ON INTEGRAL REPRESENTATIONS OF FINITE GROUPS

By WALTER FEIT†

[Received 6 February 1974]

1. Introduction

Let G be a finite group. Let K be an algebraic number field contained in the field of complex numbers which is closed under complex conjugation. Let V be a faithful $K[G]$-module. There exists a G-invariant positive definite hermitian form on V. Let R be the ring of integers in K. Then there exist finitely generated $R[G]$-modules contained in V. Such $R[G]$-modules L are all G-invariant lattices. The object of this paper is to prove some results which assert that under various conditions one can choose a G-invariant lattice in V which has special properties. These properties can then be exploited to give information about the structure of G.

For instance, if it can be shown that the group of all linear transformations on V which preserve L and the form h is a finite group generated by unitary reflections then it follows that G is a subgroup of a known group as all finite groups generated by unitary reflections have been classified ([**22**]). These methods are most effective in case the order of G is divisible by a prime which is large compared to the dimension of V. In that case one can combine these methods with results based on the theory of modular characters. Theorem 8.6 below is a result of this type.

A slightly different approach leads to results which assert that under suitably strong assumptions the group has a representation of degree nm over a subfield K_0 of K with $[K : K_0] = m$ which preserves a lattice over K_0 of a special sort. See, for instance, Theorem 3.15 and its corollaries. When n is small, this method yields some information about G. See the discussion at the end of § 3.

When the dimension of V is less than $2(p-1)$ for some prime p which divides G and K is suitably restricted, one can get some detailed information concerning the structure of at least part of the lattice L. This method was originated by J. G. Thompson (unpublished) who studied the case when $K = Q$ and the lattice in question is unimodular. In fact, all the results in § 9 were proved by him for this case. For the most part, the

† The work on this paper was supported by NSF Contract GP-33591.

proofs in § 9 are routine generalizations of his arguments. The following results are proved by a combination of these methods.

THEOREM A. *Let p be a prime, $p \geqslant 7$. Let G be a finite group with a Sylow p-group P of order p. Assume that $|\mathbf{N}_G(P) : \mathbf{C}_G(P)| = p-1$ and G has a faithful irreducible rational representation of degree n with $8 \leqslant n \leqslant 2(p-1)$. Then one of the following holds:*

(i) *G has a normal p'-subgroup G_1 such that G/G_1 is isomorphic to a subgroup of S_{n+1};*

(ii) *$p = 7$, $n = 8$, and $G = H\mathbf{Z}(G)$, where H is isomorphic to $\mathrm{W}(E_8)$, $\mathrm{W}(E_8)'$, or $\widetilde{W(E_7)}$, where $\mathrm{W}(E_8)$ is the Weyl group of type E_8 and $\widetilde{W(E_7)}$ is a covering group of the Weyl group of type E_7.*

(iii) *$\mathrm{PSL}_2(p)$ is a composition factor of G and G has a subgroup of index $p+1$.*

THEOREM B. *Let p be a prime, $p \equiv 3 \pmod 4$, $p \geqslant 7$. Let G be a finite group with a Sylow p-group P of order p. Assume that $|\mathbf{N}_G(P) : \mathbf{C}_G(P)| = 2$, $|\mathbf{Z}(G)| = 1$, and G has a faithful irreducible character of degree $p+1$. Then either G is p-solvable or $p+1 = 2^a$ and there exists a normal p'-subgroup G_1 of G such that G/G_1 is isomorphic to $\mathrm{SL}_2(2^a)$.*

THEOREM C. *Let $p = 7$ or 11. Let G be a finite group which has a rational irreducible representation of degree n with $8 \leqslant n < 2(p-1)$. Then either G is p-solvable or one of the following holds:*

(i) *G has a normal p'-subgroup G_1 such that G/G_1 is isomorphic to a subgroup S_{n+1};*

(ii) *$p = 7$, $n = 8$, and $G = H\mathbf{Z}(G)$, where H is isomorphic to $\mathrm{W}(E_8)$, $\mathrm{W}(E_8)'$, or $\widetilde{W(E_7)}$.*

The next three results are based on the methods mentioned above together with the fact that a good deal is known about unimodular rational lattices in dimension at most 24. Theorems C and E include results announced previously ([**14**], Theorems 8.3.8 and 8.3.9).

