The members of S are isometric to those of S′, or*

(b) *Case* III *holds, p is odd, n is even, and the members of S are similar to those of S′.*

(3) *For each prime divisor r of n,* Δ *is transitive on normalizers of extensions of F of degree r in* C_3, *unless case* II *or* III *holds with* $r=2$, *n even, and in* III $\mathrm{sgn}(Q)=(-1)^{n/2}$. *Here* Δ *is transitive on normalizers preserving symplectic forms or quadratic forms and on normalizers preserving unitary forms.*

(4) *Stabilizers of pairs* $\mathcal{D}=((V_1,f_1),(V_2,f_2))$ *and* $\mathcal{D}'=((V_f',f_1'),(V_2',f_2'))$ *are conjugate under* Δ *if and only if* (V_i,f_i) *is isometric to* $(V_{i\sigma}',f_{i\sigma}')$ *for* $i=1$ *and* 2, *and for some permutation* σ *of* $\{1,2\}$.

(5) *For each prime divisor r of e (where $|F|=p^e$), Δ is transitive on the subgroups in C_5 determined by the subfield K of F of index r, unless $r=2$ and either*

(a) *Case* III *holds with n even and* $\operatorname{sgn}(Q)=+1$, *where Δ is transitive on the subgroups in C_5 determined by K preserving forms of sign $+1$ and those preserving forms of sign -1, or*

(b) *Case* IV *holds with p odd and n even, where Δ is transitive on the subgroups in C_5 determined by K preserving symplectic form, on those preserving quadratic forms of sign $+1$, and on those preserving quadratic forms of sign -1.*

(6) *Δ is transitive on the members of C_6.*

(7) *Stabilizers of families $(\mathscr{D},\mathscr{F})$ and $(\mathscr{D}',\mathscr{F}')$ determined by triples (V_1,f_1,m) and (V_1',f_1,m') are conjugate under Δ if and only if $m=m'$ and (V_1,f_1) is similar to (V_1',f_1').*

(8) *Δ is transitive on stabilizers of forms of the same similarity type.*

Theorem *BO*. *Let $M\in C$. Then $M^0=M^\Delta$ unless p is odd, n is even, case* II *or case* III *holds, M^Δ splits into two O-orbits of equal length, and one of the following holds:*

(1) *$M\in C_1$ is the stabilizer of a nondegenerate space of odd dimension. (So that case* III *holds.) The O-orbits in M^Δ correspond to the isometry classes.*

(2) *$M\in C_5$ and $r=2$.*

(3) *$M\in C_6$, $r=2$, and $|F|=p\equiv \pm 1 \bmod 8$.*

Theorem *BΩ*. *Let $M\in C$. Then*

(1) *M^0 splits into $d(M)$ Ω-orbits of equal length.*

(2) *In case* II, *$M^0=M^\Omega$.*

(3) *In case* I, *$d(M)$ divides $(n,|F^{\#}|)$.*

(4) *In case* IV *$d(M)$ divides $(n,q+1)$, where $q^2=|F|$.*

(5) *In case* III, *$d(M)\leqq 2$ unless n is even, p is odd,* $\operatorname{sgn}(f)\equiv|F|^{n/2} \bmod 4$, *and* $d(M)=4$.

We will need the notion of a *standard basis* for V in cases II–IV. In case IV a standard basis (or *unitary basis*) is just an orthonormal basis. In case II a standard basis (or *symplectic basis*) is a basis $X=(x_i\colon 1\leqq i\leqq n)$ with $f(x_{2i-1},x_{2i})=1$, $f(x_{2i},x_{2i-1})=-1$ and $f(x_k,x_l)=0$ otherwise. This leaves case III. If $p=2$ then a standard basis (or *orthogonal basis*) is a symplectic basis for which $Q(x_k)=0$ for $k<n-1$, $Q(x_{n-1})=Q(x_n)=0$ if $\operatorname{sgn}(Q)=+1$ while $Q(a\,x_{n-1}+b\,x_n)=a^2\alpha+ab+b^2\alpha$ for some irreducible quadratic $\alpha x^2+x+\alpha$ in $F[x]$ if $\operatorname{sgn}(Q)=-1$. So let p be odd. If n is even and $\operatorname{sgn}(Q)=+1$ then $f(x_{2i-1},x_{2i})=f(x_{2i},x_{2i-1})=1$, and $f(x_k,x_l)=0$ otherwise. If n is odd, $\{x_i\colon i<n\}$ is an orthogonal basis for the subspace of sign $+1$ it generates and x_n is a generator for its orthogonal complement with $Q(x_n)=1$ or α, α a generator of $F^{\#}$. Finally if n is even and $\operatorname{sgn}(Q)=-1$ then $\{x_i\colon i<n-1\}$ is an orthogonal basis for the subspace of sign $+1$ it generates and $\{x_{n-1},x_n\}$ is a basis for its orthogonal complement with $Q(x_{n-1})=1$, $Q(x_n)=-\alpha$, and $f(x_{n-1},x_n)=0$.

Section 2. Representations

Let $\mathfrak{A}$ be a category and G a group. An $\mathfrak{A}$-*representation* of G is a group homomorphism π of G into the group $\mathrm{Aut}(X)$ of automorphisms of some object X in $\mathfrak{A}$. Two $\mathfrak{A}$-representations π_i: $G \to \mathrm{Aut}(X_i)$, $i=1,2$, are said to be *equivalent* if there exists an isomorphism α: $X_1 \to X_2$ such that $\pi_2 = \pi_1 \alpha^*$, where α^*: $\mathrm{Aut}(X_1) \to \mathrm{Aut}(X_2)$ is the isomorphism taking $\beta \in \mathrm{Aut}(X_1)$ to $\beta^\alpha = \alpha^{-1} \beta \alpha$. Hence if we let $R(G,X)$ denote the set of all representations of G on X, we see that:

(2.1) $\mathrm{Aut}(X)$ *acts on* $R(G,X)$ *via* α: $\pi \to \pi\alpha^*$, *for* $\alpha \in \mathrm{Aut}(X)$ *and* $\pi \in R(G,X)$. *Indeed for* $\pi, \pi' \in R(G,X)$, π *is equivalent to* π' *if and only if* $\pi' \in \pi\,\mathrm{Aut}(X)$.

Denote by $R(G,X)/\mathrm{Aut}(X)$ the set of orbits of $\mathrm{Aut}(X)$ on $R(G,X)$. Observe next that:

(2.2) $\mathrm{Aut}(G)$ *acts on* $R(G,X)$ *via* β: $\pi \to \beta\pi$, *for* $\beta \in \mathrm{Aut}(G)$ *and* $\pi \in R(G,X)$. *Further this action induces an action* β: $\pi\,\mathrm{Aut}(X) \to (\beta\pi)\,\mathrm{Aut}(X)$ *of* $\mathrm{Aut}(G)$ *on* $R(G,X)/\mathrm{Aut}(X)$.

Define two $\mathfrak{A}$-representations π_1 and π_2 of G to be *quasiequivalent* if there exists $\beta \in \mathrm{Aut}(G)$ with π_1 equivalent to $\beta\pi_2$. Evidently

(2.3) $\pi, \pi' \in R(G,X)$ *are quasiequivalent if and only if* $\pi' \in \mathrm{Aut}(G)\,\pi\,\mathrm{Aut}(X)$.

A representation π is *faithful* if π is an injection.

(2.4) *Let* π, $\sigma \in R(G,X)$ *be faithful. Then* $G\pi$ *is conjugate to* $G\sigma$ *in* $\mathrm{Aut}(X)$ *if and only if* π *is quasiequivalent to* σ.

Proof. Let $\alpha \in \mathrm{Aut}(X)$ with $(G\pi)^\alpha = G\sigma$ and define $\beta \in \mathrm{Aut}(G)$ by $\beta = \pi\alpha^*\sigma^{-1}$. Then $\sigma = \beta^{-1}\pi\alpha^* \in \mathrm{Aut}(G)\,\pi\,\mathrm{Aut}(X)$, so π and σ are quasiequivalent. Conversely if π and σ are quasiequivalent, there exists $\beta \in \mathrm{Aut}(G)$ and $\alpha \in \mathrm{Aut}(X)$ with $\sigma = \beta\pi\alpha^*$, so $G\sigma = G\beta\pi\alpha^* = (G\pi)^a$.

Observe next that if $\pi \in R(G,X)$ is faithful then π induces an isomorphism π^*: $\mathrm{Aut}(G) \to \mathrm{Aut}(G\pi)$ via π^*: $\beta \to \beta^\pi$, for $\beta \in \mathrm{Aut}(G)$.

(2.5) *Let* $\pi \in R(G,X)$ *be faithful and* $\beta \in \mathrm{Aut}(G)$. *Then*

(1) $\beta\pi$ *is equivalent to* π *if and only if* $\beta\pi^* \in \mathrm{Aut}_{\mathrm{Aut}(X)}(G\pi)$.

(2) $\mathrm{Aut}(G)$ *acts transitively on the equivalence classes in* $R(G,X)/\mathrm{Aut}(X)$ *contained in the quasiequivalence class of* π, *with* $(\pi^*)^{-1}(\mathrm{Aut}_{\mathrm{Aut}(X)}(G\pi))$ *the stabilizer in* $\mathrm{Aut}(G)$ *of* $\pi\,\mathrm{Aut}(X)$ *under this action.*

Proof. $\beta\pi\,\mathrm{Aut}(X) = \pi\,\mathrm{Aut}(X)$ if and only if $\pi = \beta\pi\alpha^*$ for some $\alpha \in \mathrm{Aut}(X)$ if and only if $\alpha \in N_{\mathrm{Aut}(X)}(G\pi)$ and α^{-1} induces $(\beta)\pi^*$ on $G\pi$. Hence the lemma holds.

(2.6) *Let* F *be a finite field and* X *a finite dimensional vector space over* F. *Let* $\mathfrak{A}$ *and* $\mathcal{B}$ *be the categories whose objects are* F-*spaces and whose morphisms are* F-*linear maps and* F-*semilinear maps respectively. Let* π: $G \to \mathrm{Aut}(X)$ *be a representation of* G *in* $\mathfrak{A}$ *and assume for all* $\sigma \in \mathrm{Aut}(F)$ *that* π^σ *is* $\mathfrak{A}$-*quasiequivalent to* π. *Then the quasiequivalence classes of* π *in* $\mathfrak{A}$ *and* $\mathcal{B}$ *are the same.*

Proof. $\mathrm{Aut}(X)=GL(X)$ and $\Gamma(X)$ in the categories $\mathfrak{A}$ and $\mathscr{B}$, respectively, and $GL(X)\subseteq\Gamma(X)$, so we must show that if $\alpha\in\Gamma(X)$ then $\pi\alpha^*\in\mathrm{Aut}(G)\pi GL(X)$. Now $\alpha=\beta\gamma$ for some $\beta\in GL(X)$ and some field automorphism γ, and without loss $\beta=1$. But $\pi\gamma^*=\pi^\sigma$ for some $\sigma\in\mathrm{Aut}(F)$, and by hypothesis $\pi^\sigma\in\mathrm{Aut}(G)\pi GL(X)$, so the proof is complete.

Section 3. Linear representations

In this section F is a finite field and G is a finite group. Several of the arguments in this section were suggested by David Wales.

(3.1) *Let K be a finite extension of F, and $\alpha\in\mathrm{Hom}_F(K,F)^\#$. For $x\in K$ let π_x: $K\to K$ be multiplication by x. Then the map φ: $x\to\pi_x\alpha$ is an F-vector space isomorphism between K and $\mathrm{Hom}_F(K,F)$.*

Proof. Let $z\in K$ with $K=F(z)$ and set $n=|K:F|$. Then $Z=\{z^i: 0\leqq i<n\}$ forms a basis for K over F. For $x\in K$, $\pi_x\in\mathrm{Hom}_F(K,K)$, so $\pi_x\alpha=\beta_x\in\mathrm{Hom}_F(K,F)=H$. We show $B=\{\beta_x: x\in Z\}$ is linearly independent of order n in H. Then as $\dim_F(H)=n$, B is a basis for H. Further φ is a linear transformation which maps the basis Z of K to the basis B of H, so φ is an isomorphism.

It remains to show B is linearly independent of order n. Let $\gamma\in H$ with $1\gamma=1$ and $z^i\gamma=0$ for $0<i<n$. We show $\{\pi_x\gamma: x\in Z\}$ is independent of order n, so that ψ: $x\to\pi_x\gamma$ is an isomorphism. Thus $\alpha=\pi_y\gamma$ for some $y\in K^\#$, so $x\pi_y\psi=xy\psi=\pi_{xy}\gamma=\pi_x\pi_y\gamma=\pi_x\alpha=x\varphi$. Hence $\varphi=\pi_y\psi$, so as π_y is an F-automorphism of K, φ is an isomorphism. Thus we may take $\alpha=\gamma$. Assume that $\sum a_i\beta_{z^i}=0$ for some $a_i\in F$ not all zero and let $m=\min\{i: a_i\neq 0\}$. Then $0=(z^{-m}(\sum a_i z^i))\alpha=\sum a_i(z^{i-m})\alpha=a_m$, contradicting the choice of m.

(3.2) *Let α: $G\to GL(V)$ be an irreducible FG-representation, $K=\mathrm{Hom}_{FG}(V,V)$, β the representation of G on V as a KG-module, and χ the character of β. Then $K=F(\chi)$ where $F(\chi)$ is the field generated by F and the elements $\chi(g)$, $g\in G$.*

Proof. Let X be a basis for V over K. Then for $g\in G$, $g\beta=g\alpha$ as a map of V, and $\chi(g)=\mathrm{Tr}(A(g\beta))$, where $A(g\beta)$ is the matrix of $g\beta$ with respect to X. Let $m=|X|$, M the ring of all m by m matrices over K, and R the F-*subalgebra of* M generated by the matrices $A(g)$, $g\in G$. By a theorem of Wedderburn, $R=M$. Thus there is $r\in R$ with $\mathrm{Tr}(r)$ a generator for K over F. But $r=\sum a_g A(g)$ for some $a_g\in F$, *so* $\mathrm{Tr}(r)=\sum a_g\chi(g)\in F(\chi)$. Thus the lemma holds.

(3.3) *Assume the hypothesis of* 3.2, *let L be a finite extension of K, and let $\sigma\in\mathrm{Gal}(K/F)^\#$. Then $L\otimes_K V^\sigma$ is not LG-isomorphic to $L\otimes_K V$.*

Proof. Let E be the fixed field of σ. As $\sigma\neq 1$, $E\neq K$. As $K=\mathrm{Hom}_{EG}(V,V)$, we may assume $E=F$. Let γ be an extension of σ to L and $U=L\otimes_K V$. Then $L\otimes_K V^\sigma=U^\gamma$, and the character of U is still the character χ of β. Thus if U is LG-isomorphic to $L\otimes_K V^\sigma=U^\gamma$ then $\chi=\chi^\gamma$, so $\chi(g)$ is contained in the fixed field k of γ. But $k\cap K=F$, so by 3.2, $K=F$, a contradiction.

(3.4) *Let K be a finite extension of F and V an irreducible KG-module. Then V is a KG-composition factor of $K\otimes_F U$ for each irreducible FG-submodule U of V.*

Proof. Let X be a basis for U over F so that $1\otimes X$ is a basis for $U_K=K\otimes_F U$ over K. Define

$$\alpha\colon\ U_K\to V,$$

$$\sum_{x\in X} a_x(1\otimes x)\to \sum_{x\in X} a_x x \qquad a_x\in K.$$

Then α is a surjective KG-homomorphism, so $U_K/\ker(\alpha)$ is KG-isomorphic to V.

(3.5) *Let V be an irreducible FG-module, k a finite extension of F, and $K=\mathrm{Hom}_{FG}(V,V)$. Then*

(1) *$V_k=k\otimes_F V=\bigoplus_{\sigma\in A} W^\sigma$ for some irreducible kG-module W and some $A\subseteq \mathrm{Gal}(k/F)=\Gamma$, and $\Gamma=N_\Gamma(W)A$.*

(2) *If $k\leqq K$ then $A=\mathrm{Gal}(k/F)$ and W^σ is kG-isomorphic to V for some $\sigma\in A$.*

(3) *If a and b are distinct members of A then W^a is not kG-isomorphic to W^b; hence A is a set of coset representatives for $N_\Gamma(W)$ in Γ.*

Proof. Part (1) appears as 5.13.3 in [4]. Assume $k\subseteq K$. As V_k is a semisimple kG-module generated by the simple kG-modules $\{W^a\colon a\in A\}$, we conclude from 3.4 that V is kG-isomorphic to W^σ for some $\sigma\in A$, and without loss $\sigma=1$. Now $|A|=\dim_F(V)/\dim_k(V)=|k\colon F|=|\mathrm{Gal}(k/F)|$, so $A=\mathrm{Gal}(k/F)$. Thus (2) holds.

To prove (3), let L be the field generated by K and k. By (2), $V_L=L\otimes_K V_K=\bigoplus_{\sigma\in\mathrm{Gal}(K/F)}(L\otimes_K U^\sigma)$ with U KG-isomorphic to V. Thus $L\otimes_K U^\sigma$ is an irreducible LG-module for each $\sigma\in\mathrm{Gal}(K/F)$ and if $\tau\neq\sigma$ then $L\otimes_K U^\sigma$ is not LG-isomorphic to $L\otimes_K U^\tau$ by 3.3. So V_L is the sum of $|K\colon F|$ nonisomorphic irreducibles. On the other hand if a and b are distinct members of A with W^a KG-isomorphic to W^b then $L\otimes_k W^a$ is LG-isomorphic to $L\otimes_k W^b$ so some irreducible occurs in V_L with multiplicity greater than 1, a contradiction.

(3.6) *Let K be a finite extension of F, $\langle\sigma\rangle=\mathrm{Gal}(K/F)$, and $\alpha\colon G\to GL(V)$ an irreducible KG-representation. Then the following are equivalent:*

(1) *α can be written over F.*

(2) *$V=K\otimes_F U$ for some irreducible FG-submodule U of V.*

(3) *V is KG-isomorphic to V^σ.*

Proof. The equivalence of (1) and (2) is trivial, as is the implication (1) implies (3). Assume V^σ is KG-isomorphic to V. Let U be an irreducible FG-submodule of V. By 3.4, V is a composition factor of $U_K=K\otimes_F U$. So by 3.5.1, $U_K=\bigoplus_{a\in A} V^a$ for some $A\subseteq\mathrm{Gal}(K/F)$. But as $\langle\sigma\rangle=\mathrm{Gal}(K/F)$ and V is isomorphic to V^σ, every composition factor of U_K is isomorphic to V. Hence by 3.5.3, $U_K=V$, so (1) holds.

(3.7) *Let K be a finite extension of F, V an irreducible KG-module, U an irreducible FG-submodule of V, and $E=N_K(U)$. Then $V=K\otimes_E U$.*

Proof. Let $U_K=K\otimes_E U$ and $\Gamma=\mathrm{Gal}(K/E)$. By 3.4 and 3.5, $U_K=\bigoplus_{a\in A} V^a$ for a set A of cost representatives of $\Delta=N_\Gamma(V)$ in Γ. Let L be the fixed field of Δ and W and LG-submodule of V; as V is a homogeneous EG-module we may assume

$U \leqq W$. If $L \neq K$ then by induction on $|K:E|$, $L \otimes_E U \cong W$, while by 3.6, $V \cong K \otimes_L W$, so $V \cong K \otimes_E U$. Thus we may take $L = K$. But then $\Delta = 1$ so $\dim_E(U) = \dim_K(U_K) = |K:E| \dim_K(V) = \dim_E(V)$, so $U = V$. Hence $K = N_K(U) = E$, and the lemma holds.

(3.8) *Let K be a finite extension of F and α: $G \to GL(V)$ an irreducible KG-representation.*

Then

(1) *If $|K:F|$ is prime and α cannot be written over F then V is an irreducible FG-module.*

(2) *If α can be written over no proper subfield of K then V is an irreducible FG-module.*

Proof. This follows from 3.6 and 3.7.

(3.9) *Let k be a finite extension of F and V an irreducible kG-module which can be written over F. Then $V = k \otimes_F U$ for some irreducible FG-submodule U of V, and taking $K = \mathrm{Hom}_{FG}(U, U)$ and k to lie in a common extension of F, we have $K \cap k = F$ and $|K:F|$ and $|k:F|$ are relatively prime.*

Proof. The first remark follows from 3.6. To prove the remaining remarks we may replace k by $k \cap K$ to assume $k \leqq K$. Then by 3.5, V is the sum of $|k:F|$ irreducible kG-modules, so as V is an irreducible kG-module, $k = F$ as desired.

(3.10) *Let K be a finite extension of F and V an absolutely irreducible KG-module which can be written over F. Then $V = K \otimes_F U$ for some absolutely irreducible FG-submodule U of V.*

Proof. By 3.6, $V = K \otimes_F U$ for some irreducible FG-submodule U of V. So by 5.11.9 in [4], $1 = \dim_K(\mathrm{Hom}_{KG}(V, V)) = \dim_F(\mathrm{Hom}_{FG}(U, U))$. Thus $F = \mathrm{Hom}_{FG}(U, U)$, so U is absolutely irreducible.

(3.11) *Let V be a finite dimensional vector space over F, $G \leqq GL(V)$, and assume $V = \bigoplus_{i=1}^{m} V_i$, $V_i \in \mathrm{Irr}(G, V)$, is a homogeneous FG-module. Let $K = \mathrm{Hom}_{FG}(V_1, V_1)$, $A = \mathrm{Hom}_{FG}(V_1, V)$, $M = C_{GL(V)}(G)$, and $\mathscr{F}$ the set of families $\boldsymbol{\alpha} = (\alpha_i\colon 1 \leqq i \leqq m)$ with $\alpha_i \in \mathrm{Hom}_{FG}(V_1, V_i)^{\#}$ and $\alpha_1 = 1$. Then there exists $\boldsymbol{\alpha} \in \mathscr{F}$ and for each such $\boldsymbol{\alpha}$ we have:*

(1) *$\boldsymbol{\alpha}$ is a K-basis for A and $\boldsymbol{\alpha}$ induces a unique K-space structure on V extending the F-structure such that $\alpha_i \in \mathrm{Hom}_{KG}(V_1, V_i)$.*

(2) *The map π: $M \to GL(A, K)$ is an isomorphism, where for $x \in M$ and $\beta \in A$, $x\pi$: $\beta \to \beta x$.*

(3) *The map ψ: $A^{\#} \to \mathrm{Irr}(G, V, F)$ defined by ψ: $\beta \to V_1 \beta$ is a surjection and defines a bijection*

$$\varphi\colon S(A) \to S_G(V)$$
$$B \to \langle b\psi : b \in B \rangle$$

between the set $S(A)$ of all K-subspaces of A and the set $S_G(V)$ of all FG-submodules of V. φ defines a permutation equivalence of the actions of M on $S(A)$ and $S_G(V)$.

(4) $K=\mathrm{Hom}_{FGM}(V,V)$ and the K-representation of $M\times G$ *on* V *defined by* $(x,g)\colon v\to vxg$ *is equivalent to the tensor product of the representations of* M *on* A *and* G *on* V *over* K.

Proof. As V is a homogeneous FG-module there is $\bar{\boldsymbol{\alpha}}\in\mathscr{F}$. $V=\bigoplus_{i=1}^{m} V_i$, so

$$\mathrm{Hom}_{FG}(V_1,V)=\bigoplus_{i=1}^{m}\mathrm{Hom}_{FG}(V_1,V_i)\cong K^m.$$

Hence as $\boldsymbol{\alpha}$ is a K-linearly independent subset of A of order m, (1) holds. Evidently $\beta x\in A$ for $\beta\in A$ and $x\in M$ and π is a KM-representation. If $\alpha_i x=\alpha_i$ then $V_i\leqq C_V(x)$. Thus π is faithful. Let $(v_j\colon 1\leqq j\leqq d)$ be a K-basis for V_1. Then $B=(v_j\alpha_i\colon 1\leqq i\leqq m, 1\leqq j\leqq d)$ is a K-basis for V. An element of $GL(A,K)$ may be regarded as an m by m matrix (a_{ij}) over K with respect to the basis $\boldsymbol{\alpha}$ of A. Given such an element, define $x\in GL(V,K)$ by $v_j\alpha_i x=\sum_k v_j a_{ik}\alpha_k$. Then $x\in M$ with $x\pi=(a_{ij})$ so that π is an isomorphism and (2) holds.

Evidently ψ maps A into $\mathrm{Irr}(G,V,F)$ and the induced map φ takes $S(A)$ into $S_G(V)$ and preserves inclusion. It is also clear that φ is an injective map of the set $S_1(A)$ of 1-dimensional subspaces of A into $\mathrm{Irr}(G,V,F)$. Let $W\in\mathrm{Irr}(G,V,F)$ and $\pi_i\colon W\to V_i$ the ith projection. π_i is trivial or an isomorphism, and there exists an isomorphism $\beta\colon V_1\to W$. Then $a_i=\beta\pi_i\alpha_i^{-1}\in K$ and $a=\sum a_i\alpha_i\in A$ with $a\psi=V_1 a=W$, so $\varphi\colon S_1(A)\to\mathrm{Irr}(G,V,F)$ is a bijection. As $(I+J)\varphi=I\varphi+J\varphi$ and $\dim_F(I\varphi)=|K:F|\dim_K(I)$ for each $I,J\in S(A)$, it follows that $\varphi\colon S(A)\to S_G(V)$ is a bijection. So (3) holds.

The map $v_j\alpha_i\to v_j\otimes\alpha_i$ induces an equivalence of the K-representation $(x,g)\colon v\to vxg$ of $M\times G$ on V with the tensor product representation

$$(x,g)\colon\ \alpha_i\otimes v_j\to\alpha_i x\otimes v_j g$$

of $M\times G$ on $A\otimes V_1$. So (4) holds.

Given a family $\mathscr{B}=(V_i\colon 1\leqq i\leqq m)$ of F-spaces let $\Gamma(\mathscr{B})$ be the subgroup of the direct product $\prod_{I\in\mathscr{B}}\Gamma(I)$ consisting of these elements $\boldsymbol{x}=(x_I\colon I\in\mathscr{B})$ such that $\sigma(x_I)$ is independant of the choice of I in B. (Recall $\sigma(x_I)$ is the field automorphism associated to the semilinear map x_I.) For $\boldsymbol{x}$ in $\Gamma(B)$ define the map $\boldsymbol{x}\pi$ on the tensor product $\bigotimes_{I\in\mathscr{B}} I$ by

$$\boldsymbol{x}\pi\colon\ \sum_i v_{i1}\otimes\ldots\otimes v_{im}\to\sum_i v_{i1}x_1\otimes\ldots\otimes v_{im}x_m.$$

If further $\mathscr{F}=(\alpha_i\colon V_1\to V_i\colon 1\leqq i\leqq m)$ is a family of isomorphisms and S is the symmetric group on $\{1,2,\ldots,m\}$, for $s\in S$ define the map $s\pi$ on $\bigotimes_{i\in\mathscr{B}} I$ by

$$s\pi\colon\ \sum_i v_{i1}\alpha_1\otimes\ldots\otimes v_{im}\alpha_m\to\sum_i(v_{i,1s^{-1}})\alpha_1\otimes\ldots\otimes(v_{i,ms^{-1}})\alpha_m.$$

The map α_i induces an isomorphism of $\Gamma(V_1)$ with $\Gamma(V_i)$ which in turn induce embeddings of S and $\Gamma(\mathscr{B})$ in the wreath product of S_m with $\Gamma(V_1)$. Denote by

$\Lambda(\mathscr{B},\mathscr{F})$ the subgroup generated by S and $\Gamma(\mathscr{B})$ subject to these embeddings. Observe that $\Lambda(\mathscr{B},\mathscr{F})$ is the semidirect product of S and $\Gamma(\mathscr{B})$. Moreover the proof of the following lemma is straightforward:

(3.12) *Let $\mathscr{B}=(V_i\colon 1\leqq i\leqq m)$ be a family of F-spaces. Then*

(1) *The map $\pi\colon \Gamma(\mathscr{B})\to\Gamma(\bigotimes_{I\in\mathscr{B}} I)$ defined above is a representation with $\sigma(\boldsymbol{x}\pi)=\sigma(x_I)$ for each $\boldsymbol{x}\in\Gamma(\mathscr{B})$.*

(2) *If $\mathscr{F}=(\alpha_i\colon V_1\to V_i\colon 1\leqq i\leqq m)$ is a family of isomorphisms with $\alpha_1=1$ then the map $\pi\colon \Lambda(\mathscr{B},\mathscr{F})\to\Gamma(\bigotimes_{I\in\mathscr{B}} I)$ defined above is a representation with $S\pi\leqq GL(\bigotimes_{I\in\mathscr{B}} I)$.*

(3) *$\Lambda(\mathscr{B},\mathscr{F})\pi$ is the semidirect product of a central product D of the groups $GL(I)$, $I\in\mathscr{B}$, with $A\times S\pi$ where $A\cong \mathrm{Aut}(F)$ induces field automorphisms on each $GL(I)$, $S\pi$ is the symmetric group on $\mathscr{B}$, and $S\pi D$ is a homomorphic image of the wreath product of S with $GL(I)$.*

(3.13) *Assume the hypothesis of* 3.11 *with $m>1$ and let $L=\Gamma(V)_{\mathrm{Irr}(G,V)}$. Then*

(1) *$L\cong GL(V_1,K)$ and $L=C_{\Gamma(V)}(M)$.*

(2) *The representation of $L\times M$ on V is a K-equivalent to the tensor product representation on $V_1\otimes_K A$.*

(3) *$\Gamma(\{V_1,A\})\pi=N_{\Gamma(V)}(ML)\cap N(L)$, where π is the representation of* 3.12.

(4) *Either $L\trianglelefteq N_{\Gamma(V)}(ML)$ or* $\dim(V_1)=\dim(A)$ *and $|N_{\Gamma(V)}(ML){:}N_{\Gamma(V)}(L)|=2$.*

Proof. Observe that V is a homogeneous FM-module with $K=\mathrm{Hom}_{FM}(I,I)$ for $I\in\mathrm{Irr}(M,V)$. Thus $L_0=C_{GL(V)}(M)\cong GL(V_1,K)$, V is the sum of m-equivalent natural modules for L_0, and $|\mathrm{Irr}(L_0,V)|=|\mathrm{Irr}(G,V)|$ by 3.11. $G\leqq L_0$ so $G\leqq\Gamma(V)_{\mathrm{Irr}(L_0,V)}$, and then $\mathrm{Irr}(G,V)=\mathrm{Irr}(L_0,V)$. So without loss, $G=L_0$. Similarly $G\leqq L$ so $\mathrm{Irr}(G,V)=\mathrm{Irr}(L,V)$ and so letting $L_1=L\cap GL(V)$, we conclude from 3.11.3 and the hypothesis that $m>1$, that V is a homogeneous. FL_1-module and $K=\mathrm{Hom}_{FL_1}(V,V)$. Hence $C_{GL(V)}(L_1)\cong M$ by 3.11, so as $C_{GL(V)}(L_1)\leqq M$ we have equality. Then $L_1\leqq C_{GL(V)}(M)=G$, so $G=L_1$. Let E be the prime field. Then $\mathrm{Irr}(G,V,E)=\mathrm{Irr}(G,V,F)$ as V_1 is the natural module for $G\cong GL(V_1,K)$. Also $L\leqq\Gamma(V,E)_{\mathrm{Irr}(G,V,E)}$ while $\Gamma(V,E)=GL(V,E)$ and we have just shown $GL(V,E)_{\mathrm{Irr}(G,V,E)}=G$. Hence $G=L$. Also we showed $L=C_{GL(V)}(M)$, and $F\leqq M$ so $C_{\Gamma(V)}(M)=C_{GL(V)}(M)$. Thus (1) holds.

Notice 3.11.4 implies (2). Let $H=N_{\Gamma(V)}(ML)$. By 3.12, $\Gamma(\{V_1,A\})\pi=MLX$, where X induces a group of field automorphisms on $GL(V)$, $MLX/L\cong\Gamma(A,K)$ and $MLX\leqq N_H(L)$. Let $R=\mathrm{Irr}(G,V)$. Then $M\trianglelefteq N_H(L)$, do by 3.11, $N_H(L)^R=P\Gamma(A,K)$ in its representation on projective space. Thus $N_H(L)^R=MX^R$, so as $L=N_H(L)_R$, $N_H(L)=MXL$. That is (3) holds.

If $\dim(V_1)\neq\dim(A)$ then clearly $L\trianglelefteq H$, while if $\dim(V_1)=\dim(A)$ there is a K-isomorphism $\beta\colon V_1\to A$ inducing an isomorphism $\beta^*\colon L\to M$, and $t\in GL(V)$ defined by $(v\otimes a)t=a\beta^{-1}\otimes v\beta$. Then $((x,y)\pi)^t=(y(\beta^*)^{-1},x\beta^*)\pi\in LM$, so $t\in H-N(L)$. Thus (4) holds.

(3.14) *Let K be a finite extension of F and V a finite dimensional vectorspace over F which also admits a K-space structure extending the F-structure. Then $N_{\Gamma(V,F)}(K)=\Gamma(V,K)$.*

Proof. If $\dim_K(V)>1$ this is a consequence of 3.13.3 with $K=G$. If $\dim_K(V)=1$, the result is well known; see for example Proposition 19.8 in [5].

(3.15) *Let V be an absolutely irreducible FG-module defined over a subfield K of F. Then*

(1) *$V=F\otimes_K U$ for some absolutely irreducible KG-submodule U of V.*

(2) *Let $H=N_{\Gamma(V,F)}(U)$. Then H is $GL(U,K)$ extended by a generator of* $\mathrm{Aut}(F)$ *inducing a field automorphism.*

(3) *$N_{\Gamma(V,F)}(G)\leqq HF$.*

Proof. Part (1) is a restatement of 3.10. Let H_0 be the split extension of $GL(U,K)=H_1$ by a generator x of $\mathrm{Aut}(F)$ inducing a field automorphism on H_1 and represent H_0 naturally on U. Tensoring the representation of H_1 with F, we obtain an FH_1-representation on V. Similarly defining x on V by $(\sum a_i\otimes u_i)x=\sum a_i^x\otimes u_i x$ for $a_i\in F$, $u_i\in U$ we embedd H_0 in $\Gamma(V,K)$ with $\sigma(x)=x$. Moreover $H_0\leqq H$. Conversely $GL(V,F)\cap H\leqq GL(U,K)=H_1$, so $H_1=GL(V,F)\cap H$. Then as $|H:H_1|\leqq|\Gamma(V,F):GL(V,F)|=|H_0:H_1|$, $H=H_0$. So (2) holds. Let $L=\Gamma(V,F)_{\mathrm{Irr}(G,V,K)}$. By (2), $L\leqq H$. We may assume $K\neq F$, so by 3.13, $H_1=FH\cap L$. Thus $L=H_1$. As $x\in H$ it remains to show $N_{GL(V,F)}(G)\leqq H_1F$. By 3.13.3, $N_{GL(V,F)}(G)\leqq LC_M(F)$, where $M=C_{GL(V,K)}(L)$, while by 3.14, $F=C_M(F)$. So (3) holds.

(3.16) *Let G be the central product of groups G_i, $1\leqq i\leqq m$, V an irreducible FG-module, and $V_i\in\mathrm{Irr}(G_i,V)$. Then*

(1) $\mathrm{Hom}_{FG}(V,V)$ *contains* $\mathrm{Hom}_{FG_i}(V_i,V_i)$.

(2) *If V is an absolutely irreducible FG-module then V_i is an absolutely irreducible FG_i-module and V is FG-isomorphic to $V_1\otimes\ldots\otimes V_m$.*

Proof. We prove (1) by induction on m. In particular we may take $m=2$. Then by 3.11.4, $\mathrm{Hom}_{FG_i}(V_i,V_i)\leqq\mathrm{Hom}_{FG}(V,V)$, completing the proof of (1).

Notice (1) implies the first remark in (2), which together with 3.11.4 implies the second remark in (2).

(3.17) *Let G be the product of components L_i, $1\leqq i\leqq m$, V an absolutely irreducible FG-module, $V_i\in\mathrm{Irr}(L_i,V)$ with $\dim(V_i)=d$ independent of i, $X_i=\Gamma(V)_{\mathrm{Irr}(L_i,V)}$, and $Y=\langle X_i\colon 1\leqq i\leqq m\rangle$. Then*

(1) *V is isomorphic $V_1\otimes\ldots\otimes V_m$ as an FG-module.*

(2) *$X_i\cong GL(V_i)$ acts naturally on V_i and Y is the central product of the groups X_i, $1\leqq i\leqq m$.*

(3) *$N_{\Gamma(V)}(G)\leqq N_{\Gamma(V)}(Y)$.*

(4) *Let $\mathscr{B}=(V_i\colon 1\leqq i\leqq m)$ and $\mathscr{F}=(\alpha_i\colon 1\leqq i\leqq m)$, where $\alpha_i\colon V_1\to V_i$ is an isomorphism and $\alpha_1=1$. Then $N_{\Gamma(V)}(E(Y))=\Lambda(\mathscr{B},\mathscr{F})\pi$, where π is the map of* 3.12.

Proof. Notice 3.16 implies (1). By 3.13, $X_i\cong GL(V_i)$ acts naturally on V_i. Let $D=X_1\times\ldots\times X_m$. We may take $D\trianglelefteq\Lambda(\mathscr{B},\mathscr{F})=\Lambda$ and by (1) and the last remark we may take $X_i\pi=X_i$ for each i. Hence by 3.12.3, Y is the central product of the groups X_i, $1\leqq i\leqq m$, so (2) holds. By construction, (3) holds. Of course $Y\trianglelefteq\Lambda\pi$, so it remains to show $N_\Gamma(E(Y))\leqq\Lambda\pi$. Adopt the notation of 3.12; then $S\pi$ induces S_m on the components of Y, so it suffices to show $B\leqq\Lambda\pi$ where B is the intersection of the groups $N_\Gamma(X)$, as X ranges over the set R of components of Y. As $|A|=|\Gamma: GL(V)|$ and $A\cap GL(V)=1$, this reduces to showing $B\cap GL(V) = Y$. $F=C_{GL(V)}(E(Y))$ as $E(Y)$ is absolutely irreducible on V, so it suffices to show $\mathrm{Aut}_{(B\cap GL(V))}(E(Y))=\mathrm{Aut}_Y(E(Y))$. But setting

$$T=\bigcap_{X\in R} N_{\mathrm{Aut}(E(Y))}(X)$$

we have T is the direct product of the groups $\mathrm{Aut}(X)$, $X\in R$, and $|\mathrm{Aut}(X): \mathrm{Aut}_Y(X)|=2$. Further if $t\in T-\mathrm{Aut}_Y(E(Y))$, then $\bigotimes_{i\in\mathscr{B}} I^t$ is not $FE(Y)$-isomorphic to V, so 2.5 completes the proof.

Section 4. Bilinear forms

In this section F is a field and U and V are finite dimensional vector spaces over F. Denote by $L(V,U)$ the set of all bilinear maps from $V\times U$ into F. $L(V,U)$ is an F-space under

$$(af)(v,u)=af(v,u) \qquad a\in F,\ v\in V,\ u\in U,$$
$$(f+g)(v,u)=f(v,u)+g(v,u) \qquad f,\ g\in L(V,U).$$

Of course this space is isomorphic to the dual space $(V\otimes U)^*$ of the tensor product space $V\otimes U$, so:

(4.1) $\dim_F(L(V,U))=\dim_F(V)\dim_F(U)$.

Define φ: $L(V,U)\to \mathrm{Hom}_F(V,U^*)$ by $u(v(f\varphi))=f(v,u)$ for $f\in L(V,U)$, $v\in V$, and $u\in U$. Then φ is an injective linear transformation, so we conclude from 4.1 and from $\dim_F(\mathrm{Hom}_F(V,U^*)=\dim_F(V)\dim_F(U)$ that:

(4.2) *φ is an F-isomorphism.*

Assume next that G is a group and α and β are FG-representations with modules V and U, respectively. Recall that dual representation β^* of G on U^* is defined by

$$x(g\beta^*): U\to F \qquad g\in G,\ x\in U^*,$$
$$u\to(ug^{-1})x \qquad u\in U.$$

We also have a representation of $G\times G$ on $L(V,U)$ defined by

$$(g,h)(f)(v,u)=f(v(g\alpha),\ u(h\beta)) \qquad g,h\in G,\ f\in L(V,U),\ v\in V,\ u\in U$$

and the *diagonal representation* of G on $L(V,U)$ defined by

$$g: f\to(g,g)(f) \qquad g\in G,\ f\in L(V,U).$$

Usually we suppress the representations α and β and write vg and ug for $v(g\alpha)$ and $u(g\beta)$.

Observe that $f\varphi\in\mathrm{Hom}_{FG}(V,U^*)$ if and only if $g(f\varphi)=(f\varphi)g$ for all $g\in G$. But $u((vg)(f\varphi))=f(vg,u)$ while $u((v(f\varphi))g)=(ug^{-1})(v(f\varphi))=f(v,ug^{-1})$. Hence

$f\varphi \in \mathrm{Hom}_{FG}(V, U^*)$ if and only if $f(vg,u) = f(v,ug^{-1})$, or equivalently $f(vg,ug) = f(v,u)$, for all $v \in V$, $u \in U$, and $g \in G$. We have shown:

(4.3) *Let $f \in L(V,U)$. Then the following are equivalent:*

(1) $f\varphi \in \mathrm{Hom}_{FG}(V, U^*)$.

(2) $f(vg,ug) = f(v,u)$ *for all* $v \in V$, $u \in U$, *and* $g \in G$.

(3) f *is a fixed point for* G *in the diagonal action.*

In the event one of the equivalent conditions of 4.3 holds, we say G *preserves* f, and write $L_G(V,U)$ for the subspace of bilinear maps preserved by G. By 4.2 and 4.3:

(4.4) φ *induces an F-isomorphism of $L_G(V,U)$ with* $\mathrm{Hom}_{FG}(V, U^*)$.

(4.5) *Assume G acts irreducibly on V and U and let $K = \mathrm{Hom}_{FG}(V,V)$. Then $L_G(V,U) \neq 0$ if and only if V is isomorphic to U^* as an FG-module, in which case K acts regularly on $L_G(V,U)$ via $\gamma(f)(v,u) = f(v\gamma,u)$ for $\gamma \in K$, $f \in L_G(V,U)$, $v \in V$, and $u \in U$.*

Proof. The first remark is a consequence of 4.4 and Schur's lemma. Assume $f \in L_G(V,U)^{\#}$. Then

$$\mathrm{Hom}_{FG}(V, U^*) = \{\gamma(f\varphi) \colon \gamma \in K\}.$$

Also $u(v(\gamma(f\varphi))) = u((v\gamma)(f\varphi)) = f(v\gamma,u)$, so $\gamma(f\varphi) = \gamma(f)\varphi$. Hence K is regular on $L_G(V,U)$.

We are primarily concerned with the case where $U = V$ and the case where F admits an automorphism θ of order 2 and $U = V^\theta$ as an FG-module. Recall in the latter case that U is equal to V as an F-space, while there is a basis $X = (x_i \colon 1 \leqq i \leqq n)$ of V such that if $A(g) = (a_{ij})$ is the matrix of $g \in G$ with respect to X on V, then $A(g)^\theta = (a_{ij}^\theta)$ is the matrix of g on U with respect to X. The following remarks are easily checked:

(4.6) *Let θ be an involutory automorphism of V. Then*

(1) *The map $\psi \colon \sum a_i x_i \to \sum a_i^\theta x_i$ is a bijective semilinear transformation of V with V^θ which commutes with the actions of G.*

(2) *ψ induces a bijection between $L(V, V^\theta)$ and the set $L^\theta(V,V)$ of sesquilinear forms on V determined by θ, via $(f\psi)(v,u) = f(v,u\psi)$.*

(3) *ψ restricts to a bijection of $L_G(V,V^\theta)$ with the set $L_G^\theta(V,V)$ of sesquilinear forms on V preserved by G.*

(4) *$f\psi$ is hermitian symmetric if and only if $f(x,y) = f(y,x)^\theta$ for all $x, y \in X$.*

(4.7) *Let θ be an automorphism of F of order at most 2, assume G acts irreducibly on V, and let $K = \mathrm{Hom}_{FG}(V,V)$. Then $L_G^\theta(V,V) \neq 0$ if and only if V is isomorphic to $V^{*\theta}$ as an FG-module, in which case K acts regularly on $L_G^\theta(V,V)$ via $\gamma(f)(v,u) = f(v\gamma,u) = f(v\gamma,u)$ for $\gamma \in K$, $f \in L_G^\theta(V,V)$, and u, $v \in V$.*

Proof. This is a consequence of 4.5 and 4.6.