THEOREM D. *Let p be a prime, $p \leqslant 23$. Let G be a group which has a faithful rational representation of degree $p-1$. Assume that $p \| |G|$. Then either $\mathrm{PSL}_2(p)$ is a composition factor of G or G has a subgroup of index p.*

THEOREM E. *Let G be a finite group which has a faithful rational-valued irreducible character of degree 23. Then one of the following holds:*

(i) *G has a subgroup of index 23 or 24;*

(ii) *$G \subseteq Z \times \mathrm{Co}.2$ or $G \subseteq Z \times \mathrm{Co}.3$, where Z is a cyclic group of order 2.*

THEOREM F. *Let G be a finite group which has a faithful rational representation of degree 24. Assume that $23 \mid\mid G\mid$. Then one of the following holds:*

(i) *G has a subgroup of index 23, 24, or 25,*

(ii) $G' \subseteq \mathrm{Co}.0$.

The notation used throughout this paper is standard notation from group theory and number theory and I hope is self-explanatory.

Theorem E arose in connection with D. Fendel's thesis ([**15**]). I am indebted to him for actually identifying the various lattices that arise in the proof of that theorem, see § 15. I am also indebted to A. Rudvalis, who informed me of some of his results concerning subgroups of $\mathrm{W}(E_8)$ (see Theorem 4.4).

Over the past few years, I have had many conversations with R. Steinberg and T. Tamagawa which have formed an education concerning quadratic forms, reflection groups, and rational lattices. The information thus imparted has proved invaluable in the preparation of this paper. I also wish to express my thanks to J. G. Thompson who, in a voluminous correspondence, informed me of many of his ideas and results on this subject, most especially the ideas underlying § 9 of this paper.

2. Lattices

The results in this section are closely related to those in [**6**], Chapter 1, § 3.

Let K be an algebraic number field. Let R be the ring of integers in K. Let V be an n-dimensional vector space over K. An ideal of K will always mean a fractional ideal. An ideal in R will be called an *integral ideal*. A prime ideal of R will always mean a non-zero integral prime ideal.

A *lattice* is a finitely generated R-module L with $L \subseteq V$ and $L \otimes_R K \approx V$.

Let L, M be lattices. Let $\mathfrak{p}$ be a prime ideal in R and let $L_\mathfrak{p}, M_\mathfrak{p}, V_\mathfrak{p}, R_\mathfrak{p}$ denote the completions of L, M, V, R at $\mathfrak{p}$ respectively. Since $R_\mathfrak{p}$ is a principal ideal domain, $L_\mathfrak{p}$ and $M_\mathfrak{p}$ are free $R_\mathfrak{p}$-modules of rank n. Thus there exists a linear transformation f on $V_\mathfrak{p}$ with $fL_\mathfrak{p} = M_\mathfrak{p}$. Let $(\det f)R_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^{a_\mathfrak{p}}$. Define the *module index* $[L : M]$ by $[L : M] = \prod_\mathfrak{p} \mathfrak{p}^{a_\mathfrak{p}}$. It is easily seen that $[L : M]$ is a well-defined ideal of K ([**6**], p. 10).

These definitions immediately yield the following results.

LEMMA 2.1. *Let L, M, N be lattices.*

(i) $[L : N] = [L : M][M : N]$.

(ii) *Suppose that $L \subseteq M$. Then $L = M$ if and only if $[M : L] = (1)$. M/L is an irreducible R-module if and only if $[M : L]$ is a prime ideal $\mathfrak{p}$ in R. In this case, $\mathfrak{p}$ annihilates M/L and M/L is a 1-dimensional vector space over the field $R/\mathfrak{p}$.*

Let σ be an automorphism of K with $\sigma^2 = 1$. Let h be a non-degenerate hermitian symmetric form with respect to σ on V. Let L be a lattice. The *h-dual of* L, denoted by L_h^*, is defined by

$$L_h^* = \{v \mid v \in V, h(u,v) \in R \text{ for all } u \in L\}.$$

Since h is non-degenerate L_h^* is a lattice. L is *unimodular* if $L_h^* = L$.