(4.8) *Let θ be an automorphism of F of order at most 2 and assume V is an absolutely irreducible FG-module and $L_G^\theta(V,V) \neq 0$. Then*

(1) *If* $\theta=1$ *then either* (V, f) *is a symplectic space for all* $f \in L_G(V, V)^{\#}$ *or* q *is odd and* (V, f) *is an orthogonal space for all* $f \in L_G(V, V)^{\#}$.

(2) *If* θ *is an involution then there exists a unitary form* $g \in L_G^\theta(V, V)$. *Moreover* $f \in L_G^\theta(V, V)^{\#}$ *is a unitary form if and only if* $f=\tau(g)$ *for some* $\tau \in K^{\#}$, *where* K *is the fixed field of* θ.

Proof. First observe that if θ is an involution then there is $b \in F$ with $b \neq b^\theta$. Let $a=b-b^\theta$; then $a^\theta=-a$.

Let $f \in L_G^\theta(V, V)^{\#}$. As $f \neq 0$ and G acts irreducibly on V, f is nondegenerate. Suppose $\theta=1$ and f is symmetric or skew symmetric. Then so is $\tau(f)$ for each $\tau \in F^{\#}$, so (1) holds. Similarly if θ is an involution and f is hermetian symmetric then for $\tau \in F^{\#}$ and $x, y \in V$, $(\tau f)(y, x)=\tau f(y, x)=\tau f(x, y)^\theta =\tau^{1-\theta}(\tau f)(x, y)^\theta$, so τf is unitary if and only if $\tau \in K^{\#}$, and hence (2) holds.

So we may assume f does not have the appropriate symmetry condition. Let $g(x, y)=f(x, y)-f(y, x)^\theta$. By our assumption on $f, g \neq 0$, so $g \in L_G^\theta(V, V)^{\#}$. But $g(y, x)=-g(x, y)^\theta$, so if $\theta=1$ then g is skew symmetric and we are done. If θ is an involution ag is hermitian where $a \in K^{\#}$ with $a^\theta=-a$, so again we are done.

(4.9) *Let* $\operatorname{char}(F)=2$ *and* f *a nondegenerate symplectic form on* V *preserved by* G. *Assume* V *is an irreducible* FG*-module. Then there exists at most one quadratic form* Q *on* V *preserved by* G *with* $f(x, y)=Q(x+y)+Q(x)+Q(y)$.

Proof. Suppose Q and P are two such forms. If $Q(x)=P(x)$ for some $x \in V^{\#}$, then we must have $P=Q$. For as G is irreducible on V, $V=\langle xG\rangle$, so there is a basis $Y \subseteq xG$ of V. For each $y \in Y$, there is $g \in G$ with $xg=y$, so $Q(xg)=Q(x) =P(x)=P(xg)=P(y)$. Thus $Q=P$, establishing the claim.

It remains to show Q and P agree on some member of $V^{\#}$. But as (V, f) is a symplectic space, $\dim(V)>1$, so for $x \in V^{\#}$ there is $y \in xG-\langle x\rangle$. Then $Q(x+y)=Q(x)+Q(y)+(x, y)=(x, y)$, as $Q(x)=Q(y)$. Similarly $P(x+y)=(x, y)$, and we are done.

In the next lemma we use the following terminology: Let π_i: $G_i \rightarrow \operatorname{Aut}(X_i)$, $i=1,2$, be representations. We say π_1 is *quasiequivalent* to π_2 if there exists an isomorphism α: $G_1 \rightarrow G_2$ such that π_1 is equivalent to $\alpha \pi_2$ as representations of G_1.

(4.10) *Assume* F *is finite and* π_i: $G_i \rightarrow GL(V_i)$, $i=1,2$, *are quasiequivalent representations in the category of* F*-spaces and semilinear transformations. Assume* $f_i \in L_{G_i}^\theta(V_i, V_i)^{\#}$ *with* π_i *an absolutely irreducible* FG*-representation. Then* (V_1, f_1) *is similar to* (V_2, f_2).

Proof. By hypothesis there exists an isomorphism α: $G_1 \rightarrow G_2$ such that $\alpha \pi_2$ is equivalent to π_1. Let β: $V_1 \rightarrow V_2$ be such an equivalence. Then β is an invertible semilinear transformation commuting with the actions of $G=G_1$. Let $\tau=\sigma(\beta)$, $f=f_1$, $V=V_1$, and define g: $V \times V \rightarrow F$ by $g(u, v)=f_2(u\beta, v\beta)^{\tau^{-1}}$. A straightforward calculation shows $g \in L_G^\theta(V, V)^{\#}$, so by 4.7, $g=\tau f$ for some $\tau \in F^{\#}$. It is now easy to show (V_1, f_1) is similar to (V_2, f_2).

Section 5. Nondegenerate spaces

In this section F is a finite field of characteristic p and either (V, f) is a unitary or symplectic space over F or (V, Q) is an orthogonal space over F with associated bilinear form f. G is a subgroup of $\Gamma(V, f)$, or $\Gamma(V, Q)$, respectively.

(5.1) *Let $I \in \operatorname{Irr}(G, V)$. Then one of the following holds:*

(1) *I is nondegenerate.*

(2) *I is totally singular.*

(3) *(V, Q) is orthogonal, $p=2$, and I is of dimension* 1.

Proof. As G is irreducible on I, either $I \cap I^{\perp}=0$ or $I \leqq I^{\perp}$. In the first case (1) holds, and in the second case (2) holds unless (V, Q) is orthogonal and $p=2$, in which case I has a unique totally singular subspace of codimension 1. But then as G is irreducible on V, (3) holds.

(5.2) *Assume V is a homogeneous FG-module and G is not a group of scalars. Then $V=U \perp W$, where U and W are FG-submodules of V such that:*

(1) $U=\perp_i U_i$, $U_i \in \operatorname{Irr}(G, V)$, *and U_i is nondegenerate.*

(2) $W=\perp_i W_i$, $W_i=W_{i1} \oplus W_{i2}$ *is nondegenerate, and* $W_{ij} \in \operatorname{Irr}(G, V)$. *Every member of* $\operatorname{Irr}(G, W)$ *is totally singular.*

Proof. The proof is by induction on the dimension of V. Let $I \in \operatorname{Irr}(G, V)$. As G is not a group of scalars, $\dim(I)>1$, so by 5.1 either I is nondegenerate or I is totally singular. In the first case $V=I \oplus I^{\perp}$ and as $\dim(I^{\perp})<\dim(V)$, we are done by induction. Thus we may assume each member of $\operatorname{Irr}(G, V)$ is totally singular. Let $J \in \operatorname{Irr}(G, V)$ with $J \nleqq I^{\perp}$. Then $I \oplus J=W_1$ is nondegenerate, so an earlier argument completes the proof.

(5.3) *Assume the hypothesis and notation of* 5.2. *Then*

(1) *$I \in \operatorname{Irr}(G, V)$ is totally singular if and only if $I \leqq W$ or the projection of I on U is a totally singular member of* $\operatorname{Irr}(G, U)$.

(2) *Let S be the set of all nondegenerate FG-submodules M of V such that each member of* $\operatorname{Irr}(G, M)$ *is totally singular and let S^* be the set of maximal members of S under inclusion. Then* $W \leqq \bigcap_{M \in S^*} M$.

(3) *If $N_{\Gamma(V,f)}(G)$ (or $N_{\Gamma(V,Q)}(G)$) is irreducible on V, then $V=U$ or W.*

Proof. Let π and σ be the projection maps of V on U and W, respectively, and let $I \in \operatorname{Irr}(G, V)$. Then $I\sigma \in \operatorname{Irr}(G, W)$ or $I \leqq U$, and in either case $I\sigma$ is totally singular. So for $x, y \in I$, $(x, y)=(x\pi+x\sigma,\ y\pi+y\sigma)=(x\pi, y\pi)$. Hence (1) holds. Notice (1) implies (2) and (2) implies (3).

(5.4) *$O(V, f)$ (or $O(V, Q)$) is transitive on the set T of pairs (U, W) such that $V=U \oplus W$ and U and W are totally singular. T is nonempty if and only if $\dim(V)$ is even and in addition $\operatorname{sgn}(Q)=+1$ in case (V, Q) is orthogonal. If $(U, W) \in T$ then the stabilizer in $O(V, f)$ (or $O(V, Q)$) of $\{U, W\}$ is $H\langle t\rangle$, where $H \cong GL(U)$ acts naturally on U, W is FH-isomorphic to $U^{*\theta}$, with θ the automor-*

phism of F of order 2 if (V,f) is unitary and $\theta=1$ otherwise, $U^t=W$, t induces a graph or graph-field automorphism on H for $|\theta|=1$ or 2, respectively, and $t^2=\varepsilon 1_V$, with $\varepsilon=-1$ if (V,f) is symplectic and $\varepsilon=+1$ otherwise.

Proof. Let $G=O(V,f)$ or $O(V,Q)$ in the appropriate case. If $(U,W)\in T$ then $\dim(V)=2m$ is even and there is a basis $X=(x_i\colon 1\leqq i\leqq 2m)$ with $(x_{2i-1}\colon 1\leqq i\leqq m)$ and $(x_{2i}\colon 1\leqq i\leqq m)$ bases for U and W respectively, and with $(x_{2i-1},x_{2j})=\delta_{ij}$. As G is transitive on such bases, G is transitive on T.

Let H be the stabilizer in G of $(U,W)\in T$. Then $|N_G(\{U,W\})\colon H|=2$ and H contains the group $H_0=GL(U)$ acting naturally on U and with φ defining an FH_0-isomorphism of U with $W^{*\theta}$, where $\varphi\in \mathrm{Hom}_F(U,W)$ maps x_{2i-1} to x_{2i}, $1\leqq i\leqq m$. Conversely if $h\in H$ then φ defines an $F\langle h\rangle$-isomorphism of U with $W^{*\theta}$, so $H=H_0$. Finally let $t\in GL(V)$ with $x_{2i-1}t=x_{2i}$ and $x_{2i}t=\varepsilon x_{2i-1}$, where $\varepsilon=+1$ unless (V,f) is symplectic, where $\varepsilon=-1$. Then $t\in N_G(\{U,W\})-H$ induces a graph or graph field automorphism on H with $U^t=W$ and $t^2=\varepsilon 1_V$.

(5.5) *Let $L\trianglelefteq G$ with G irreducible on V. Assume $L\leqq GL(V)$ but L does not act as a group of scalars. Let $(V_i\colon 1\leqq i\leqq m)$, be the homogeneous components of L on V and assume $m>1$. Then one of the following holds:*

(1) $\perp_{1\leqq i\leqq m} V_i$ *with V_i isometric to V_j for each $1\leqq i\leqq j\leqq m$.*

(2) $V=U_1\perp U_2$ *with* $U_1=\perp_{1\leqq i\leqq m/2} V_i$, $U_2=\perp_{m/2<i\leqq m} V_i$, *$V_i$ is isometric to V_j for $1\leqq i\leqq j\leqq m/2$ and $m/2<i\leqq j\leqq m$, (V,Q) is orthogonal, p is odd, $\dim(V_1)$ is odd, and V_1 is similar but not isometric to V_m.*

(3) $V=\perp_{1\leqq i\leqq m/2} U_i$, $U_i=V_{2i-1}\oplus V_{2i}$, *$U_i$ is isometric to U_j for $1\leqq i\leqq j\leqq m/2$, and V_i is totally singular for each $1\leqq i\leqq m$.*

Proof. By Clifford's Theorem, $V=\bigoplus_{1\leqq i\leqq m} V_i$, and the set $S=(V_i\colon 1\leqq i\leqq m)$ is transitively permuted by G. Hence $\dim(V_i)=\dim(V_j)=r$ is constant, V_i is nondegenerate if and only if V_j is nondegenerate, and in case (V,Q) is orthogonal, r is even, and (V_i,Q) is nondegenerate of sign ε, then (V_j,Q) also has sign ε. As G is irreducible on V, $N_G(V_i)$ is irreducible on V_i, so by 5.1 either V_i is nondegenerate or totally singular or (V,Q) is orthogonal, q is even, and $r=1$. We conclude that either V_i is isometric to V_j for all $1\leqq i\leqq j\leqq m$, or (V,Q) is orthogonal, p is odd, r is odd, V_i is nondegenerate, and $S=S_1\cup S_2$ is partitioned into two equal parts with the members of S_i isometric and the members of S_1 similar but not isometric to those of S_2.

Now if V_1 is nondegenerate then $V=V_1\oplus V_1^\perp$ with $V_1^\perp$ FL-isomorphic to V/V_1, which is in turn FL-isomorphic to $\hat{V}_1=\langle V_i\colon i\neq 1\rangle$. Thus $\hat{V}_1=V_1^\perp$, and we see from the discussion above that (1) or (2) holds. So assume V is totally isotropic. The map $W\to W^\perp/V^\perp$ induces a bijection φ of the FL-submodules of V_1 and V/V_1 with φ reversing inclusion, so as V_1 is a homogeneous FL-module, so is $V/V_1^\perp$. Thus we may choose notation so that $V=V_1^\perp\oplus V_2$. Hence $U_1=V_1\oplus V_2$ is nondegenerate, and then as above (3) holds unless (V,Q) is orthogonal, $r=1$, $p=2$, and V_1 is not totally singular. In that case $C_L(V_1)=C_L(U_1)$

and $1 \neq L/C_L(V_1)$ is cyclic of order d dividing $|F^{\#}|$. As U_1 is a nondegenerate 2-space it follows that U_1 has sign $+1$ and the L-invariant points of U_1 are both totally singular, contrary to our assumption.

(5.6) *Let (V,f) be symplectic with $\dim(V)=4$ and $p=2$. Let U and W be totally singular subspaces of V with $V=U\oplus W$, and let $M=N_{\Gamma(V,f)}(\{U,W\})$. Then $M\leqq\Gamma(V,Q)$ for some quadratic form Q of sign $+1$ associated to f.*

Proof. By 5.4 there is $L_2(q)\cong L\trianglelefteq M$ with L acting naturally on U. Let $G=O(V,f)$. Then $E_q\cong O_2(N_G(W))\cap C(L)=P(W)$ and $U^{P(W)}$ is of order $q=|F|$. Hence L acts homogeneously on V and as U is an absolutely irreducible FL-module, $q+1=|\mathrm{Irr}(L,V)|$ by 3.11. So $P(W)$ is regular on $\mathrm{Irr}(L,V)-\{W\}$ and by symmetry $P(U)$ is regular on $\mathrm{Irr}(L,V)-\{U\}$, so by 3.11, $L'=\langle P(U),P(W)\rangle\cong L_2(q)$ and $X=LL'$ acts naturally as $\Omega_4^+(q)$ on V with $L'=O^{2'}(C_{GL(V)}(L))$ being M-invariant. In particular $M\leqq N_\Gamma(X)$ and X preserves a quadratic form Q on V of sign $+1$ associated to f. By 4.9, Q is uniquely determined. But if $g\in N_{O(V,f)}(X)$ then gQ is such a form, so $gQ=Q$ and hence $g\in O(V,Q)$. Then as $|\Gamma(V,f):\Delta(V,f)|=|\Gamma(V,Q):\Delta(V,Q)|=\mathrm{Aut}(F)$ and $|\Delta(V,f):O(V,f)|=|\Delta(V,Q):O(V,Q)|$ (Eg. 6.3 and 6.5) we conclude $N_\Gamma(X)=\Gamma(V,Q)$, completing the proof.

(5.7) *Assume U is a finite dimensional vector space over F and f is an F-form on U of one of the types* I–IV *of Sect.* 1, *with Q the quadratic form in case* III. *Let $\Gamma=\Gamma(U,f)$, except in case* III *where $\Gamma=\Gamma(U,Q)$, and similarly let $O=O(U,f)$ or $O(U,Q)$ in the respective case. Assume $G\leqq 0$ acts homogeneously on U but not by scalar multiplication and $N_\Gamma(G)$ is irreducible on U. Let $K^{\#}=Z(C_{GL(U)}(G))$. Then K is a finite extension of F, $N_\Gamma(G)\leqq N_\Gamma(K)$, and if $C_O(K)$ acts homogeneously on U then $C_O(K)$ is irreducible on U.*

Proof. Let $I\in\mathrm{Irr}(G,U)$, $n=\dim_F(U)$, and $d=\dim_F(I)$. By 3.11, $C_{GL(U)}(G)\cong GL_{n/d}(K_0)$, where $K_0=\mathrm{Hom}_{FG}(I,I)$. Thus $K=K_0$, and $N_\Gamma(G)\leqq N_\Gamma(K)$. We may assume $C_0(K)$ is homogeneous on U and it remains to prove $C_0(K)$ is irreducible. So without loss $G=C_0(K)$. If f is trivial then $G=GL(U,K)$ is certainly irreducible, so we may assume one of the cases II–IV holds. Then by 5.3.3, U satisfies one of 5.2.1 or 5.2.2.

Suppose 5.2.1 holds and let $I=U_1$. Then $V=I\oplus I^\perp$ and K centralizes the projection P of G on $O(I)$ with P irreducible on I. Then $P\leqq C_0(K)=G$, while every P-invariant submodule of U contains I or is contained in $I^\perp$. Thus from the homogeneous action of G and 3.11, $I=V$, so the lemma holds in this case.

So assume 5.2.2 holds and let $I=W_{1,1}$, $J=W_{1,2}$, and $A=I\oplus J$. By 5.4 the stabilizer in $O(A)$ of I and J is $M\cong GL(I)$ acting naturally on I with J FM-isomorphic to $I^{*\theta}$. Then $P=C_M(K)\cong GL_m(K)$, where $m=d/|K:F|$, with I the natural module for P and J FP-isomorphic to $I^{*\theta}$. We may assume $K\neq F$, so $|K|>3$ and in case IV even $|K|>4$. Thus I is not FP-isomorphic to $I^{*\theta}$, so $\mathrm{Irr}(P,A,F)=\{I,J\}$. Hence every P-invariant submodule of U contains I or J or is contained in $A^\perp$, so again as $P\leqq G$, the homogeneous action of G supplies a contradiction.

Section 6. Stabilizers of forms

In this section F is a finite field of characteristic p and (V,f) is a unitary or symplectic space over F, or (V,Q) is an orthogonal space over F with associated bilinear form f.

(6.1) *Let $X=(x_i\colon 1\leqq i\leqq n)$ be a basis for V and $\alpha\colon X\to V$ with $X\alpha$ a basis for V. Then α extends to a member of $\Gamma(V,f)$ (or $\Gamma(V,Q)$) if and only if*

(*) *There exists $a\in F^{\#}$ and $\tau\in\mathrm{Aut}(F)$ with $f(x\alpha,y\alpha)=af(x,y)^{\tau}$ and also $Q(x\alpha)=aQ(x)^{\tau}$ if (V,Q) is orthogonal and $p=2$.*

Moreover if α extends then its extension β is unique, $\tau(\beta)=a$, $\sigma(\beta)=\tau$, and $(\sum a_i x_i)\beta=\sum a_i^{\tau} x_i\alpha$.

Proof. This is a straightforward calculation.

(6.2) *Let (V,f) be unitary, K the subfield of F of index 2, and $q=|K|$. Then*

(1) *$f(x,x)\in K$ for each $x\in V$.*

(2) *$\tau(g)\in K$ for each $g\in\Gamma(V,f)$.*

(3) *$\Delta(V,f)=O(V,f)*\langle aI\rangle$ and $\langle aI\rangle\cap O(V,f)=\langle bI\rangle$, where a is a generator for $F^{\#}$ and $b\in F^{\#}$ is of order $q+1$.*

(4) *$\Gamma(V,f)$ is the split extension of $\Delta(V,f)$ by $A=\langle h\rangle$, where $\sigma(h)$ is a generator of $\mathrm{Aut}(F)$, $\tau(h)=1$, and h fixes some unitary basis pointwise.*

Proof. Recall the automorphism θ of F is the q-power map. So as $f(x,x)=f(x,x)^{\theta}$ for $x\in V$, (1) holds. Similarly for $g\in\Gamma(V,f)$,

$$\tau(g)f(x,x)^{\sigma(g)}=f(xg,xg)=f(xg,xg)^{\theta}=(\tau(g)f(x,x)^{\sigma(g)})^{\theta}=\tau(g)^{\theta}f(x,x)^{\sigma(g)},$$

so $\tau(g)=\tau(g)^{\theta}$ and (2) holds.

Let a be a generator of $F^{\#}$ and $\alpha=aI$. Then $f(x\alpha,y\alpha)=a^{q+1}f(x,y)$, so $\alpha\in\Delta(V,f)$ with $\tau(\alpha)=a^{q+1}$ generating $K^{\#}$. Hence by (2), if $\beta\in\Delta(V,f)$ then $\tau(\beta)=\tau(\alpha^i)$ for some i, so $\beta\in\alpha^i O(V,f)$ and the first part of (3) holds. $\alpha^i\in O(V,f)$ if and only if $a^{i(q+1)}=1$, so the second part of (3) holds too. (4) is a consequence of 6.1.