LEMMA 2.2. *Let L be a lattice and let h be a non-degenerate hermitian symmetric form on V with respect to σ.*

(i) *Let $\mathfrak{a}$ be a non-zero ideal of K. Then $(\mathfrak{a}L)_h^* = (\mathfrak{a}^\sigma)^{-1}(L_h^*)$.*

(ii) *Let $c \in K$, $c \neq 0$, $c^\sigma = c$. Then $L_{ch}^* = (cL)_h^* = c^{-1}(L_h^*)$.*

(iii) *If M is a lattice with $L \subseteq M$ then $M_h^* \subseteq L_h^*$ and $[M : L] = [L_h^* : M_h^*]^\sigma$.*

(iv) $(L_h^*)_h^* = L$.

Proof. (i) Every element in $\mathfrak{a}L$ is a linear combination of elements of the form au where $a \in \mathfrak{a}$, $u \in L$. Thus $v \in (\mathfrak{a}L)_h^*$ if and only if $h(u, a^\sigma v) = h(au, v) \in R$ for all $a \in \mathfrak{a}$, $u \in L$. This is the case if and only if $a^\sigma v \in L_h^*$ for all $a \in \mathfrak{a}$. The result follows.

(ii) By definition,

$$\begin{aligned} L_{ch}^* &= \{v \mid v \in V,\ ch(u,v) \in R \text{ for all } u \in L\} \\ &= \{v \mid v \in V,\ h(cu,v) \in R \text{ for all } u \in L\} = (cL)_h^*. \end{aligned}$$

The second equality follows from (i) with $\mathfrak{a} = (c)$.

(iii) Clearly $M_h^* \subseteq L_h^*$. We shall first prove that $[L_h^* : M_h^*] \mid [M : L]^\sigma$. By considering a composition series of the finite R-module M/L and using Lemma 2.1, it is sufficient to handle the case where M/L is an irreducible R-module. Thus $[M : L] = \mathfrak{p}$ is a prime ideal in R and M/L is a 1-dimensional vector space over the field $R/\mathfrak{p}$. If $a \in \mathfrak{p}$, $v \in L_h^*$ then for $u \in M$, au is in L and $h(u, a^\sigma v) = h(au, v) \in R$. Therefore L_h^*/M_h^* is a vector space over the field $R/\mathfrak{p}^\sigma$. It suffices to prove that L_h^*/M_h^* has dimension at most 1 because in that case $[L_h^* : M_h^*] \mid \mathfrak{p}^\sigma = [M : L]^\sigma$.

Let $u \in M$, $u \notin L$ and let $v, w \in L_h^*$. There exist $a, b \in R$, not both a, b in $\mathfrak{p}$, with

$$h(u, a^\sigma v + b^\sigma w) = ah(u,v) + bh(u,w) \in R.$$

Thus $a^\sigma v + b^\sigma w \in M_h^*$ since M/L is 1-dimensional. Consequently L_h^*/M_h^* does not have two linearly independent vectors.

Suppose that $[L_h^* : M_h^*] \neq [M : L]^\sigma$. For some integral ideal $\mathfrak{a}$ in R, $\mathfrak{a}M \subseteq L$. Thus Lemma 2.1 and the first part of the proof imply that $[(\mathfrak{a}M)_h^* : M_h^*] \neq [M : \mathfrak{a}M]^\sigma$. Hence, by (i),

$$(\mathfrak{a}^\sigma)^n = [(\mathfrak{a}^\sigma)^{-1} M_h^* : M_h^*] = [(\mathfrak{a}M)_h^* : M_h^*] \neq [M : \mathfrak{a}M]^\sigma = (\mathfrak{a}^\sigma)^n.$$

This contradiction establishes the result.

(iv) Clearly $L \subseteq (L_h^*)_h^*$. Furthermore, $L_h^* = ((L_h^*)_h^*)_h^*$. Hence, by (iii),

$$[(L_h^*)_h^* : L] = [L_h^* : ((L_h^*)_h^*)_h^*]^\sigma = (1)^\sigma = (1)$$

and so $L = (L_h^*)_h^*$.

Let L be a lattice. *The discriminant $d_h(L)$ of L with respect to h* is defined by $d_h(L) = [L_h^* : L]$. The following is a direct corollary of Lemmas 2.1 and 2.2.