(6.3) *If f is bilinear and q is even then $\Delta(V,f)=O(V,f)\times\langle aI\rangle$ and $\Delta(V,Q)=O(V,Q)\times\langle aI\rangle$, where a is a generator for $F^{\#}$ and τ maps $\Delta(V,f)$ and $\Delta(V,Q)$ surjectively onto $F^{\#}$.*

Proof. If $\alpha=aI$ then $f(x\alpha,y\alpha)=a^2f(x,y)$, so $\alpha\in\Delta(V,f)$, and as the square map is an automorphism of F, the lemma holds.

(6.4) *Let f be bilinear and q odd. Let $n=\dim(V)$ and a a generator for $F^{\#}$. Then*

(1) *If n is odd then $\Delta(V,f)=O(V,f)*\langle aI\rangle$.*

(2) *If (V,f) is symplectic then $\Delta(V,f)=(O(V,f)*\langle aI\rangle)\langle\rho\rangle$ where $x_{2i-1}\rho=x_{2i-1}$ and $x_{2i}\rho=ax_{2i}$ for some symplectic basis $X=(x_i\colon 1\leqq i\leqq n)$.*

(3) *If* (V,f) *is orthogonal and* n *is even then* $\Delta(V,f)=(O(V,f)*\langle aI\rangle)\langle\rho\rangle$, *where* $x_{2i}\rho=x_{2i-1}$ *and* $x_{2i}\rho=ax_{2i}$ *for* $i\leqq n/2$ *if* $\operatorname{sgn}(f)=+1$, *and for* $i<n/2$ *if* $\operatorname{sgn}(f)=-1$, *where* $x_{n-1}\rho=\alpha x_{n-1}+\beta x_n$ *and* $x_n\rho=a\beta x_{n-1}+\alpha x_n$ *and* $\alpha,\beta\in F$ *with* $\alpha^2-a\beta^2=a$, *for some orthogonal basis* $X=(x_i\colon 1\leqq i\leqq n)$.

(4) *Either* $\Delta(V,f)\tau=F^{\#}$ *or* (V,f) *is orthogonal of odd dimension and* $\Delta(V,f)\tau$ *is the set of quadratic residues in* $F^{\#}$.

Proof. Let $g\in\Delta(V,f)$. Then for $x\in V$, $(xg)^{\perp}=(x^{\perp})g$, so $x^{\perp}$ is similar to $(xg)^{\perp}$. Hence if n is odd then $Q(xg)=\tau(g)Q(x)$ is a residue if and only if $Q(x)$ is a residue, so $\tau(g)$ is a residue. Thus $\Delta(V,f)\tau$ is contained in the set of residues in $F^{\#}$ when n is odd.

Next $aI\in\Delta(V,f)$ with $\tau(aI)=a^2$, so (1) holds and (4) holds if n is odd. Moreover $\langle aI\rangle*O(V,f)$ is the inverse image under τ of the residues in $F^{\#}$, so as $\tau(\rho)=a$, where ρ is the map defined in (2) and (3), it remains to show $\rho\in\Delta(V,f)$. This last fact follows from a straightforward calculation.

(6.5) *Let* f *be bilinear. Then either*

(1) $\Gamma(V,f)$ *(or* $\Gamma(V,Q)$*) is the split extension of* $\Delta(V,f)$ *(or* $\Delta(V,Q)$*) by* $A=\langle h\rangle$, *where* $\sigma(h)$ *is a generator of* $\operatorname{Aut}(F)$ *and* $\tau(h)=1$.

(2) (V,Q) *is orthogonal of even dimension with* $\operatorname{sgn}(Q)=-1$ *and* $\Gamma(V,Q)=\Delta(V,Q)A$, *where* $A=\langle h\rangle$, $A\cap\Delta(V,Q)=\langle t\rangle$, t *is a reflection if* p *is odd,* t *is a transvection if* $p=2$, $\sigma(h)$ *is a generator of* $\operatorname{Aut}(F)$, *and* $\tau(h)=1$.

Proof. Let $X=(x_i\colon 1\leqq i\leqq n)$ be a standard basis for (V,f) or (V,Q). An easy calculation using 6.1 shows we can choose (1) to hold with h fixing X pointwise unless (V,Q) is orthogonal and either

(i) n is even and $\operatorname{sgn}(Q)=-1$, or

(ii) n is odd and $Q(x_n)=a$ generates $F^{\#}$.

In these last two cases we define $h\in\Gamma(V,Q)$ with $\sigma(h)$ generating $\operatorname{Aut}(F)$ and $\tau(h)=1$; by 6.1 it suffices to define h on X and check condition $(*)$ of 6.1. If p is odd define $x_ih=x_i$ for $i<n$ and $x_nh=a^{(p-1)/2}x_n$. If $p=2$ define $x_ih=x_i$ for $i<n-1$ and let $u=x_{n-1}$ and $v=x_n$. Then $Q(\mathrm{a}u+bv)=a^2\alpha+ab+b^2\alpha$, where $\alpha x^2+x+\alpha$ is an irreducible quadratic in $F[x]$ and $f(u,v)=1$. Here define $uh=\alpha^{1/2}u$ and $vh=(\alpha^{1/2}+\alpha^{-3/2})u+\alpha^{-1/2}v$. A straightforward calculation shows (1) or (2) holds for this choice of h.

(6.6) *Let* G *consist of those* $g\in\Gamma(V,f)$ *(or* $\Gamma(V,Q)$*) with* $\tau(g)=1$. *Then* $G\sigma=\operatorname{Aut}(F)$.

Proof. This is a consequence of 6.2.4 and 6.5.

Section 7. Extensions of F

In this section F is a finite field of characteristic p and order $q=p^e$, and K is a finite extension of F. Let θ be an automorphism of K of order at most 2 and V a vector space over K which is an n-dimensional as a vector space over F.

Recall $L^\theta(V,V,K)$ is the space of sesquilinear maps from $V\times V$ into K with respect to θ; in particular if $\theta=1$, these maps are K-bilinear. For $\alpha\in \mathrm{Hom}_F(K,F)^\#$ and $f\in L^\theta(V,V,K), f\alpha$: $V\times V\to F$ is the composition of f with α. Similarly if Q is a quadratic K-form on V then $Q\alpha$: $V\to F$ is the composition of Q with α.

(7.1) *Define*

$$\mathrm{Tr}_F^K=\sum_{i=1}^{|K:F|}\sigma^i$$

where σ *is a generator of the Galois group* $\mathrm{Gal}(K/F)$ *of* K *over* F. *Then* $\mathrm{Tr}_F^K\in\mathrm{Hom}_F(K,F)^\#$ *and* Tr_F^K *commutes with each member of* $\mathrm{Aut}(K)$.

Proof. This is well known.

(7.2) *Let* $\alpha\in\mathrm{Hom}_F(K,F)^\#$, $G\leqq GL(V,K)$, *and* $f\in L_G(V,V,K)^\#$. *Then*

(1) $f\alpha\in L_G(V,V,F)^\#$.

(2) *If* Q *is a quadratic* K*-form on* V *preserved by* G *then* $Q\alpha$ *is a quadratic* F*-form on* V, *also preserved by* G.

(3) *If* f *is nondegenerate, so is* $f\alpha$.

(4) *If* f *is symmetric, so is* $f\alpha$.

(5) *If* f *is skew symmetric, so is* $f\alpha$.

(6) *If* $\alpha=\mathrm{Tr}_F^K$ *then* $\Gamma_F(V,f,K)\leqq\Gamma(V,f\alpha,F)$ *and* $\Gamma_F(V,Q,K)\leqq\Gamma(V,Q\alpha,F)$.

Proof. These remarks follow from straightforward calculations. In (6) we use the fact that Tr_F^K commutes with $\mathrm{Aut}(K)$.

(7.3) *Let* $\alpha\in\mathrm{Hom}_F(K,F)^\#$ *and assume* Q *is a nondegenerate quadratic form on* V. *Then*

(1) $\mathrm{sgn}(Q\alpha)=\mathrm{sgn}(Q)$ *if* $\dim_K(V)$ *is even.*

(2) *If* $\dim_K(V)$ *is odd and* $|K:F|$ *is even then for* $\varepsilon\in\{+1,-1\}$ *there exists* $\alpha_\varepsilon\in\mathrm{Hom}_F(K,F)^\#$ *with* $\mathrm{sgn}(Q\alpha_\varepsilon)=\varepsilon$.

Proof. If (W,Q) is a totally singular subspace of (V,Q) then $(W,Q\alpha)$ is a totally singular subspace of $(V,Q\alpha)$. In particular if $\mathrm{sgn}(Q)=+1$ we may choose W with $\dim_K(W)=\dim_K(V)/2$, so $\dim_F(W)=\dim_F(V)/2$, and hence $\mathrm{sgn}(Q\alpha)=+1$.

Next if $(V,Q)=(V_1,Q)\perp(V_2,Q)$ then also $(V,Q\alpha)=(V_1,Q\alpha)\perp(V_2,Q\alpha)$. Moreover we can choose V_1 and V_2 so that (V_1,Q) has sign $+1$ and $\dim_K(V_2)\leqq 2$. Thus replacing V by V_2 we may assume $\dim_K(V)\leqq 2$.

Suppose $\dim_K(V)=1$. We may assume $|K:F|$ is even and it remains to establish (2). Let E be the subfield of K of index 2. If $E\neq F$ then by induction on $|K:F|$ there exists $\beta_\varepsilon\in\mathrm{Hom}_E(K,E)^\#$ with $\mathrm{sgn}(Q\beta_\varepsilon)=\varepsilon$ and for each $\gamma\in\mathrm{Hom}_F(E,F)^\#$, $\mathrm{sgn}(Q\beta_\varepsilon)=\mathrm{sgn}(Q\beta_\varepsilon\gamma)$. So we take $\alpha_\varepsilon=\beta_\varepsilon\gamma$. Thus we may assume $F=E$. Now $V=Kx$ with $Q(ax)=a^2Q(x)$. As $\dim_K(V)$ is odd, q is odd. As $|K|=q^2$, each member of F is a quadratic residue in K. Further $\dim_F(\ker(\alpha))=1$, so $\ker(\alpha)=Fu$ for some $u\in K$, and either $\ker(\alpha)\cap K^2Q(x)=0$ or $\ker(\alpha)\subseteq K^2Q(x)$, depending on whether u and $Q(x)$ have the same quadratic character. In the first case $(Q\alpha)(ax)\neq 0$ for all $a\in K^\#$, so $\mathrm{sgn}(Q\alpha)=-1$, while in the second there is $a \in K^{\#}$ with $(Q\alpha)(ax)=0$, and hence $\mathrm{sgn}(Q\alpha)=+1$. As both choices of α are possible, we see that (2) holds.

So we may assume $\dim_K(V)=2$ and $\mathrm{sgn}(Q)=-1$, and it remains to show $\mathrm{sgn}(Q\alpha)=-1$. Let $k=|K:F|$; then there exists g of order $(q^k+1)/m$ in $O(V,Q,K)$, where $m=(q^k+1,2)$. $O(V,Q\alpha,F)\cong O_{2k}^{\varepsilon}(q)$, where $\varepsilon=\mathrm{sgn}(Q\alpha)$, and by 7.2.2, $g\in O(V,Q\alpha,F)$. Choose s a prime divisor of $q^{2k}-1$ such that s does not divide q^i-1 for $i<2k$; this is possible unless $q=2$ and $k=3$, where we choose $s=9$. Then there is $h\in\langle g\rangle$ of order s. But $O_{2k}^{+}(q)$ contains no element of order s, so $\varepsilon=-1$. Therefore (1) holds.

(7.4) *Let θ be an automorphism of K of order 2, $\beta=\mathrm{Tr}_F^K$, $G\leqq GL(V,K)$, and $f\in L_G^{\theta}(V,V,K)^{\#}$. Then*

(1) $\bar\theta=\theta_{|F}\in\mathrm{Aut}(F)$, *$\bar\theta$ has order 2 if $|K:F|$ is odd, and $\bar\theta=1$ if $|K:F|$ is even.*

(2) $f\beta\in L_G^{\bar\theta}(V,V,F)^{\#}$.

(3) *If f is hermitian symmetric then $f\beta$ is hermitian symmetric when $|K:F|$ is odd and $f\beta$ is symmetric if $|K:F|$ is even.*

(4) *If f is nondegenerate, so is $f\beta$.*

(5) $\Gamma_F(V,f,K)\leqq\Gamma(V,f\alpha,F)$.

(6) *Assume (V,f) is unitary and $|K:F|$ is even. Let E be the subfield of K of index 2 and define $P\colon V\to F$ by $P(v)=f(v,v)\mathrm{Tr}_F^E$. Then P is a quadratic form on V with $P(u+v)=P(u)+P(v)+(f\beta)(u,v)$, and $\mathrm{sgn}(P)=(-1)^{\dim_K(V)}$.*

Proof. The proof of the first five remarks is straightforward and uses 7.1, particularly the fact that β commutes with $\mathrm{Aut}(K)$. Thus it remains to prove (6), so we may take (V,f) to be a unitary space and $|K:F|$ to be even. Another easy calculation verifies all but the last remark of (6). For that observe that (V,f) is the orthogonal sum of 1-dimensional nondegenerate subspaces (V_i,f), so (V,P) is the orthogonal sum of the subspaces (V_i,P). If $m=\dim_K(V)>1$ then by induction on m, (V_i,P) is of sign -1, so (V,P) is of sign $(-1)^m$. Thus we may take $m=1$. Next if $E\neq F$ then (V,R) is of sign -1 by induction on $|K:F|$, where $R\colon V\to E$ is defined by $R(v)=f(v,v)$. Then by 6.3.1, (V,P) has the same sign as (V,R), and we are done. So we may take $E=F$. Now $V=Kx$ for some $x\in V$ with $f(x,x)=1$ and $P(ax)=a^{1+\theta}\neq 0$ for $a\in K^{\#}$, so (V,P) contains no nonsingular vectors. We conclude (V,P) has sign -1, so the proof is complete.

(7.5) *Let θ be an automorphism of K of order at most 2, $f\in L_G^{\theta}(V,V,K)^{\#}$, and $\alpha\in\mathrm{Hom}_F(K,F)^{\#}$. Let $\bar\theta=\theta_{|F}$. Then*

(1) *The map $\Psi\colon\tau\to\tau(f)\alpha$ is an injective F-linear transformation from K into $L_G^{\bar\theta}(V,V,F)$, where $\tau(f)(v,u)=f(\tau v,u)$.*

(2) *Assume V is an irreducible FG-module and $K=\mathrm{Hom}_{FG}(V,V)$. Then Ψ is an isomorphism and if $\alpha=\mathrm{Tr}_F^K$ then one of the following holds:*

(i) *$\theta=1$ and each member of $L_G(V,V,K)^{\#}$ and $L_G(V,V,F)^{\#}$ is nondegenerate symmetric.*

(ii) *$\theta=1$ and each member of $L_G(V,V,K)^{\#}$ and $L_G(V,V,F)^{\#}$ is nondegenerate skew symmetric.*

(iii) *Let θ be an involution, S the set of unitary forms in $L_G^{\theta}(V,V,K)$, and T the set of skew unitary forms g in $L_G^{\theta}(V,V,K)$ (ie. $g(x,y)=-g(y,x)^{\theta}$). Then S*

and T are the nontrivial elements in 1-dimensional E-subspaces of $L_G^\theta(V, V, K)$, *where E is the subfield of index 2 in K and* $S\Psi$ *and* $T\Psi$ *are the sets of nondegenerate symmetric or unitary forms, skew symmetric or skew unitary forms in* $L_G^\theta(V, V, F)$, *for* $|K:F|$ *even or odd, respectively.*

Proof. Let $\beta \in \mathrm{Hom}_F(K, F)^{\#}$ with $\beta = \mathrm{Tr}_F^K$ if θ is an involution. For $\tau \in K$, $\tau(f) \in L_G^\theta(V, V, K)$, so by 7.2 and 7.4, $\tau\varphi = \tau(f)\beta \in L_G^\theta(V, V, F)$. Moreover it is evident that φ is F-linear. $\tau\varphi = \sigma\varphi$ if and only if $x\tau\beta = x\sigma\beta$ for all $x \in K$, so by 3.1, φ is an injection. Indeed by 3.1, $\alpha = \pi_a\beta$ for some $a \in K^{\#}$, where $\pi_a\colon K \to K$ is multiplication by a. Thus for $\tau \in K$, $\tau(f)\alpha = (a\tau)(f)\beta$, so the map $\Psi\colon \tau \to \tau(f)\alpha$ is also an injective F-linear transformation, as $\Psi = \pi_a\varphi$.

Assume V is an irreducible FG-module with $K = \mathrm{Hom}_{FG}(V, V)$. Then by 4.7, K is isomorphic to $L_G^\theta(V, V, F)$ as an F-space, so Ψ is an isomorphism. 4.8 and an easy calculation complete the proof of (2).

(7.6) *Assume* (V, f) *is a symplectic of unitary space over F or Q is a quadratic form and* (V, Q) *is an orthogonal space over F with associated bilinear form f. Assume V is an irreducible FG-module and* $K = \mathrm{Hom}_{FG}(V, V)$. *Then either*

(1) *There exists a K-form g on V preserved by G of the same type as f, and if Q is defined there exists a K-quadratic form P on V preserved by G such that* $g\,\mathrm{Tr}_F^K = f$ *or* $P\,\mathrm{Tr}_F^K = Q$, *respectively.* $|K:F|$ *is odd if* (V, f) *is unitary.*

(2) *f is symmetric,* $|K:F|$ *is even, and there exists a unitary K-form g on V preserved by G such that* $g\,\mathrm{Tr}_F^K = f$, *and if* (V, Q) *is orthogonal then* $g\,\mathrm{Tr}_F^E = Q$, *where E is the subfield of K of index* 2, *and* $\mathrm{sgn}(Q) = (-1)^{\dim_K(V)}$.

(3) *f is symplectic,* $|K:F|$ *is even, and there exists a unitary K-form g on V preserved by G such that* $eg\,\mathrm{Tr}_F^K = f$, *where* $e \in K$ *with* $e\sigma = -e$ *and* σ *is the involution in* $\mathrm{Gal}(K/F)$.

Proof. To begin, assume (V, f) is unitary but $|K:F|$ is even, and let L be the subfield of F of index 2. We wish to obtain a contradiction. Assume first the FG-representation on V is not defined over L. Then by 3.6, V is not FG-isomorphic to V^σ, where σ is the automorphism of F of order 2, and by 3.8, V is an irreducible LG-module. By 7.4 there is $\beta \in \mathrm{Hom}_L(F, L)^{\#}$ such that $f\beta$ is a nondegenerate symmetric L-form on V preserved by G. The existence of $f\beta$ and induction on the order of F imply there exists a K-form g on V preserved by G which is symmetric or hermitian. Hence if E is the subfield of K of index 2, $L_G(V, V, E) \neq 0$ by 7.2 and 7.4, so V is EG-isomorphic to V^* by 4.7. Hence V is also FG-isomorphic to V^* as $F \leqq E$, while as f exists, V is FG-isomorphic to $V^{*\sigma}$ by 4.7. So V^* is FG-isomorphic to V^σ, contrary to an earlier remark.

So the FG-representation on V is defined over L. Then by 3.9, $V = F \otimes_L W$ for some irreducible LG-submodule W of V, and $|D:L|$ is odd, where $D = \mathrm{Hom}_{LG}(W, W)$. The extension d generated by D and F is contained in K as F and D commute with G. Thus we may regard V as a dG-module and W as a DG-module. As $|d:D| = 2 = |F:L|$, $V = d \otimes_D W$. Hence as W is an absolutely irreducible DG-module, V is an absolute irreducible dG-module, so $K \leqq d$, contradicting $|K:F|$ even and $|d:F|$ odd.

We have shown that if f is hermitian then $|K:F|$ is odd, so that the automorphism σ of F of order 2 lifts to the automorphism θ of K of order 2.

Let $V_K = K \otimes_F V$. Observe that if f is hermitian then $(V_K)^\theta = (V^\sigma)_K$. In that event let f_K be the hermitian form on V_K which agrees with f on $1 \otimes V$. If f is bilinear let f_K be the bilinear form on V_K which restricts to f on $1 \otimes V$. If Q is a quadratic form on V, let Q_K be the K-quadratic form on V_K which agrees with Q on $1 \otimes V$.

By 3.5, $V_K = \bigoplus_{\alpha \in \mathrm{Gal}(K/F)} W^\alpha$, with W KG-isomorphic to V. Assume first that W is a nondegenerate subspace of (V_K, f_K) and let g_0 be the restriction of f_K to W and P_0 the restriction of Q_K to W if (V,Q) is orthogonal. Then G preserves g_0 and P_0, and as f_K is the same type as f, so is g_0. By 6.5 there is $\tau \in K^\#$ with $\tau(g_0)\mathrm{Tr}_F^K = f$ and if (V,Q) is orthogonal then $\tau(P_0)\mathrm{Tr}_F^K = Q$ by 4.9. So (1) holds in this case with $g = \tau(g_0)$ and $P = \tau(P_0)$.

Thus we may assume (W, f_K) is not nondegenerate. For $\alpha \in \mathrm{Gal}(K/F)$ and $x = \sum a_i x_i$ and $y = \sum b_i x_i$ in V_K with $x_i \in 1 \otimes V$ and $a_i, b_i \in K$ we have

$$f_K(x\alpha, y\alpha) = f_K(\sum a_i^\alpha x_i, \sum b_j^\alpha x_j) = \sum_{i,j} a_i^\alpha b_j^{\alpha\theta} f(x_i, x_j)$$
$$= (f_K(\sum_{i,j} a_i b_j^\theta f(x_i, x_j)))^\alpha = f_K(x, y)^\alpha.$$

Thus $\alpha \in \Gamma(V_K, f_K)$, so as $(W^\alpha\colon \alpha \in \mathrm{Gal}(K/F))$ are distinct KG-irreducibles, $G\,\mathrm{Gal}(K/F) \leqq \Gamma(V_K, f_K)$ is irreducible. Hence by 5.5, $V_K = \perp_{1 \leqq i \leqq m/2} U_i$ where $U_i = W^{\alpha_{2i-v}} \oplus W^{\alpha_{2i}}$ and W^α is totally singular for each $\alpha \in \mathrm{Gal}(K/F)$. In particular $m = |\mathrm{Gal}(K/F)| = |K:F|$ is even, so f is not hermitian. Moreover $\alpha_{2i} = \alpha_{2i-1}\sigma$, where σ is the involution in $\mathrm{Gal}(K/F)$ and $U = W \oplus W^\sigma$ is nondegenerate. Now f_K restricted to $W \times W^\sigma$ is in $L_G(W, W^\sigma)^\#$, so by 4.6 and 7.5 there is $g \in L_G^\sigma(V, V, K)$ with $g\,\mathrm{Tr}_F^K = f$, and by 7.5 (V, g) or (V, eg) is a unitary space, where $e \in K$ with $e^\sigma = -e$. If (V,Q) is orthogonal and q is even, $g\,\mathrm{Tr}_F^E = Q$ by 4.9 and 7.4.6. Indeed if (V,Q) is orthogonal then by 7.4.6, $\mathrm{sgn}(Q) = (-1)^{\dim_K(V)}$.