LEMMA 2.3. *Let L be a lattice. Let h be a non-degenerate hermitian symmetric form on V with respect to σ.*

(i) *Let $\mathfrak{a}$ be a non-zero ideal of K. Then $d_h(\mathfrak{a}L) = (\mathfrak{a}\mathfrak{a}^\sigma)^n d_h(L)$.*

(ii) *Let $c \in K$, $c \neq 0$, $c^\sigma = c$. Then $d_{ch}(L) = c^n d_h(L)$.*

(iii) *Let M be a lattice. Then $d_h(M) = d_h(L)[L : M][L : M]^\sigma$.*

A lattice L is *integral with respect to h* if $h(u, v) \in R$ for all $u, v \in L$. The following result is clear.

LEMMA 2.4. *Let L be a lattice. Let h be a non-degenerate hermitian symmetric form on V with respect to σ.*

(i) *$L \cap L_h^*$ is integral with respect to h.*

(ii) *L is integral with respect to h if and only if $L \subseteq L_h^*$.*

(iii) *Let M be a lattice with $M \subseteq L$. If L is integral with respect to h then M is integral with respect to h.*

(iv) *For some non-zero element c in R with $c^\sigma = c$, L is integral with respect to ch.*

(v) *For some non-zero element c in R, cL is integral with respect to h.*

LEMMA 2.5. *Let h be a non-degenerate hermitian symmetric form on V with respect to σ. Let L be a lattice which is integral with respect to h. Let $\mathfrak{a}$ be an integral ideal of K. Then $(\mathfrak{a}^\sigma L_h^* \cap \mathfrak{a}^{-1}L) + L$ is integral with respect to h.*

Proof. By Lemma 2.2(i), $\mathfrak{a}^\sigma L_h^* = (\mathfrak{a}^{-1}L)_h^*$. Thus by Lemma 2.4(i), $\mathfrak{a}^\sigma L_h^* \cap \mathfrak{a}^{-1}L$ is integral with respect to h. The result follows from the fact that $\mathfrak{a}^\sigma L_h^* \cap \mathfrak{a}^{-1}L \subseteq L_h^*$.

LEMMA 2.6. *Let K' be a finite extension field of K such that σ extends to an automorphism σ' of K' with $(\sigma')^2 = 1$. Let R' be the ring of integers in K'. Let $V' = V \otimes_K K'$. For any lattice L in V, let $L' = L \otimes_R R'$. Let h be a non-degenerate hermitian symmetric form on V with respect to σ. Then h extends uniquely to a non-degenerate hermitian symmetric form h' on V'. Furthermore, if L, M are lattices in V then $[L' : M'] = [L : M]R'$ and $d_{h'}(L') = d_h(L)R'$.*

Proof. All statements are immediate consequences of the definitions.

Let K be a field in which 2 is totally ramified. In other words, $(2) = \mathfrak{p}^{[K:Q]}$ for some prime ideal $\mathfrak{p}$ in R. Let h be a non-degenerate hermitian symmetric form on V and let L be a lattice which is integral with respect to h. Then L is *even with respect to* h if $h(v, v) \in \mathfrak{p}$ for all $v \in L$.

LEMMA 2.7. *Let K be a field in which 2 is totally ramified. Let $\mathfrak{p}$ be a prime divisor of 2 in R. Let h be a non-degenerate symmetric hermitian form on V and let L be a lattice which is integral with respect to h. Define $L_0 = \{v \mid v \in L, h(v, v) \in \mathfrak{p}\}$. Then L_0 is a lattice and either $L = L_0$ or $[L : L_0] = \mathfrak{p}$.*

Proof. Since $(2) = \mathfrak{p}^{[K:Q]}$ it follows that $R/\mathfrak{p}$ is a field of 2 elements. Thus if $v, w \in L$ then $h(v, w) \equiv 0$ or $1 \pmod{\mathfrak{p}}$. In particular, this implies that $h(v, w) \equiv h(w, v) \pmod{\mathfrak{p}}$ and so $h(v, w) + h(w, v) \in \mathfrak{p}$. Thus

$$h(v+w, v+w) \equiv h(v, v) + h(w, w) \pmod{\mathfrak{p}}.$$

Hence L_0 is a lattice and if $v, w \in L$, $v, w \notin L_0$ then $v + w \in L_0$.