(7.7) *Lemma* 7.6 *remains valid for any field K between F and* $\mathrm{Hom}_{FG}(V, V)$.

Proof. Let $F \leqq K \leqq k = \mathrm{Hom}_{FG}(V, V)$, and let h or R be the k-form on V with $h\,\mathrm{Tr}_F^k = f$ or $R\,\mathrm{Tr}_F^k = Q$, whose existence is insured by 7.6. Let $g = h\,\mathrm{Tr}_K^k$ and $P = R\,\mathrm{Tr}_K^k$ in the respective case. Then as $\mathrm{Tr}_F^k = \mathrm{Tr}_K^k \mathrm{Tr}_F^k$, $g\,\mathrm{Tr}_F^k = f$ or $P\,\mathrm{Tr}_F^K = Q$. By 7.2 and 7.4, g and P have the desired properties.

(7.8) *Assume (V,f) is a symplectic or unitary space over F, or Q is a quadratic form and (V,Q) is an orthogonal space over F with associated bilinear form f. Assume V is an irreducible FG-module and $F \leqq K \leqq \mathrm{Hom}_{FG}(V, V)$. Choose g or P as in Lemma* 7.7, *let $\Gamma = \Gamma(V,f)$ or $\Gamma(V,Q))$ and $H = \Gamma_F(V, g, K)$ or $\Gamma_F(V, P, K)$ in the appropriate case. Then $N_\Gamma(G) \leqq N_\Gamma(K) = H$.*

Proof. K is characteristic in $C_{\Gamma(V,F)}(G) = \mathrm{Hom}_{FG}(V, V)$, so $N_\Gamma(G) \leqq N_\Gamma(K)$. By 3.14, $N_{\Gamma(V,F)}(K) = \Gamma(V, K)$, so $N_\Gamma(K) = \Gamma(V,K) \cap \Gamma$, so it remains to show $\Gamma(V,K) \cap \Gamma = H$. By 6.6, $H/C_H(K) \cong \mathrm{Aut}(K) \cong \Gamma(V,K)/GL(V,K)$, so $N_\Gamma(K) = HC_\Gamma(K)$ and it remains to show $C_\Gamma(K) = C_H(K)$. By 6.2, 6.3, and 6.4.4 either $C_H(K)\tau = F^\#$ or (V,P) is orthogonal, $\dim_K(V)$ is odd, and $C_H(K)\tau$ consists of the K-residues in $F^\#$. If the latter set is not $F^\#$ then $|K:F|$ is odd, so by another application of 6.4.4, $C_H(K)\tau = C_\Gamma(K)\tau$. Thus it remains to show $C_H(K)\cap O(V,f) = C_\Gamma(K)\cap O(V,f)$. But without loss $G = C_\Gamma(K)\cap O(V,f)$, so G preserves g or P and thus $G \leqq H$, completing the proof.

Section 8. Subfields of F

In this section F is a finite field of characteristic p and K is a subfield of F of index r.

Suppose for the moment U is a K-space and let $V = U_F = F\otimes_K U$. Given $f\in L(U,U)$, define $F\otimes f$ to be the unique member of $L(V,V,F)$ whose restriction to $1\otimes U$ agrees with f. Observe that if (U,f) is symplectic or orthogonal then so is $(V,F\otimes f)$ and that $O(U,f)\leqq O(V,F\otimes f)$ and $\Delta(U,f)\leqq \Delta(V,F\otimes f)$, where the embeddings are obtained by tensoring the original representations. Similarly if Q is a quadratic form on U with bilinear form f, let $F\otimes Q$ be the unique quadratic form on V, with bilinear form $F\otimes f$, whose restriction to $1\otimes U$ is Q.

Suppose further θ is an automorphism of F of order 2. If $r=2$ and $f\in L(U,U)$ is symmetric define $F\otimes(1,f)$ to be the unique form in $L^\theta(V,V)$ agreeing with f on $1\otimes U$. Observe that if (U,f) is nondegenerate then $(V,F\otimes(1,f))$ is unitary. If $r=2$, p is odd, (U,f) is a symplectic space, and $t\in F$ with $t^{q-1}=-1$, where $q=|K|$, then define $F\otimes(t,f)$ to be the unique form in $L^\theta(V,V)$ which agrees with tf on $1\otimes U$. Observe that $F\otimes(t,f)$ is unitary. Finally if r is odd then $\bar\theta = \theta_{|K}$ is an automorphism of K of order 2 and if f is a unitary form on U we define $F\otimes(1,f)$ to be the unique unitary form on V which agrees with f on $1\otimes U$. Again we have

$$O(U,f)\leqq O(V,F\otimes(s,f)) \quad\text{and}\quad \Delta(U,f)\leqq \Delta(V,F\otimes(s,f)).$$

(8.1) *Assume (V,f) is a symplectic or unitary F-space or Q is a quadratic F-form on V and (V,Q) is an orthogonal space with associated bilinear form f. Assume K is a subfield of F of prime index r and $G\leqq O(V,f)$ or $O(V,Q)$ acts absolutely irreducibly on V with the representation defined over K. Then there exists an absolutely irreducible KG-submodule U of V such that $V=F\otimes_K U$ and a nondegenerate K-form g on U preserved by G such that either*

1) *f and g are bilinear with* $\operatorname{sym}(f)=\operatorname{sym}(g)$ *and $F\otimes g=\tau f$ for some $\tau\in F^\#$. If (V,Q) is orthogonal there is also a quadratic K-form P on U preserved by G and associated to g with $F\otimes P=\tau Q$. If $\dim_F(V)$ is even then* $\operatorname{sgn}(Q)=\operatorname{sgn}(P)^r$.

2) *f is unitary and $\tau f = F\otimes(s,g)$ for some τ, $s\in F^\#$. Moreover one of the following holds:*

   i) *g is unitary, r is odd and $s=1$.*
   ii) *g is symmetric, $r=2$, and $s=1$.*
   iii) *g is symplectic, p is odd, $r=2$, and $s^{q-1}=-1$, where $q=|K|$.*

Proof. By 3.10, $V=F\otimes_K U$ for some absolutely irreducible KG-submodule U of V. Let $\beta\in\operatorname{Hom}_K(F,K)^\#$ and if f is unitary let $\beta=\operatorname{Tr}^F_K$. Let $h=f\beta$ and $R=Q\beta$ if (V,Q) is orthogonal. By 7.2 and 7.4 either h is a K-form on V of the same type as f or f is unitary, $r=2$, and h is a nondegenerate symmetric bilinear K-form on V. Similarly R is a quadratic K-form on V. Let f_U and Q_U be the restrictions of f and Q to U. Observe $f_U \neq 0 \neq Q_U$ as $f \neq 0 \neq Q$ and U contains an F-basis of V.

Suppose f_U is bilinear and let g and P be the restrictions of h and R to U. As $f_U \neq 0$ we can choose β so that $g \neq 0$. Thus (U,g) (or (U,P)) is a K-space of the same type as (V,f) (or (V,Q)). Let $\bar{g}=F\otimes g$ and $\bar{P}=F\otimes P$. As $\bar{g}$ and $\bar{P}$ are preserved by G, 4.7 implies $\bar{g}=\tau f$ for some $\tau\in F^{\#}$ and by 4.9, $\bar{P}=\tau Q$. In particular $\mathrm{sgn}(\bar{P})=\mathrm{sgn}(Q)$ if $\dim_F(V)$ is even, so it remains to show $\mathrm{sgn}(\bar{P}) =\mathrm{sgn}(P)^r$ under this hypothesis. Let W be a nondegenerate 2-dimensional subspace of U of sign ε. Then W has a basis (x,y) with $P(ax+y)=d(a)$ for some quadratic $d(z)\in K[z]$, with d reducible if and only if $\varepsilon=+1$. Now d is reducible in $F[z]$ precisely when $\varepsilon=+1$ or $r=2$, so $\mathrm{sgn}(W,\bar{P})=\varepsilon^r$. We conclude that $\mathrm{sgn}(\bar{P})=\mathrm{sgn}(P)^r$, as desired.

So assume f is unitary and let θ be the automorphism of F of order 2. If (U,h) is nondegenerate let g be the restriction of h to U. Then either (U,g) is unitary or $r=2$ and (U,g) is orthogonal or symplectic for p odd or even, respectively. In any case $F\otimes(1,g)=\bar{g}$ is a unitary form on V preserved by G, so by 4.7, $\bar{g}=\tau f$.

Thus we may assume (U,h) is degenerate for each $U\in\mathrm{Irr}(G,V,K)$. Hence by 5.2, V is the orthogonal sum of nondegenerate KG-subspaces W_i, $1\leqq i\leqq m$, with $W_i=U_i\oplus U_i'$ and U_i, $U_i'\in\mathrm{Irr}(G,V,K)$. In particular $\dim_K(V)/\dim_K(U)=k$ is even. But of course $k=r$, so $r=2$ and $V=U\oplus U'$. As U' is KG-isomorphic to U, the existence of h implies $L_G(U,U,K)\neq 0$. Let $g\in L_G(U,U,K)^{\#}$. By 4.8, g is symmetric or skew symmetric. In the first case $F\otimes(1,g)=\tau f$ by 4.7, so we may take q odd and (U,g) symplectic. Here $F\otimes(t,g)=\tau f$, completing the proof.

(8.2) *Assume the hypothesis of* 8.1 *and let* (U,g) (*or* (U,P)) *be the K-space supplied by that lemma. Then*

(1) $N_{\Gamma(V,f)}(G)\leqq FH$ (*or* $N_{\Gamma(V,Q)}(G)\leqq FH$) *where* $H=N_{\Gamma(V,f)}(U)$ (*or* $H=N_{\Gamma(V,Q)}(U)$),
and

(2) $H=A\Delta(U,g)$ (*or* $A\Delta(U,P)$), $C_H(U)=C_A(U)$ *is of order r with* $\sigma(C_A(U))$ *also of order r*, $H/C_H(U)=\Gamma(U,g)$ (*or* $\Gamma(U,P)$), *and* $A/C_A(U)=\langle h\rangle$ *is as in* 6.2 *or* 6.5.

Proof. Part (1) is a consequence of the fact, established in Sect. 6, that $F\leqq\Delta(V,f)$ (or $\Delta(V,Q)$) and 3.15. Let $\Gamma=\Gamma(V,f)$ or $\Gamma(V,Q)$ in the appropriate case. By 3.15, $H=\Gamma\cap BGL(U,K)$ with $C_B(U)=C_{\Gamma(V)}(U)$ of order r, $\sigma(C_B(U))$ of order r, and $N_{\Gamma(V)}(U)/C_B(U)=\Gamma(U,K)$.

Let $A=\langle h\rangle\cong\mathrm{Aut}(F)$ unless (U,P) is orthogonal of sign -1, $r=2$, and either

(a) (V,Q) is orthogonal of sign $+1$, or

(b) p is odd and (V,f) is unitary.

In these latter cases let $A=\langle h\rangle\times\langle e\rangle$ with e of order 2.

Suppose (U,P) is not orthogonal of sign -1. Then by 6.2 and 6.5 there is a representation π_K: $A\to\Gamma(U,g,K)$ such that $\Gamma(U,g,K)=\Delta(U,g,K)A\pi_K$, $\ker(\pi_K)$ is of order r, and $\sigma_K(h)$ is a generator of $\mathrm{Aut}(K)$. Then $\sigma_K(h)$ extends to a generator $\sigma(h)$ of Aut(F) and we have an isomorphism σ: $A \to$ Aut(F). Now by 6.1, π_K extends to π: $A \to \Gamma(V,f)$ defined by $(\sum a_i \otimes u_i)(h\pi) = \sum a_i^{\sigma(h)} \otimes u_i h \pi_K$. On the otherhand if (U,P) is orthogonal of sign -1 then by 8.1 case (a) or (b) holds. By 6.5 we again have a representation π_K with $\ker(\pi_K) = \langle e \rangle$ and with $\ker(\sigma_K) \cong E_4$. We extend $\sigma_K(h)$ to a generator $\sigma(h)$ of Aut(F) and define $\sigma(e)$ to be the automorphism of F of order 2. Then we have a homomorphism σ: $A \to$ Aut(F) with $\ker(\sigma) \cap \ker(\pi_K) = 1$, so we can extend π_K as above to a faithful representation π: $A \to \Gamma(V,f)$. In any event, as we observed at the beginning of this section, $H_1 = \Delta(U,g) \leqq \Delta(V,f)$, and by construction $AH_1 \leqq H$ with $AH_1/C_A(U) \cong \Gamma(U,g)$. Thus it remains to show $AH_1 = H$. As $A\sigma = \mathrm{Aut}(K) = \Gamma\sigma$ and H_1 is the kernel of $\sigma_{|AH_1}$, it suffices to show $H_1 = H \cap GL(V,F)$. By 8.1, $O(U,g) = H_0 = H \cap O(V,f)$, so as $K = C_{\Delta(V,f) \cap H}(H_0)$, it suffices to show $\mathrm{Aut}_{H_1}(H_0) \geqq \mathrm{Aut}_{GL(V,F)}(H_0)$. This last fact follows from 2.5.

Section 9. Tensoring forms

In this section F is a finite field of characteristic p and θ is an automorphism of F of order at most 2.

If $\mathscr{B} = (V_i\colon 1 \leqq i \leqq m)$ is a family of F-spaces and $f_i \in L^\theta(V_i, V_i)$ define $f_1 \otimes \ldots \otimes f_m$ to be the unique member of $L^\theta(V_1 \otimes \ldots \otimes V_m,\ V_1 \otimes \ldots \otimes V_m)$ such that

$$(f_1 \otimes \ldots \otimes f_m)(v_1 \otimes \ldots \otimes v_m, u_1 \otimes \ldots \otimes u_m) = \prod_{i=1}^{m} f_i(v_i, u_i)$$

for all u_i, $v_i \in V_i$, $1 \leqq i \leqq m$. Observe

(9.1) (1) *$f_1 \otimes \ldots \otimes f_m$ is nondegenerate if and only if f_i is nondegenerate for each i.*

(2) *If $\theta = 1$ and each f_i is symmetric or skew symmetric, then $f_1 \otimes \ldots \otimes f_m$ is symmetric or skew symmetric with* $\mathrm{sym}(f_1 \otimes \ldots \otimes f_m) = \prod_{i=1}^{m} \mathrm{sym}(f_i)$.

(3) *If θ is an involution and each f_i is unitary then $f_1 \otimes \ldots \otimes f_m$ is unitary.*

(4) *If $p = 2$ and (V_i, f_i) is a symplectic space for $1 \leqq i \leqq m$, then $V_1 \otimes \ldots \otimes V_m$ admits a unique quadratic form Q with associated bilinear form $f_1 \otimes \ldots \otimes f_m$ such that $Q(v_1 \otimes \ldots \otimes v_m) = 0$ for all $v_i \in V_i$.*

Recall the definitions of $\Gamma(\mathscr{B})$, $\Lambda(\mathscr{B}, \mathscr{F})$ and the representation π of these groups, defined in Sect. 3 before 3.12. If $\mathscr{D} = ((V_i, f_i)\colon 1 \leqq i \leqq m)$ is a family with $f_i \in L^\theta(V_i, V_i)$, let $\Gamma(\mathscr{D})$ be the subgroup of $\Gamma(\mathscr{B})$ consisting of these $\boldsymbol{x} = (x_i\colon i \leqq i \leqq m)$ with $x_i \in \Gamma(V_i, f_i)$. If $\mathscr{F} = (\alpha_i\colon 1 \leqq i \leqq m)$ is a family of similarities α_i: $(V_1, f_1) \to (V_i, f_i)$ with $\alpha_1 = 1$, let $\Lambda(\mathscr{D}, \mathscr{F})$ be the subgroup of $\Lambda(\mathscr{B}, \mathscr{F})$ generated by $\Gamma(\mathscr{D})$ and the group S defined before 3.12. Observe

(9.2) (1) *$\Gamma(\mathscr{D})\pi \leqq \Gamma(V_1 \otimes \ldots \otimes V_m, f_1 \otimes \ldots \otimes f_m)$, whete π is the representation defined above. Moreover* $\tau(\boldsymbol{x}\pi) = \prod_{i=1}^{m} \tau(x_i)$.

(2) *If* $\mathscr{F}=(\alpha_1: 1\leqq i\leqq m)$ *is a family of similarities* α_i: $(V_1,f_1)\to(V_i,f_i)$ *with* $\alpha_1=1$, *then* $\Lambda(\mathscr{D},\mathscr{F})\pi\leqq\Gamma(V_1\otimes\ldots\otimes V_m,\ f_1\otimes\ldots\otimes f_m)$ *and* $S\pi\leqq O(V_1\otimes\ldots\otimes V_m,\ f_1\otimes\ldots\otimes f_m)$.

(3) $\Lambda(\mathscr{D},\mathscr{F})\pi$ *is the product of a central product* D *of the groups* $\Delta(V_i,f_i)$, $1\leqq i\leqq m$, *with* $A\times S\pi$ *where* A *and its action on each* $\Delta(V_i,f_i)$ *is described in* 6.2 *and* 6.5, $S\pi$ *is the symmetric group on* m *letters, and* $S\pi D$ *is a homomorphic image of the wreath product of* S *with* $\Delta(V_1,f_1)$.

(4) *If* $p=2$ *and each member of* $\mathscr{D}$ *is a symplectic space then* $\Gamma(\mathscr{D})\pi$ *and* $\Lambda(\mathscr{D},\mathscr{F})\pi$ *preserve the quadratic form defined in* 9.1.4.

(5) *If* f_i *is nondegenerate for each* i *then*

$$\Gamma(\mathscr{B})\pi\cap\Gamma(V_1\otimes\ldots\otimes V_m,f_1\otimes\ldots\otimes f_m)=\Gamma(\mathscr{D})\pi$$

and

$$\Lambda(\mathscr{B},\mathscr{F})\cap\Gamma(V_1\otimes\ldots\otimes V_m,f_1\otimes\ldots\otimes f_m)=\Lambda(\mathscr{D},\mathscr{F}).$$

In the remainder of this section U, V and W are F-spaces equipped with bilinear forms f_U, f_V, and f_W. $U\otimes V$ is understood to be equipped with the bilinear form $f_{U\otimes V}=f_U\otimes f_V$. Write (,) for each form.

(9.3) $(U\perp W)\otimes V=(U\otimes V)\perp(W\otimes V)$.

Proof. For $u\in U$, $w\in W$, and $v_i\in V$, $(u\otimes v_1, w\otimes v_2)=(u,w)(v_1,v_2)=0$ as $(u,w)=0$.

(9.4) *Let* U *and* V *be hyperbolic planes with hyperbolic bases* (u_1,u_2) *and* (v_1,v_2), *respectively. Then* $(u_1\otimes v_1,\ u_2\otimes v_2)$ *and* $(u_1\otimes v_2,\ u_2\otimes v_1)$ *are hyperbolic bases for the hyperbolic spaces* A *and* B *they generate, and* $U\otimes V=A\perp B$. *If* $p=2$ *then* $\langle u_1\otimes v_1,\ u_1\otimes v_2\rangle$ *is totally singular with respect to the quadratic form* Q *of* 9.1, *so* $\mathrm{sgn}(Q)=+1$.

(9.5) *If* $p=2$ *and* U *and* V *are symplectic and* Q *is the quadratic form in* 9.1, *then* $\mathrm{sgn}(Q)=+1$.

Proof. $U=\perp_i U_i$ and $V=\perp_j V_j$ with U_i and V_j hyperbolic planes. So by 9.3, $U\otimes V=\perp_{i,j} U_i\otimes V_j$, and by 9.4, Q restricted to $U_i\otimes V_j$ is of sign $+1$ for each i, j, so the lemma holds.

Because of 9.5 we may take p odd in the remaining lemmas in this section.

(9.6) *If* A *is a totally singular subspace of* U *of dimension* $\dim(U)/2$, *then* $A\otimes V$ *is a totally singular subspace of* $U\otimes V$ *of dimension* $\dim(U\otimes V)/2$.

(9.7) *Assume either*

(1) $\mathrm{sym}(f_U)=\mathrm{sym}(f_V)=-1$, *or*

(2) $\mathrm{sym}(f_U)=\mathrm{sym}(f_V)=+1$ *and* U *is of even dimension with* $\mathrm{sgn}(f_U)=+1$.

Then $\mathrm{sym}(f_{U\otimes V})=+1$, $\dim(U\otimes V)$ *is even, and* $\mathrm{sgn}(f_{U\otimes V})=+1$.

Proof. This is a consequence of 9.1 and 9.6.

(9.8) *Let* W *be orthogonal of dimension* 2 *and sign* -1. *Then* $W\otimes W$ *is an orthogonal space of dimension* 4 *and sign* $+1$.

Proof. This is an easy calculation.

(9.9) *If U and V are orthogonal spaces of sign -1 then $U \otimes V$ is an orthogonal space and sign $+1$.*

Proof. Argue as in 9.5 using 9.7 and 9.8.

(9.10) *If U and V are orthogonal spaces with* $\dim(U)$ *odd,* $\dim(V)$ *even, and* $\mathrm{sgn}(f_V) = -1$, *then $U \otimes V$ is an orthogonal space of even dimension and sign -1.*

Proof. $U = U_1 \perp \langle u \rangle$ and $V = V_1 \perp W$ with $\mathrm{sgn}(U_1) = \mathrm{sgn}(V_1) = +1$, $\dim(W) = 2$, and $\mathrm{sgn}(f_W) = -1$. Then by 9.3 and 9.7, $U \otimes V = A \perp (\langle u \rangle \otimes W)$ with A of sign $+1$, so we may assume $U = \langle u \rangle$ and $V = W$. But then the result is clear.

Section 10. Stabilizers of tensored forms

In this section F is a finite field of characteristic p and (V,f) is a unitary or symplectic space over F or (V,Q) is an orthogonal space over F with associated bilinear form f. Let $O = O(V,f)$ or $O(V,Q)$ in the respective case. Γ and Δ are defined similarly.

(10.1) *Assume the hypothesis and notation of Lemma* 3.11. *In addition assume* $K = F$, $G \leqq O$, $m > 1$, *and the sum* $V = \bigoplus_{i=1}^{m} V_i$ *is orthogonal. Then*

(1) $(\alpha_i, \alpha_i)(f_{|V_i}) = e_i f_{|V_1}$, *for some* $e_i \in F^{\#}$, *and if f is unitary, e_i is in the subfield of F of index* 2.

(2) *There exists a unique form* $g \in L^{\theta}(A,A)$ *with* $g(\alpha_i, \alpha_j) = \delta_{ij} e_i$, *where* $\theta = 1$ *if f is bilinear and θ is the automorphism of F of order 2 if f is unitary.*

(3) *For* $a, b \in A$, *and* $u, v \in V_1$, $f(ua, vb) = f(u,v)\, g(a,b)$ *and* $(V_1 a, f)$ *is totally singular if and only if* $g(a,a) = 0$.

(4) *If* $N_{\Gamma(V,f)}(G)$ *is irreducible on V and $p = 2$, then f is unitary.*

Proof. $(\alpha_i, \alpha_i)(f_{|V_i})$ and $f_{|V_1}$ are in $L^{\theta}_G(V_1, V_1)^{\#}$ and both are unitary if f is unitary, so part (1) follows from 4.7 and 4.8.2. Part (2) is trivial. Let u, $v \in V_1$ and $a = \sum a_i \alpha_i$, $b = \sum b_j \alpha_i \in A$. Then

$f(ua, vb) = \sum a_i b_j^{\theta} f(u\alpha_i, v\alpha_j) = f(u,v)(\sum_i e_i a_i b_i^{\theta}) = f(u,v)\, g(a,b)$. So $(V_1 a, f)$ is totally singular if and only $g(a,a) = 0$, since as V_1 is nondegenerate there is a choice of u and v with $f(u,v) \neq 0$. Therefore (3) holds.

Assume $p = 2$ and f is bilinear. Then $a = \sum a_i \alpha_i \in A$ is singular if and only if $\sum a_i^2 e_i = 0$. As $p = 2$, $\sum a_i^2 e_i = (\sum a_i d_i)^2$, where $d_i^2 = e_i$. Thus the set B of singular vectors of A forms a subspace of codimension 1, and then as $m > 1$, we conclude from (3) and 3.11.3 that the set of totally singular members of $\mathrm{Irr}(G,V)$ generates a proper nontrivial subspace of V, so that (4) holds.

(10.2) *Assume the hypothesis and notation of Lemma* 3.11. *In addition let* $V_{2i-1} \oplus V_{2i} = U_i$, *assume* $K = F$, $G \leqq O$, *each member of* $\mathrm{Irr}(G,V)$ *is totally singular, and* $V = \perp_i U_i$. *Then*

(1) *f is bilinear.*

(2) *We may choose* α *and* FG*-isometries* $\beta_i\colon U_1 \to U_i$, $1 \leqq i \leqq m/2$, *such that* $\alpha_{2i-1} = \beta_{i|V_1}$ *and* $\alpha_2^{-1}\alpha_{2i} = \beta_{i|V_2}$.

(3) *There exists a unique symplectic form g on A with* α *a symplectic basis for g.*

(4) $C_0(G)\pi = O(A,g)$ *and* $C_\Delta(G)\pi = \Delta(A,g)$.

(5) *Define* $h \in L(V_1, V_1)$ *by* $h(u,v) = f(u, v\alpha_2)$. *Then G preserves h, h is nondegenerate, and* $\mathrm{sym}(h) = -\mathrm{sym}(f)$. *For* $a, b \in A$, $u, v \in V_1$, $f(ua, vb) = h(u,v)\,g(a,b)$.

Proof. Let $\alpha = \alpha_2$ and $u, v \in V_1$, $b \in F$. Then $V_1(1 + b\alpha) \in \mathrm{Irr}(G,V)$, so $O = f(u + bu\alpha, v + bv\alpha) = b^\theta f(u, v\alpha) + bf(u\alpha, v)$. Since we can choose u and v with $f(u, v\alpha) \neq 0$, we conclude $b = b^\theta$ for all $b \in F$ and $f(u, v\alpha) = -f(u\alpha, v)$ for all u, $v \in V_1$. The first remark implies (1) and the second shows $f(u, v\alpha) = -\mathrm{sym}(f) f(v, u\alpha)$.

Notice (3) is trivial and (2) is trivial when $m=2$. Assume for the moment that (2) holds when $m>2$. Then $f(u\alpha_{2i-1}, v\alpha_{2i}) = f(u, v\alpha)$. Further proceeding as in 10.1, $f(ua, vc) = f(u, v\alpha)\,g(a,c)$ for a, $c \in A$. So (4) holds by 9.2.5. Thus (4) holds under our assumption that (2) is satisfied for $m>2$.

In particular (4) holds when $m=2$, so even when $m>2$, $Sp_2(F) \leqq C_{O(V_1,f)}(G)$. This implies $C_0(G)$ is transitive on the set P of pairs (I,J) in $\mathrm{Irr}(G,V) \times \mathrm{Irr}(G,V)$ with $J \nleqq I^\perp$. For example if $(I,J) \in P$ then $C_{O(I+J)}(G)$ maps I to J, while if $K \in \mathrm{Irr}(G,V)$ with $K \leqq I^\perp$, there exists $J \in \mathrm{Irr}(G,V)$ with (I,J) and (K,J) in P, so $\langle C_{O(I+J)}(G), C_{O(K+J)}(G)\rangle$ maps I to K. Next if $(I, J_i) \in P$, $i=1,2$, then either $I + J_1 = I + J_2$ or $W = I + J_1 + J_2$ can be writen $I + J_i + J_0$ for $i=1$ and 2 and some $J_0 \in \mathrm{Irr}\langle G, W\rangle$ with $W \leqq J_0^\perp$. In the first case $Sp(I+J_1) \cap N(I) \leqq C(G)$ maps J_1 to J_2. In the second let $X_i = C_{O(I+J_i)}(G)$ and $X = \langle X_1, X_2\rangle$. Then $N_{X_1}(I)$ maps $J_1 + J_0$ to $J_2 + J_0$, so without loss $J_1 + J_0 = J_2 + J_0$. Further $O_p(X)$ induces the group of transvections with center J_0 on W and hence the subgroup of $O_p(X)$ with axis $J_0 + I$ maps J_1 to J_2.

We have shown that even when $m>2$, $C_0(G)$ is transitive on P, so we can pick $\beta_i \in C_0(G)$ with $(V_1, V_2)\beta = (V_{2i-1}, V_{2i})$, and choose $\alpha_{2i-1} = \beta_{|V_1}$ and $\alpha_{2i} = \alpha\beta_i$. Hence (2), (3) and (4) are established.

Define h as in (5); evidently $h \in L_G(V_1, V_1)$. We observed earlier that $f(u, v\alpha) = -\mathrm{sym}(f) f(v, u\alpha)$, so $h(u,v) = -\mathrm{sym}(f)\,h(v,u)$. The check of the last statement of (5) goes just as in 10.1.

(10.3) *Assume* $G \leqq 0$ *acts homogeneously but not irreducibly on V, and not as a group of scalars. Assume* $N_\Gamma(G)$ *acts irreducibly on V and each member of* $\mathrm{Irr}(G,V)$ *is an absolutely irreducible FG-module. Then there exists a family* $\mathscr{D} = ((V_1, f_1), (V_2, f_2))$ *of F-spaces such that* (V,f) *is FG-isometric to* $(V_1 \otimes V_2, f_1 \otimes f_2)$ *and* $N_\Gamma(G) \leqq \Gamma(\mathscr{D})\pi$ *in the notation of* 9.2. *Moreover either f,* f_1, *and* f_2 *are unitary or the following holds:*

(1) *f,* f_1 *and* f_2 *are orthogonal or symplectic (but not necessarily all of the same type).*

(2) $\mathrm{sym}(f) = \mathrm{sym}(f_1)\,\mathrm{sym}(f_2)$.

(3) *If* $p=2$ *and* (V,Q) *is orthogonal then* $\mathrm{sgn}(Q) = +1$ *and* $\Gamma(\mathscr{D})\pi \leqq \Gamma(V,Q)$.

(4) *If* $p=2$ *and* (V,f) *is symplectic then* $\Gamma(\mathscr{D})\pi \leqq \Gamma(V,Q) < \Gamma$, *for some quadratic form Q on V.*

(5) *If p is odd and f is orthogonal, then one of the following holds:*

(i) $\dim(V)$ *is even and* $\operatorname{sgn}(f)=+1$.

(ii) *For some* $i\in\{1,2\}$, $\dim(V_i)$ *and* $\dim(V)$ *are even*, $\operatorname{sym}(f_1)=\operatorname{sym}(f_2)=+1$, $\dim(V_{3-i})$ *is odd, and* $\operatorname{sgn}(f_i)=\operatorname{sgn}(f)=-1$.

(iii) *f, f_1, and f_2 are orthogonal and V, V_1, and V_2 are of odd dimension.*

Proof. By 5.2 and 5.3 the hypothesis of 10.1 or 10.2 is satisfied. Let V_1 be the subspace supplied in 10.1 or 10.2, let $f_1=f_{|V_1}$ in 10.1, let $f_1=h$ in 10.2, and let $(V_2,f_2)=(A,g)$ in either case. By 10.1.3 and 10.2.5, the map $va\mapsto v\otimes a$ defines an isometry of (V,f) with $(V_1\otimes V_2, f_1\otimes f_2)$ and by 3.13.3 and 9.2.5, $N_\Gamma(G)\leqq\Gamma(\mathscr{D})\pi$.

By construction f_1 and f_2 are unitary if f is unitary, while if f is orthogonal or symplectic then f_1 and f_2 are both nondegenerate and each is symmetric or skew symmetric. We may assume f is bilinear. Then by 9.1.2, $\operatorname{sym}(f)=\operatorname{sym}(f_1)\operatorname{sym}(f_2)$. If $p=2$ then by 9.2.4, $\Gamma(\mathscr{D})\pi$ preserves a quadratic form Q on V whose associated bilinear form is f, and by 9.5, Q is of sign $+1$. Hence (4) holds and (3) follows from 4.9. Part (5) follows from 9.7, 9.9, and 9.10.

In the next lemma we use the following terminology: Let $\pi_i\colon G_i\to\operatorname{Aut}(X_i)$, $i=1,2$, be representations. We say π_1 is *quasiequivalent* to π_2 if there exists an isomorphism $\alpha\colon G_1\to G_2$ such that π_1 is equivalent to $\alpha\pi_2$ as representations of G_1.

(10.4) *Let $G\leqq 0$ be the product of components L_i, $1\leqq i\leqq m$. Assume V is an absolutely irreducible FG-module, $V_i\in\operatorname{Irr}(L_i,V)$, $1\leqq i\leqq m$, and for each i,j, the representation of L_i on V_i is quasiequivalent to that of L_j on V_j in the category of F-spaces and semilinear maps. Then there exist forms f_i on V_i, a family $\mathscr{D}=((V_i,f_i)\colon 1\leqq i\leqq m)$ of spaces, and a family $\mathscr{F}=(\alpha_i\colon 1\leqq i\leqq m)$ of similarities $\alpha_i\colon(V_1,f_1)\to(V_i,f_i)$ such that (V,f) is FG-isometric to $(V_1\otimes\ldots\otimes V_m, f_1\otimes\ldots\otimes f_m)$ and $N_\Gamma(G)\leqq\Lambda(\mathscr{D},\mathscr{F})\pi$. Moreover either f and f_1 are unitary, or*

(1) *f and f_1 are orthogonal or symmetric.*

(2) $\operatorname{sym}(f)=\operatorname{sym}(f_1)^m$.

(3) *If $p=2$ and (V,Q) is orthogonal then* $\operatorname{sgn}(Q)=+1$ *and* $\Lambda(\mathscr{D},\mathscr{F})\pi\leqq\Gamma(V,Q)$.

(4) *If $p=2$ and (V,f) is symplectic then $\Lambda(\mathscr{D},\mathscr{F})\pi\leqq\Gamma(V,Q)<\Gamma(V,f)$, for some quadratic form Q on V.*

(5) *If p is odd and f is orthogonal then either*

(i) $\dim(V)$ *is even and* $\operatorname{sgn}(f)=+1$, *or*

(ii) $\dim(V)$ *and* $\dim(V_1)$ *are odd and f_1 is orthogonal.*

Proof. Let $\mathscr{B}=(V_i\colon 1\leqq i\leqq m)$. By 3.17, V is FG-isomorphic to $V_1\otimes\ldots\otimes V_m$ and $N_\Gamma(G)\leqq\Lambda(\mathscr{B},\mathscr{F})\pi$, for some family $\mathscr{F}=(\alpha_i\colon 1\leqq i\leqq m)$ of isomorphisms. Let $L=L_1$ and $M=\langle L_i\colon 1\leqq i\leqq m\rangle$. Then LM is irreducible on V and by 3.16, V_1 is an absolutely irreducible FL-module, so by 10.3 there exist forms f_1 on V_1 and g on $U=V_2\otimes\ldots\otimes V_m$ such that (V,f) is FG-isometric to $(V_1\otimes U, f_1\otimes g)$. By induction on m there exist forms f_i on V_i, $1<i\leqq m$, such that (U,g) is FG-isometric to $(U,f_2\otimes\ldots\otimes f_m)$. So (V,f) is FG-isometric to $(V_1\otimes\ldots\otimes V_m, f_1\otimes\ldots\otimes f_m)$. By 4.10, we may choose the maps α_i to be similarities.

By 9.2.5, $\Gamma \cap \Lambda(\mathscr{B}, \mathscr{F})\pi = \Lambda(\mathscr{D}, \mathscr{F})\pi$, so $N_\Gamma(G) \leqq \Lambda(\mathscr{D}, \mathscr{F})\pi$. The remaining remarks in the lemma follow from 9.2, 10.3, and induction on m.

(10.5) *Let $\pi, \sigma: G \to 0$ be representations and assume $\alpha \in GL(V)$ is an equivalence of π and σ as FG-representations. Assume V is an irreducible FG-module and let $K = \mathrm{Hom}_{FG}(V, V)$. Then*

(1) *If V is an absolutely irreducible FG-module then $\alpha \in \Delta$.*

(2) *There exists an FG-equivalence $\gamma \in 0$ of π and σ unless p is odd and (V, f) is orthogonal or symplectic. Even then we can choose $\gamma \in \Delta$ to be an FG-equivalence unless also $|K:F|$ and $\dim_K(V)$ are even.*

(3) *In the last case of (2), if $G = O(V, g, K)$ for some orthogonal or symplectic K-form g on V, then there exists $\gamma \in 0$ which is an FG-quasiequivalence of π and σ.*

Proof. As α is an FG-equivalence of π and σ, $\alpha(x\sigma) = (x\pi)\alpha$ for all $x \in G$. Let $h = (\alpha, \alpha)(f)$. Then $h(u(x\pi), v(x\pi)) = f(u(x\pi)\alpha, v(x\pi)\alpha) = f(u\alpha(x\sigma), v\alpha(x\sigma)) = f(u\alpha, v\alpha) = h(u, v)$, so $G\pi \leqq O(V, h)$. Hence by 4.7, $h = \tau(f)$ for some $\tau \in K^\#$. In particular if $K = F$ then α is a similarity. Thus (1) is established.

By 7.6 there exists $\beta \in \mathrm{Hom}_F(K, F)^\#$ and a K-form g on V preserved by G such that $g\beta = f$, while by 7.5 the map $a \to (a(g))\beta$ is a bijection between K and the F-forms on V preserved by G. So $h = (a(g))\beta$ for some $a \in K^\#$.

Let $b \in K^\#$. Then $\gamma = b\alpha$ is also an FG-equivalence of π with σ. Let $\theta = 1$ if g is bilinear and θ the automorphism of K of order 2 if g is unitary. Then $(\gamma, \gamma)(f)(u, v) = (\alpha, \alpha)(f)(ub, vb) = (ag(ub, vb))\beta = (ab^{1+\theta} g(u, v))\beta$. Now if θ is an involution then by 7.6 either $|K:F|$ is even and f is symmetric or $|K:F|$ is odd and f is unitary. In either case by 7.5, a is in the fixed field of θ, so there exists $b \in K^\#$ with $a^{-1} = b^{1+\theta}$. Hence $(\gamma, \gamma)(f)(u, v) = g(u, v)\beta = f(u, v)$, so γ is an isometry. Thus we may take $\theta = 1$. Similarly we may assume a is a nonresidue in K, so p is odd. If $|K:F|$ is odd there is a nonresidue c in K with $c \in F$. Then we may choose $b \in K^\#$ with $b^2 = a^{-1}c$, so $(\gamma, \gamma)(f)(u, v) = (cg(u, v))\beta = c(g(u, v)\beta) = cf(u, v)$, and hence γ is a similarity. So take $|K:F|$ even. If $\dim_K(V)$ is odd then by 7.3.2 and 7.5 there is $d \in K^\#$ with $\mathrm{sgn}(f) \neq \mathrm{sgn}(d(g)\beta)$. We have shown that if e is a residue in K then $(e(g))\beta$ is similar to f, so d is a nonresidue, and then as a is also a nonresidue, we have $\mathrm{sgn}(f) \neq \mathrm{sgn}(h)$. This is impossible as α defines an equivalence of f and h as F-forms. Hence $\dim_K(V)$ is even, so (2) is established and we may assume $G = O(V, j, K)$ for some K-form j. Then j is similar to g by 4.7, so G is also $O(V, g, K)$. Now there exists $t \in \Delta(V, g, K)$ with $(t, t)(g) = a^{-1} g$. Then $t \in N(G)$ so $\gamma = t\alpha$ is a quasiequivalence of π and σ as FG-representations and $\gamma \in 0$.

Section 11. The proofs of Theorem A and Theorem Γ

In this section F is a finite field of characteristic p, V is an n-dimensional vector space over F, and f is an F-form on V satisfying one of the four cases I–IV of section 1 with Q the quadratic form on V in case III. Let $\Gamma = \Gamma(V, f)$, except in case III where $\Gamma = \Gamma(V, Q)$. Similarly $\Delta = \Delta(V, f)$ or $\Delta(V, Q)$, $O = O(V, f)$ or $O(V, Q)$, and $\Omega = \Omega(V, f)$ or $\Omega(V, Q)$ in the respective case. Assume Ω is quasisimple and let $P\Omega = \Omega/Z(\Omega)$.

(11.1) *Let* $X \leqq \mathrm{Aut}(\Omega)$ *with* $X \cap P\Omega = 1$. *Then there exists a nontrivial normal subgroup* Y *of* X *with* $1 \neq N_{P\Omega}(Y) \neq P\Omega$.

Proof. Let $A = \mathrm{Aut}(\Omega)$. Then X is isomorphic to a subgroup of $A/P\Omega = \mathrm{Out}(\Omega)$ so either X has a normal subgroup Y of prime order or $P\Omega \cong P\Omega_8^+(q)$, q odd, and X has a normal subgroup $Y \cong E_4$. In the first case by a result of Thompson, $C_{P\Omega}(Y) \neq 1$, and in the second this certainly holds as $P\Omega_8^+(q)$ is of even order.

The next result is the principle one in this section.

Theorem $\boldsymbol{\Gamma}$. *Let* $H \leqq \Gamma$ *with* $\Omega \nleqq H$. *Then either* H *is contained in some member of* C, *or the following hold:*

(1) $F^*(H) = LZ$ *where* Z *induces scalars on* V, L *is quasisimple, and* $Z = C_H(L)$.

(2) V *is an absolutely irreducible* FL*-module defined over no proper subfield of* F.

(3) *If* $a \in \mathrm{Aut}(F)$, V^* *is the dual of* V, *and* V *is* FL*-isomorphic to* V^{*a}, *then either*

(i) $a = 1$ *and case* II *or* III *holds, or*

(ii) a *is an involution and case* IV *holds.*

Notice that Theorem Γ implies the Main Theorem for groups G contained in $P\Gamma$. We prove Theorem A at the same time we prove Theorem Γ.

During the rest of this section assume H is a counter example to Theorem Γ, or some member of C does not satisfy Theorem A. We may assume H contains the group of scalars and by 11.1 we may assume:

(11.2) $H \cap \Omega \nleqq Z(\Omega)$.

As H is contained in no member of C_1 or C_2 we conclude:

(11.3) *H acts irreducibly on V.*

By 11.2 the set $\mathscr{L}(H)$ of normal subgroups L of H such that $L \leqq 0$ but $L \nleqq C(\Omega)$ is nonempty. Throughout this section let $L \in \mathscr{L}(H)$. As H is contained in no member of C_2, and as H is contained in no member of C_8 in case II when $p = 2$ and $n = 4$, we conclude from 5.5 and 5.6 that:

(11.4) *V is a homogeneous FL-module.*

(11.5) *Each member of* $\mathrm{Irr}(L, V)$ *is an absolutely irreducible* FL*-module. Moreover the members of* C_3 *satisfy Theorem A.*

Proof. The final remark follows from 3.14, 7.6, 7.7, and 7.8. Let $K = \mathrm{Hom}_{FL}(I, I)$ for $I \in \mathrm{Irr}(L, V)$, and suppose $K \neq F$. We saw in 5.7 that we can identify $K^\#$ with $Z(C_{GL(V)}(L))$ and $H \leqq N_\Gamma(L) \leqq N_\Gamma(K)$. Thus $N_\Gamma(K)$ is irreducible on V and by 11.4 we may assume $C_0(K)$ is homogeneous on V, so 5.7 implies $C_0(K)$ is irreducible on V. Hence if $F \leqq k \leqq K$ with $|k:F|$ prime then $C_0(k)$ is irreducible on V, so $H \leqq N_\Gamma(k) \in C_3$, completing the proof of the lemma.

(11.6) *V is an absolutely irreducible FL-module. Further the members of C_4 satisfy Theorem A.*

Proof. The second remark follows from 3.13, 9.2 and 10.3, while the first remark follows from those lemmas together with 11.3 and 11.5 and the fact that H is contained in no member of C_4, C_7, or C_8. Notice that if case II holds with $p=2$ then by 10.3.4 H is contained in a member of C_8, so the exclusion of case II for $p=2$ in the definition of C_4 causes no problems.

(11.7) *The representation of L on V is defined over no proper subfield of F. The members of C_5 satisfy Theorem A.*

Proof. The second remark is a consequence of 3.15, 8.1, and 8.2, while the first remark follows from these lemmas and 11.6.

(11.8) *No member of $\mathscr{L}(H)$ is solvable. Further the members of C_6 satisfy Theorem A.*

Proof. Assume L is minimal subject to $L\in\mathscr{L}(H)$ and L solvable. Then L is an r-group for some prime r. As L is irreducible on V, $r\neq p$ and $Z(L)$ induces scalars on V. By minimality of L, $Z(L)$ is the unique maximal abelian characteristic subgroup of L, so L is of symplectic type. Then by a result of Phillip Hall and minimality of L, either r is odd and L is extraspecial of exponent r, or $r=2$ and $L=Z(L)*L_0$ with L_0 extraspecial, and L is of exponent 4.

As $Z(L)$ induces scalars on V, $q\equiv 1 \bmod s$, where $s=|Z(L)|$. Hence F is a splitting field for L and L has $r-1$ faithful irreducible representations over F indexed by the action of a generator z of $Z(L)$, unless $Z(L)$ is of order 4, where L has two such representations. Now the field of definition of these representations is of order p^e where e is the order of p in the group of units of Z_s. Thus $|F|=p^e$ by 11.7.

As the faithful irreducible representations are indexed by the eigenvalue of z, $C_{\mathrm{Aut}(L)}(z)$ is the stabilizer in $\mathrm{Aut}(L)$ of the representation of L on V. So in case I, $\mathrm{Aut}_{GL(V)}(L)\cong C_{\mathrm{Aut}(L)}(z)$ by 2.5. Indeed by 4.7 and 4.9 each form on V preserved by L is similar to f, so even in the remaining cases $\mathrm{Aut}_{\Delta}(L)\cong C_{\mathrm{Aut}(L)}(z)$ by 2.5. Notice these remarks establish that Theorem A holds for the members of C_6.

The faithful irreducibles for L are of degree r^m, where $|L:Z(L)|=r^{2m}$. So $n=r^m$. In particular if n is even then $r=2$.

By 4.7 and 4.8, L preserves a symplectic or orthogonal form on V if and only if V is LF-isomorphic to V^*, while L preserves a unitary form if and only if e is even and V is FL-isomorphic to $V^{*\theta}$, where θ is the automorphism of F of order 2. Now if τ is the eigenvalue of z on V then τ^{-1} and τ^{-q} are the eigenvalues of z on V^* and $V^{*\theta}$, respectively, where $|F|=q^2$ in the latter case. Hence L preserves a symplectic or orthogonal form if and only if $s=2$, and L preserves a unitary form if and only if e is even, since e is the order of p in the group of units of Z_s.

Assume $s>2$. We have shown that f is trivial or e is even and f is unitary. Indeed if e is even then L preserves a unitary form g on V, so if f is trivial then $L\leqq\Gamma(V,g)<\Gamma=\Gamma(V)$. Further we have shown that $\mathrm{Aut}_{\Gamma(V,g)}(L)\cong\mathrm{Aut}_{\Gamma}(L)$, so $H\leqq N_{\Gamma}(L)\leqq\Gamma(V,g)\in C_8$. On the other hand if e is odd or e is even and f is unitary then $H\leqq N_{\Gamma}(L)\in C_6$.

So take $s=2$. Thus p is odd and $e=1$, so F is of order p. Moreover we showed that L preserves an orthogonal or symplectic form on V, so an argument in the last paragraph shows case II or III holds. Now $L \cong D_8^{m-1} Q_8$ or D_8^m, and it remains to show case II holds if $L \cong D_8^{m-1} Q_8$ while case III holds with $\mathrm{sgn}(f) = +1$ if $L \cong D_8^m$, since then $H \leqq N_\Gamma(L) \in C_6$.

Notice $Q_8 \leqq Sp_2(p) \cong SL_2(p)$, so Q_8 preserves a symplectic form f_1 on V_1 of dimension 2, while $D_8 \leqq O_2^\varepsilon(p)$ for $\varepsilon = +1$ or -1. Then proceeding by induction on m, there are spaces V_2 and V_3 of dimension 2^{m-1} with forms f_2 and f_3 such that f_2 is symplectic and preserved by $D_8^{m-2} Q_8$ and f_3 is orthogonal and preserved by D_8^{m-1}. Hence by 9.7 and 9.1.2, $D_8^m = D_8^{m-2} Q_8^2 \leqq O(V_1 \otimes V_2, f_1 \otimes f_2)$ with $f_1 \otimes f_2$ orthogonal of sign $+1$ and $D_8^{m-1} Q_8 \leqq O(V_1 \otimes V_3, f_1 \otimes f_3)$ with $f_1 \otimes f_3$ symplectic.

(11.9) *$F^*(H) = E(H) Z$ where $Z = C_H(E(H))$ induces a group of scalars on V, and H is transitive on its components.*

Proof. Let $Z_0 = O_\infty(H \cap O)$. By 11.8, Z_0 induces a group of scalars on V. So as $\mathscr{L}(H)$ is nonempty there exists a component X of $O \cap H$. Then $L = \langle X^H \rangle \in \mathscr{L}(H)$, so by 11.6, V is an absolutely irreducible FL-module, and then by 11.7 and 3.8.2, V is an irreducible KL-module, where K is the prime subfield. But $\Gamma(V, F) \leqq GL(V, K)$, so $C_H(L) \leqq \mathrm{Hom}_{KL}(V, V) = F$. Thus $C_H(L)$ induces scalars on V and $E(H) = L$, so the lemma holds.

(11.10) *$E(H)$ is quasisimple. The members of C_7 satisfy Theorem A.*

Proof. The second remark is a consequence of 3.17, 9.2, and 10.4, while the first remark is a consequence of these lemmas, 11.6 and 11.9.

(11.11) *Let $L = E(H)$ and suppose $a \in \mathrm{Aut}(F)$ with V FL-isomorphic to V^{*a}. Then either*

(1) *$a = 1$ and case* II *or* III *holds, or*

(2) *a is an involution and case* IV *holds.*

Proof. As $V \cong V^{*a}$, also $V \cong V^{a^2}$, so by 11.7 and 3.6 we have $a^2 = 1$. Thus either $a = 1$ or a is an involution. So by 4.7 and 4.8, L preserves a form g on V with g symplectic or orthogonal if $a = 1$ and with g unitary if a is an involution. If f is nontrivial then by 4.7 and 4.8, f is similar to g, so that the lemma holds. So assume case I holds. Observe $M = \Gamma(V, g) \in C_8$, so it suffices to show $H \leqq M$.

Let $h \in H$ and define $g'\colon V \times V \to F$ by $g'(u, v) = g(uh, vh)^{\sigma(h)^{-1}}$. It is straightforward to check that g' is a form on V preserved by L, so by 4.7 g' is similar to g. Hence there is $\tau \in F^\#$ with $g(uh, vh) = \tau g(u, v)^{\sigma(h)}$; that is $h \in M$.

Notice that we have now established Theorem Γ and Theorem A.

Section 12. The proof of Theorem *B*

In this section we continue to assume the hypothesis and notation established in the first paragraph of Sect. 11. Our object is to establish Theorem B, which describes the action of various subgroups of Γ on C.

We first establish Theorem $B\Delta$. The action of Δ on C_1 and C_2 follows from Witt's lemma, and from 5.4 in case $(C_2 3)$. In the remaining cases each $H \in C_i$ is of the form $H = N_\Gamma(L)$ for some $L \leqq \Omega$ with $L \nleqq Z(\Omega)$ and L irreducible on V. L will continue to have this meaning throughout this section. Now either V is an absolutely irreducible FL-module or $H \in C_3$ and $L = O(V, g, K)$ for some K-form g on V, where $K = \mathrm{Hom}_{FL}(V, V)$. So by 2.4 and 10.5, the Δ-conjugacy class of H is determined by the quasiequivalence class of the F-representation of L on V. On the other hand the parameters in the statement of Theorem $B\Delta$ determine this quasiequivalence class, completing the proof of Theorem $B\Delta$.

We next prove Theorem $B\Gamma$. Observe that if $x \in \Gamma$ and U is a subspace of V then Ux is similar to U, and indeed in case III if n is odd then Ux is isometric to U. These remarks follow from a straightforward calculation. Hence, from Theorem $B\Delta$, the orbits of Δ and Γ on C_1 and C_2 are the same. If $H \in C_i$ for $i > 2$, then $H = N_\Gamma(L)$, where L was defined earlier. To complete the proof in this case we observe that if $\alpha \in \mathrm{Aut}(F)$, then V^α is quasiequivalent to V as an FL-module, so 2.4 and 2.6 establish Theorem $B\Gamma$. The observation can be seen as follows: Let π and π' be the representations of L on V and V^α; then $\pi' = \beta\pi$ for a suitable field automorphism β of L.

Now the proof of Theorem BO. By 6.2–6.4, either $\Delta = OZ(\Delta)$ or p is odd, n is even, and case II or III holds. In the first case clearly $M^0 = M^\Delta$, so we may assume the second holds. As $OZ(\Delta)$ is a normal subgroup of Δ of index 2 and $Z(\Delta) \leqq M$, $M^0 \neq M^\Delta$ if and only if $M \cap \Delta = M \cap 0$, in which case M^Δ splits into two O-orbits of equal length. It remains to check when $M \cap \Delta \leqq 0$. For the most part this is straightforward and the details are omitted; the case when $M \in C_6$ and $r = 2$ is somewhat more complicated, so we sketch a proof in that case. $M = N_\Gamma(L)$, where L is an extraspecial 2-group of width m, $n = 2^m$, and $p = |F|$. We show O is transitive on M^Δ if $p \equiv \pm 3 \bmod 8$ but not if $p \equiv \pm 1 \bmod 8$. Let t be a noncentral involution of L. Then $M/Z(L) \cong \mathrm{Aut}(L) \cong O^\varepsilon_{2m}(2)/E_{2^{2m}}$ and $V = C_V(t) \perp [V, t]$ with $C_M(t)/C_M(\langle t, U\rangle)$ acting as $O^\varepsilon_{2m-2}(2)/2^{1+2(m-1)}$ on $U = C_V(t)$. Notice there exists $x \in M - 0$ if and only if there is $x \in C_M(t) - 0$, since $N_M(\langle Z(L), t\rangle)$ contains a Sylow 2-group of M and $N_M(\langle Z(L), t\rangle) = C_M(t)L$ with $L \leqq 0$. Moreover $x \in C_M(t) - 0$ if and only if $x_{|U} \in A - O(U, f)$, where $A = C_M(t)/C_M(\langle t, U\rangle)$. For $m = 2$ such an element exists if and only if $p \equiv \pm 3 \bmod 8$, so the result holds by induction on m. This completes the proof of Theorem BO.

Finally the proof of Theorem $B\Omega$. Part (1) of the theorem follows as $\Omega \trianglelefteq 0$. The remaining parts follow from the observation that $d(M)$ divides $|0 : \Omega C_0(\Omega)|$.

Section 13. Aut $(L_n(q))$

In this section F is a finite field of characteristic p and V is an n-dimensional vector space over F, $n > 2$. Let A be the split extension of $\Gamma(V) = \Gamma$ by the transpose inverse map. Let $\Omega = \Omega(V)$ and $\Delta = GL(V)$. Then $\Omega/Z(\Omega) \cong L_n(q)$ and $A/Z(\Delta) \cong \mathrm{Aut}(L_n(q))$.

Let Λ consist of the pairs of subspaces (U, W) of V such that $n = \dim(U) + \dim(W)$, $0 < \dim(U) \leqq \dim(W) < n$, and either $U \leqq W$ or $V = U \otimes W$. Let C'_1 consist of the stabilizers $N_\Gamma(\{U, W\})$, $(U, W) \in \Lambda$, and for $i > 1$ let $C'_i = C_i$. Finally let $\mathscr{C}_A$ consist of the groups $N_A(M)$, $M \in \bigcup_i C'_i$. We prove:

(13.1) **Theorem.** *Let $H \leqq A$ with $\Omega \nleqq H$ and $A = H\Gamma$. Then either*

(1) *H is contained in some member of* $\mathscr{C}_A$, *or*

(2) $F^*(H)=E(H)\,C_H(F^*(H))$, $C_H(F^*(H))$ *induces a group of scalars on V,* $E(H)$ *is quasisimple, V is an absolutely irreducible* $FE(H)$*-module, and the representation of* $E(H)$ *on V is defined over no proper subfield of F. V is not* $FE(H)$*-isomorphic to* V^{*a} *for any* $a\in \mathrm{Aut}(F)$.

We also prove:

(13.2) (1) *Let* $M\in C_i'$. *Then* $M^A=M^\Delta$, *so* $A=\Delta N_A(M)$.

(2) *Members* (U,W) *and* (U',W') *of* Λ *are conjugate under* Δ *if and only if* $\dim(U)=\dim(U')$ *and* $\dim(U\cap W)=\dim(U'\cap W')$.

Lemma 13.2 gives us the action of A and Δ on $\mathscr{C}_A$. If $L_n(q)\leqq G\leqq \mathrm{Aut}(L_n(q))$ with $L_n(q)\nleqq G\nleqq \Gamma L_n(q)$ then $G=HZ(\Delta)/Z(\Delta)$ for some $H\leqq A$ satisfying the hypothesis of Theorem 13.1, and we let $\mathscr{C}_G$ consist of the groups $MZ(\Delta)/Z(\Delta)\cap G$. Then by Theorem 13.1, the Main Theorem holds for G.

Pick a basis $X=\{x_1,\dots,x_n\}$ for V and let V^* be the dual space of V (as a Γ-module) and $X^*=\{x_1^*,\dots,x_n^*\}$ the dual basis of X. Form the space $V\otimes V^*$ and let $d\in GL(V\oplus V^*)$ be the map interchanging x_i and x_i^*, $1\leqq i\leqq n$. Then we may take $A=\langle d,\Gamma\rangle\leqq\Gamma(V\oplus V^*)$ and d induces the transpose inverse map on Γ.

For $U\leqq V$ define
$$U\varphi=\{\alpha\in V^*\colon U\leqq \ker(\alpha)\}$$
and observe that:

(13.3) φ *defines a bijection between the projective spaces of V and* V^* *which reverses inclusion, and with* $\dim(U\varphi)=n-\dim(U)$.

We next establish 13.2. Let $M\in C_i'$. If $i>2$ then $M=N_\Gamma(L)$ for some $L\leqq\Delta$ with L irreducible on V. Let π and π^* be the representations of L on V and V^*, respectively. Recall from Sect. 2 that for $g\in L$, $g\pi^*d^*=(g\pi^*)^d$. By construction π^*, and then also $\pi^*\mathrm{d}^*$, is the dual of π. From the structure of the representations of the members of C_i', $i>2$, π is quasiequivalent to its dual as an FL-representation. Hence by 2.4, $L^d=L\pi^*d^*\in L^\Delta$, so $M^d=N_\Gamma(L^d)\in M^\Delta$.

Next let $i=2$. Then M is the stabilizer of some collection $P=U^M$ of subspaces of V with $V=\bigoplus_{W\in P}W$. For $W\in P$ let $D(W)=\langle P-\{W\}\rangle$. M is also the stabilizer of $Q=\{D(W)\colon W\in P\}$ and hence also of $Q\varphi$. Hence for $a\in A-\Gamma$, M^a is the stabilizer of $Q\varphi a$. However $V=\bigoplus_{Z\in Q\varphi a}Z$ with $\dim(Z)=\dim(U)$ for each $Z\in Q\varphi a$, so as Δ is transitive on such collections, $M^a\in M^\Delta$.

Observe that 13.2.2 is trivial. Finally let $i=1$. Then $M=N_\Gamma(P)$, $P=\{U,W\}$, $(U,W)\in\Lambda$, so for $a\in A-\Gamma$, $M^a=N_\Gamma(P\varphi a)$, with $(W\varphi a,U\varphi a)\in\Lambda$, $\dim(W\varphi a)=\dim(U)$, and $\dim(W\varphi a\cap U\varphi a)=\dim(U\cap W)$. Hence $M^a\in M^\Delta$, and the proof of Lemma 13.2 is complete.

We now establish Theorem 13.1. Let H be a counter example with $|A:H|$ minimal. By 11.1, $H\cap\Omega\nleqq Z(\Omega)$, so the set $\mathscr{L}(H)$ of normal subgroups L of H with $L\leqq\Delta$ but $L\nleqq Z(\Delta)$ is nonempty. Let $L\in\mathscr{L}(H)$. We next prove:

(13.4) $H\cap\Gamma$ *is irreducible on V.*

For assume otherwise and let U be a minimal nontrivial $H\cap\Gamma$-invariant subspace of V. Then $W=U\varphi a$ is $H\cap\Gamma$-invariant for $a\in H-\Gamma$ so by minimality of U either $U \leqq W$ or $U \cap W = 0$. Thus $(U, W) \in \Lambda$ and $H \leqq N_A(\{U, W\}) \in \mathscr{C}_A$, contrary to the choice of H. Thus 13.4 is established

(13.5) *V is a homogeneous FL-module.*

Proof. Assume otherwise and let $P = (V_i : 1 \leqq i \leqq r)$ be the homogeneous components of L on V, with $r > 1$. By minimality of $|A:H|$, $H = N_A(L)$. $H \cap \Gamma \leqq M = N_\Gamma(P) \in C_2'$, so it suffices to show that if $a \in A - \Gamma$ then $M^a = M$. Let $D = LC_\Delta(L)$. By 3.11, $P = \mathrm{Irr}(D, V)$, so P is the unique collection Q of subspaces of V fixed pointwise by D with $\dim(Z) = \dim(V_i)$ for $Z \in Q$ and $V = \bigoplus_{Z \in Q} Z$. However $M^a \in M^\Delta$ by 13.2, so $M^a = N_\Gamma(Q)$ for some such Q, (the proof of 13.2 shows D fixed Q pointwise) so by uniqueness of Q, we have $P = Q$ and hence $M = M^a$.

(13.6) *V is an absolutely irreducible FL-module.*

Proof. Let $I \in \mathrm{Irr}(L, V)$ and $K = \mathrm{Hom}_{FL}(I, I)$. By 3.11 we may identify K with $Z(C_\Delta(L))$. Hence $H \leqq N_A(K)$ and if $K \neq F$ then $N_A(K) \in \mathscr{C}_A$, contrary to the choice of H.

So I is an absolutely irreducible FL-module. Suppose $I \neq V$. By minimality of $|A:H|$, $D = C_\Delta(L) \trianglelefteq H$. But $N_\Gamma(D) \in C_4$ unless $n = \dim(I)^2$, where by minimality of $|A:H|$, we may take $L = C_\Delta(D)$ and $H \leqq N_A(LD)$ with $N_\Gamma(LD) \in C_7$. In either case the choice of H as a counter example to Theorem 13.1 is contradicted.

(13.7) *The representation of L on V is defined over no proper subfield of F.*

Proof. We may assume the representation is defined over a subfield K of F of prime index r. Then $L \leqq M \in C_5$ with $M = N_\Gamma(\mathrm{Irr}(L, V, K))$. Moreover if P is the set of proper KL-submodules U of V with L irreducible on V/U, then for $a \in H - \Gamma$, $P\varphi a = \mathrm{Irr}(L, V, K)$ is preserved by M^a so $M = M^a$. Thus $H \leqq N_A(M) \in \mathscr{C}_A$, contrary to the choice of H.

(13.8) *No member of $\mathscr{L}(H)$ is solvable.*

Proof. If not, 13.6, 13.7, and the proof of 11.8 show there is a prime $r \neq p$ and an r-group $L \in \mathscr{L}(H)$ of symplectic type such that either $N_\Gamma(L) \in C_6$ or $N_\Gamma(L) \leqq M \in C_8$ with $N_\Gamma(L) \in \mathscr{C}_M$. In the first case $H \leqq N_A(L) \in \mathscr{C}_A$, contrary to the choice of H. In the second case, by Theorem B, M is transitive on its subgroups isomorphic to L, so as $N_\Gamma(L) \leqq M$, M is the unique member of M^Γ containing L. Thus as $L \leqq M^a \in M^\Gamma$ for $a \in N_A(L)$, $H \leqq N_A(L) \leqq M$.

(13.9) *$F^*(H) = E(H)Z$ where $Z = C_H(F^*(H))$ induces a group of scalars on V and H is transitive on the components of H.*

Proof. The proof of 11.9 can be repeated almost verbatim to show that 13.9 holds, except possibly $C_H(E(H)) = Z\langle a \rangle$ where $a \in H - \Gamma$ and Z induces scalars on V. Now $a = \gamma d$, $\gamma \in \Gamma$. Let π be the representation of $L = E(H)$ on V and $\sigma = \sigma(\gamma)$. $\sigma^2 = \sigma(a^2)$ and $a^2 \in Z$, so $\sigma^2 = 1$. Further as $a \in C(L)$, π is equivalent to πa^*, (where the $*$ map is defined in Sect. 2) while $\pi a^* = \pi \gamma^* d^*$ is equivalent to the dual $\pi^{*\sigma}$ of π^σ. Hence by 4.7 and 4.8, L preserves a unitary, symplectic, or orthogonal form f on V. Let $M=\Gamma(V,f)$. Then $L\leqq M\in C_8$. Further for $h\in H$, $L\leqq M^h$ so by 4.7, $M=M^h$. Thus $H\leqq N_A(M)\in\mathscr{C}_A$, a contradiction.

(13.10) *$E(H)$ is quasisimple.*

Proof. Let S be the set of components of H, $P=\{\mathrm{Irr}(X,V): X\in S\}$ and $T=\bigcup_{X\in S}\mathrm{Irr}(X,V)$. Let M be the subgroup of Γ preserving T and the partition P of T, and assume S is of order at least 2. Then by 3.17, $H\cap\Gamma\leqq M\in C_7$. Next for $X\in S$ let $I(X,V)$ consist of the FX-submodules U of V with X irreducible on V/U, let $Q=\{I(X,V): X\in S\}$ and $R=\bigcup_{X\in S} I(X,V)$. Then for $a\in H-\Gamma$, $Q\varphi a=P$ and $R\varphi a=T$ are preserved by M^a, so $M=M^a$.

(13.11) *V is not $FE(H)$-isomorphic to V^{*a} for any automorphism a of F.*

Proof. If V is isomorphic to V^{*a}, then by 13.7, 3.8, and 3.6, $a^2=1$. Thus $L=E(H)$ preserves a unitary, symplectic or orthogonal form by 4.7 and 4.8. But then an argument in the proof of 13.9 shows H is contained in a member of $\mathscr{C}_A$.

Notice the proof of Theorem 13.1 is now complete.

Section 14. Aut($Sp_4(q)$)

In this section F is a field of order $2^e=q$ and (V,f) a 4-dimensional symplectic space over F. Let $\Omega=O(V,f)\cong Sp_4(q)$, $\Gamma=\Gamma(V,f)$, and $A=\mathrm{Aut}(\Omega)$. Then $|A:\Gamma|=2$. Let us first see how A acts on C:

(14.1) (1) *The Γ-orbits of stabilizers of points and stabilizers of totally singular lines are fused in A.*

(2) *C_2 is fused under A to the Δ-orbit of C_8 consisting of subgroups preserving a quadratic form of sign $+1$.*

(3) *C_3 is fused to the Δ-orbit of C_8 consisting of subgroups preserving a quadratic form of sign -1.*

(4) *The orbits of A and Δ on C_5 are the same.*

(5) *C_4, C_6 and C_7 are empty.*

Proof. By definition of C, C_4, C_6 and C_7 are empty. It is well known that (1) holds. Moreover if U_1 and U_2 are a point and a totally singular line of V then there exist involutions $t_i\in\Omega$ with $[t_i,V]=U_i$, so that t_1 and t_2 are fused in A.

Let $M\in C_2$. Then if $q>2$, $E(M)\cong\Omega_4^+(q)$ and we may take t_1 to be contained in a component of $E(M)$. Then for $a\in A-\Gamma$, $t_1^a\in t_2^\Omega$ is contained in a component of $E(M^a)$, so $M^a\notin M^\Omega$. But $\Omega_4^+(q)$ has just two quasiequivalence classes of faithful 4-dimensional representations, so M^a must be in the second class, and thus $M^a\in C_8$, and (2) holds. If $q=2$, $\Omega\cong S_6$ and $C_2=C_8=(N_\Omega(P))^\Delta$, for $P\in\mathrm{Syl}_3(\Omega)$.

Let $M\in C_3$. Then $E(M)\cong L_2(q^2)$ and we may take t_2 to induce an outer automorphism of $E(M)$. Again $t_2^a\in t_1^\Omega$ so $M^a\notin M^\Omega$, so as $L_2(q^2)$ has just two quasiequivalence classes of 4-dimensional representations, $C_3^a\subseteq C_8$, and (3) holds.

There is just one quasiequivalence class of 4-dimensional representations of $Sp_4(2^m)$, so (4) holds.

We can now define $\mathscr{C}_A$ to consist of the subgroups of A of the form $N_A(X)$, where X is one of the following:

$\mathscr{C}_1$: $X \in \mathrm{Syl}_2(\Omega)$.

$\mathscr{C}_2$: $q > 2$ and X is the stabilizer in $M \in C_8$ of a nondegenerate line of V, with $M = \Gamma(V, Q)$ for some quadratic form Q of sign $+1$. There are, up to conjugation in M, two such stabilizers. If $q = 2$, $X \in \mathrm{Syl}_3(\Omega)$.

$\mathscr{C}_3$: $X \cong Z_{q^2+1}$.

$\mathscr{C}_4$: $X \in C_5$.

$\mathscr{C}_5$: e is odd and X is generated by an involutory outer automorphism.

We prove:

(14.2) **Theorem.** *Let $H \leqq A$ with $E(A) \nleqq H$ and $A = H\Gamma$. Then either*

(1) *H is contained in some member of $\mathscr{C}_A$, or*

(2) *$F^*(H) = E(H)\,C_H(F^*(H))$, $C_H(F^*(H))$ induces scalars on V, $E(H)$ is simple, and V is an absolutely irreducible $FE(H)$-module defined over no proper subfield of F.*

(14.3) (1) *A is transitive on $\mathscr{C}_i$ for $i \neq 2, 4$.*

(2) *A has two orbits on $\mathscr{C}_2$ if $2^e > 2$ and one orbit if $2^e = 2$.*

(3) *A is transitive on the groups in $\mathscr{C}_4$ determined by each prime divisor r of e.*

Let us first prove 14.3. It is clear that A is transitive on $\mathscr{C}_1$, and if $q = 2$ on $\mathscr{C}_2$. 14.3.3 follows from 14.1.4 and Theorem $B\Delta$. Transitivity on $\mathscr{C}_5$ follows from 19.5 in [3]. Let r be a prime divisor of q^2+1 that does not divide $2^i - 1$ for $i < 4e$. Then $\mathscr{C}_3 = \{N_G(R)\colon R \in \mathrm{Syl}_r(\Omega)\}$, so A is transitive on $\mathscr{C}_3$. Finally let r_ε be a prime divisor of $q - \varepsilon$, $\varepsilon = \pm 1$. Then if $q > 2$, $\mathscr{C}_2 = \mathscr{C}_{2,+1} \cup \mathscr{C}_{2,-1}$, with $\mathscr{C}_{2,\varepsilon} = \{N_G(R)\colon R \in \mathrm{Syl}_{r_\varepsilon}(\Omega)\}$, so that A has two orbits on $\mathscr{C}_2$. So 14.3 is established.

We next prove Theorem 14.2. We proceed as in the last section. In particular let H be a counter example with $|A:H|$ minimal and $L \in \mathscr{L}(H)$.

(14.4) *$H \cap \Gamma$ is irrducible on V and is not contained in a member of C_2 or C_2^a, $a \in A - \Gamma$.*

Proof. Suppose $H \cap \Gamma$ stabilizes a point or totally singular line. Then by 14.1.1 it stabilizes a point U and a totally singular line $W = U^a$, $a \in H - \Gamma$. If $U \leqq W$ then $H \leqq N_A(\{U, W\}) \in \mathscr{C}_1$. So $U \nleqq W$. Now $H \cap \Gamma$ acts on the point $U_0 = U^\perp \cap W$ and on the singular line $W_0 = U + U_0$. Moreover U_0 is the unique point on W such that $U + U_0$ is totally singular, so U_0^a is the unique line through $W^a = U$ such that $U^a \cap U_0^a = W \cap U_0^a$ is a point. Hence $U_0^a = W_0$. Hence $H \leqq N_A(\{U_0, W_0\}) \in \mathscr{C}_1$.

So if $H \cap \Gamma$ is not irreducible on V then $H \cap \Gamma$ fixes a nondegenerate line U. Then $H \cap \Gamma \leqq M = N_\Gamma(\{U, U^\perp\}) \in C_2$. So in any event we may take $H \cap \Gamma \leqq M$. By 14.1.2, $M^a \in C_8$, so $H \cap \Gamma \leqq X = M \cap M^a = N_{M^a}(\{U, U^\perp\})$ with $M^a = \Gamma(V, Q)$ for some quadratic form Q of sign $+1$. $a^2 \in H \cap \Gamma \leqq M$, so $H \leqq N_A(X) \in \mathscr{C}_A$, contrary to the choice of H.

(14.5) (1) *L acts homogeneously on V.*

(2) *$H \cap \Gamma$ is not contained in a member of C_3 or C_8.*

(3) *Each member of* $\mathrm{Irr}(L, V)$ *is an absolutely irreducible FL-module.*

Proof. Part (1) follows from 14.4, 5.5, 5.6, and 14.1.2. (1), (2), 5.7, and 14.4 imply (3) so we may assume $H \cap \Gamma \leqq M \in C_3 \cup C_8$. By 14.1 and 14.4 we may assume $M \in C_3$ and $M^a \in C_8$. Then $H \cap \Gamma \leqq X = M \cap M^a$ and as $a^2 \in H \cap \Gamma \leqq M$, $H \leqq N_A(X)$. We show $O(X \cap \Omega) \cong Z_{q^2+1}$ so that $N_A(X) \in \mathscr{C}_A$, contrary to the choice of H. It suffices to show M is transitive on $M^{a\Omega}$ and $M^\infty \cap N \cong D_{2(q^2+1)}$ for some $N \in M^{a\Omega}$. But $|M^{a\Omega}| = |\Omega\colon M^a \cap \Omega| = q^2(q^2-1)/2$ and there is $Z_{q^2+1} \cong Y \leqq M^\infty$. We showed in the proof of 14.3 that Ω is transitive on subgroups isomorphic to Y, so as M^a contains such a subgroup, $Y \leqq N \in M^{a\Omega}$. Indeed $N_\Gamma(Y)$ is a maximal subgroup of M and N, so $M \cap N = N_\Gamma(Y)$, completing the proof.

(14.6) *V is an absolutely irreducible FL-module defined over no proper subfield of F.*

Proof. If V is not an irreducible FL-module, then by 14.5 and 10.3.4, $H \cap \Gamma$ is contained in a member of C_8 contrary to 14.5. So V is irreducible and then, by 14.5.3, even absolutely irreducible. Next if V is defined over a subfield K of F of prime index as an L-module, then by 8.1 and 8.2 $H \cap \Gamma$ is contained in $M \in C_5$. Let $P = \mathrm{Irr}(L, V, K)$; then $\Gamma_P \cong Sp_4(K) \times K$ is a weakly closed subgroup of M, so by 14.1.4, $\Gamma_P^a = \Gamma_Q$, where $Q = \mathrm{Irr}(E(M^a), V, K)$. Then $L = L^a \leqq \Gamma_Q$, so $Q = \mathrm{Irr}(L, V, K) = P$ and hence $a \in N_A(M)$. Thus, $A \leqq N_A(M) \in \mathscr{C}_A$, a contradiction.

(14.7) *$F^*(H) = E(H)Z$ where $E(H)$ is simple and $Z = C_H((F^*(H))$ induces scalars on V.*

Proof. 14.6 and the proof of 11.8 shows that if $\mathscr{L}(H)$ contains a solvable member, then n is a power of an odd prime. As $n=4$ this is impossible. Then the proof of 11.9 can be repeated to show either $H \cap \Gamma$ is contained in a member of C_7 or H centralizes an element a of order 2 in $A - \Gamma$. The first case is out by 14.1. In the second by 19.5 in [3], e is odd, so $H \leqq C_A(a) \in \mathscr{C}_A$, a contradiction.

Notice the proof of Theorem 14.2 is now complete.

Section 15. $\mathrm{Aut}(\Omega_8^+(q))$

In this section F is a finite field of characteristic p and order q and (V, Q) is an 8-dimensional orthogonal space over F of sign $+1$ with associated bilinear form f. Let $\Gamma = \Gamma(V, Q)$, $\Delta = \Delta(V, Q)$, $O = O(V, Q)$ and $\Omega = \Omega(V, Q)$. Let $A = \mathrm{Aut}(P\Omega)$ and B the largest subgroup of $P\Gamma$ normal in A. Recall $|A\colon P\Gamma| = 3$ and $A/B \cong S_3$. A does not act on Ω if p is odd but on its covering group, which is twice as big.

In this section we prove:

(15.1) *A has the following orbits with representatives in $\mathscr{C}_B$:*

(1) *Stabilizers of singular points and stabilizers of totally singular 4-spaces.*

(2) *Stabilizers of totally singular lines.*

(3) *Stabilizers of nonsingular points and conjugates of these stabilizers under* A *which act absolutely irreducible in the spin representation of* $\Omega_7(q)$ *or* $Sp_6(q)$, *for p odd or even, respectively.*

(4) *Stabilizers of nondegenerate lines of sign* $+1$ *and members of* $(C_2 3)$.

(5) *Stabilizers of nondegenerate lines of sign* -1 *and members of* C_3 *stabilizing a unitary form over a quadratic extension of* F.

(6) *If p is odd, stabilizers of nondegenerate* 3*-spaces and the members of* C_4 *stabilizing a family* $\mathscr{D}$ *with* f_1 *and* f_2 *symplectic,* $\dim(V_1)=2$, *and* $\dim(V_2)=4$.

(7) *The members of* C_2 *stabilizing a pair consisting of a degenerate* 4*-space of sign* $+1$ *and its orthogonal complement.*

(8) *The members of* C_2 *stabilizing a pair consisting of a nondegenerate* 4*-space of sign* -1 *and its orthogonal complement, and the members of* C_3 *stabilizing a quadratic form over a quadratic extension of* F.

(9) *The members of* C_2 *stabilizing a* 4*-tuple of nondegenerate lines of sign* $+1$. (*If* $q \leqq 3$ *this stabilizer is contained in a member of* (7) *or a parabolic, and we ignore it.*)

(10) *The members of* C_2 *stabilizing a* 4*-tuple of nondegenerate lines of sign* -1.

(11) *If* $q=p$ *is odd, the members of* C_2 *stabilizing an* 8*-tuple of nondegenerate points and members of* C_6. (*If p is odd and* $q>p$, *such members of* C_2 *are contained in members of* C_5.)

(12) *The members of* C_4, *other than those mentioned in* (6), *are contained in some member of* C_1^A, C_2, *or* C_3, *so we ignore them.*

(13) *The orbits of* A *and* Δ *on* C_5 *are the same.*

(14) *The members of* C_7 *are contained in a member of* C_1^A *or* C_2.

We use the term C_i loosely here, since we are really concerned with groups of the form $M \cap B$, where M is the image in $P\Gamma$ of a group in C_i. We sketch a proof of 15.1. Parts (1), (2), (3), and (13) are well known. Let U be a subspace of V and $H=N_B(U)$.

Suppose U is a nondegenerate line of sign $+1$. Then U contains two singular points U_1 and U_2 and $|H\colon N_H(U_1)|=2$. By (1) there is $a \in A$ with $N_B(U_1)^a$ the stabilizer of a totally singular 4-space W_1. Similarly $N_B(U_2)^a$ stabilizes a 4-space W_2 and as $f(U_1, U_2) \neq 0$, $V=W_1 \oplus W_2$. So $H^a \leqq N_B(\{W_1, W_2\}) \in C_2$, and as $H \cong N_B(\{W_1, W_2\})$, the containment is an equality, so (4) holds.

Next let U be a nondegenerate line of sign -1. Then H has a component $L \cong \Omega_6^-(q)$. Let U_1 be a point of U. By (3) there is $a \in A$ with $N_B(U_1)^a$ acting in the spin representation on V, so as $L \leqq N(U_1)$, we conclude L^a is irreducible on V since a subgroup of $\Omega_7(q)$ or $Sp_6(q)$ isomorphic to L is irreducible in the spin representation. As L centralizes an element of H of order $q+1$, $\mathrm{Hom}_{FV}(L, L)$ contains a quadratic extension of F, so we conclude (5) holds.

Assume p is odd and U is a nondegenerate 3-space. H has a component $L \cong \Omega_5(q)$ stabilizing a singular point U_1 of U, so by (1) there is $a \in A$ such that L^a acts on a totally singular 4-space W_1. We conclude L^a acts irreducible on W_1 as $Sp_4(q)$, and as L centralizes $J \cong \Omega_3(q)$ we conclude $(LJ)^a$ acts irreducibly on V, and then that (6) holds.

Let U be a nondegenerate 4-space of sign $+1$. H has four components L_i, $1 \leqq i \leqq 4$, isomorphic to $SL_2(q)$, and it is well known that these components are permuted by a suitable triviality automorphism in A, so $N_B(\{U, U^\perp\})^B = N_B(\prod_i L_i)^B$ is A-invariant and (7) holds.

Let U be a nondegenerate 4-space of sign -1. Then H has components L_1 L_2 isomorphic to $\Omega_4^-(q)$. L_1 stabilizes a singular point U_1 of U, so by (1) there is $a \in A$ such that L_1^a acts faithfully on a totally singular 4-space W_1. $N_{L_2}(U_1)$ contains a subgroup of order q^2-1 centralizing L_1, so we conclude L_1^a acts naturally as $SL_2(q^2)$ on W_1 and $K = \mathrm{Hom}_{FL_1^a}(W_1, W_1)$ is a quadratic extension of F. Then as L_2^a centralizes L_1^a, $C_0(K)$ is irreducible on V, so (8) holds.

Let $V = \perp_{i=1}^{4} V_i$, with V_i of dimension 2 and sign ε. If $q=2$ and $\varepsilon=+1$ then the member of C_2 stabilizing this decomposition is contained in a parabolic, so take $q>2$. Let r be a prime divisor of $q-\varepsilon$ and $R \in \mathrm{Syl}_r\left(\bigcap_{i=1}^{4} N_\Delta(V_i)\right)$. Then $N_B(R) \in C_2$ is the stabilizer of $\{V_i : 1 \leqq i \leqq 4\}$, and if $r \neq 2$ or 3 then $R \in \mathrm{Syl}_r(\Delta)$, so that (9) and (10) hold by a Frattini argument. Even if $r=3$, $R = J(P)$ for $R \leqq P \in \mathrm{Syl}_3(\Delta)$, so the same argument works. This leaves the case $q-\varepsilon = 2^m$, which can be handled using Lemmas 2.2 and 1.4 in [1] and a Frattini argument, unless $q=3$ and $\varepsilon=+1$. In this last case each V_i contains a unique nonsingular point $\langle u_i \rangle$ with $Q(u_i)$ a residue. Then $U = \langle u_i : 1 \leqq i \leqq 4 \rangle$ is nondegenerate of sign $+1$ and dimension 4, and the stabilizer of $\{V_i : 1 \leqq i \leqq 4\}$ acts on $\{U, U^\perp\}$. Thus (9) holds.

Let $V = \perp_{i=1}^{8} V_i$ with $\dim(V_i)=1$ and V_i's isometric. Let M be the stabilizer in O of this decomposition, $P: O \to PO$ the projection map, and for $X \leqq PO$ let $X\alpha$ denote the preimage of X in O. Then M is the wreath product of Z_2 by S_8, and M centralizes a field automorphism of Ω if $q \neq p$, and hence is contained in a member of C_5. So take $p=q$. Let $t \in O_2(M)$ act trivially on exactly two V_i's. Then t is an involution but for suitable $a \in A$, $(\langle Pt \rangle^a)\alpha$ is of order 4. (Remember A does not act on Ω; $\Omega_1((\langle Pt \rangle^a)\alpha) = Z(\Omega)$.) Thus $[O_2(((PM)^a)\alpha), ((PM)^a)\alpha] \simeq D_8^3$, so that $((PM)^a)\alpha \in C_6$ and (11) holds.

Let M be a member of C_4 stabilizing $\mathscr{D} = ((V_1, f_1), (V_2, f_2))$ and let $n_i = \dim(V_i)$. Then $n_1 n_2 = \dim(V) = 8$, so we may take $n_1 = 2$ and $n_2 = 4$. Suppose f_1 and f_2 are symplectic. If p is odd we handled this case in (6), so let $p=2$. M has normal subgroups $L_i \cong Sp_{n_i}(q)$. L_2 acts irreducibly on a pair of totally singular 4-spaces, so from (1) there is $a \in A$ with L_2^a stabilizing a nondegenerate line U of sign $+1$. Indeed L_2^a stabilizes a nonsingular point $W \leqq U$, so by (3), $L_2 \leqq S \cong Sp_6(q)$ acting in the spin representation. Now $N_{N(S)}(L_2) \cong M$, so $M \leqq N(S) \in C_1^A$.

So we may take p odd and f_1 and f_2 orthogonal. Then as $n_1 = 2$, M has a normal cyclic subgroup M_1 which does not act by scalars on V. It follows that M is contained in a member of C_2 or C_3.

Similar arguments establish (14). Namely if M is a member of C_7 determined by a tuple (V_1, f_1, m) then $m=3$, f_1 is symmetric, and $\dim(V_1)=2$, so either $p=2$ and f_1 is symplectic or $\Omega(V_1, f_1)$ is not quasisimple, contrary to the definition of C_7. Therefore the former alternative holds, where an argument above shows M is contained in the normalizer of an $Sp_6(q)$ acting in the spin representation.

This completes our sketch of the proof of 15.1. Presumably 15.1 can be used to define a suitable $\mathscr{C}_A$, just as in the previous two sections, but the details would be much more complicated. Hopefully there is a more elegant approach.

References

1. Aschbacher, M.: On finite groups of Lie type and odd characteristic. J. Alg. **66**, 400–424 (1980)
2. Aschbacher, M., Scott, L.: Maximal subgroups of finite groups. J. Alg. in press (1984)
3. Aschbacher, M., Seitz, G.: Involutions in Chevalley groups over fields of even order. Nagoya Math. J. **63**, 1–91 (1976)
4. Huppert, B.: Endliche Gruppen, Vol. I, Berlin-Heidelberg-New York: Springer 1967
5. Passman, D.: Permutation groups. New York: Benjamin 1968

Oblatum 18-XI-1983