Let V, V' be vector spaces over K. Let h, h' be non-degenerate hermitian symmetric forms on V, V' respectively. An *isometry* from V to V' is a linear map f from V to V' such that $h(v, w) = h'(f(v), f(w))$ for all $v, w \in V$. If L, L' are lattices in V, V' respectively then *the pair (L, h) is isometric to the pair (L', h')* if there exists an isometry from V to V' which maps L onto L'. An *automorphism* of the pair (L, h) is an isometry from V to V which sends L onto L. The group of all automorphisms of (L, h) will be denoted by $\mathrm{Aut}((L, h))$. Clearly isometric pairs (L, h) and (L', h') have isomorphic automorphism groups.

I am indebted to J. G. Thompson who informed me of the following result.

THEOREM 2.8 (Thompson). *Let V be an n-dimensional vector space over Q with $n \equiv 0 \pmod 8$. Let h be a positive definite symmetric bilinear form on V. Let L be a lattice in V which is integral with respect to h such that $L_h^* = L$. Let $G = \mathrm{Aut}((L, h))$. Then there exists a subgroup G_0 of G with $|G : G_0| \leqslant 2$ and a lattice L_0 which is integral and even with respect to h such that $(L_0)_h^* = L_0$ and $G \subseteq \mathrm{Aut}((L_0, h))$.*

Proof. If L is even, there is nothing to prove. Suppose that L is not even. Let $L_1 = \{v \mid v \in L, h(v, v) \equiv 0 \pmod 2\}$. By Lemma 2.7, L_1 is even and $d_h(L_1) = (4)$. It is known that there exists an even lattice $L_0 \subseteq (L_1)_h^*$ with $d_h(L_0) = (1)$ (see, for example, [**21**], pp. 87, 88). Thus $(L_1)_h^*/L_1$ is a non-cyclic group of order 4 since $L_1 \subseteq L$, $L_0 \subseteq (L_1)_h^*$. Thus there are

three lattices L' with $L_h'^* = L'$ and $L_1 \subseteq L' \subseteq (L_1)_h^*$. Either one or two of these are even. The group G permutes these even lattices. Hence, if G_0 is the subgroup which leaves L_0 fixed, $|G : G_0| \leqslant 2$ and $G_0 \subseteq \mathrm{Aut}((L_0, h))$.

LEMMA 2.9. *Let $\mathfrak{p}_1, \mathfrak{p}_2^\sigma$ be distinct prime ideals of R. Let L, M_1, M_2 be lattices such that $L \subseteq M_j$ and $[M_j : L] = \mathfrak{p}_j^{m_j}$ for $j = 1, 2$, where m_1, m_2 are non-negative rational integers. If M_1 and M_2 are integral with respect to h then $M_1 + M_2$ is integral with respect to h.*

Proof. It clearly suffices to show that if $v_j \in M_j$ for $j = 1, 2$ then $h(v_1, v_2) \in R$. By assumption $v_2 \in L_h^*$ and $\mathfrak{p}_1^{m_1} v_1 \subseteq L$. Thus if $c \in \mathfrak{p}_1^{m_1}$ then $ch(v_1, v_2) = h(cv_1, v_2) \in R$. Therefore $\mathfrak{p}_1^{m_1} h(v_1, v_2) \in R$. Similarly $(\mathfrak{p}_2^\sigma)^{m_2} h(v_1, v_2) \subseteq R$. Consequently $h(v_1, v_2) \in R$ as $\mathfrak{p}_1^{m_1}$ and $(\mathfrak{p}_2^\sigma)^{m_2}$ are relatively prime.

For the remainder of this section the following situation will be considered.

V_1, V_2 are vector spaces over K. For $j = 1, 2$, h_j is a non-degenerate hermitian symmetric form on V_j with respect to σ. $V = V_1 \oplus V_2$ is the orthogonal direct sum of V_1 and V_2 and $h = h_1 \oplus h_2$. Thus h is a non-degenerate hermitian symmetric form on V with respect to σ. For $j = 1, 2$, h restricted to V_j coincides with h_j.

LEMMA 2.10. *For $j = 1, 2$, let L_j be a lattice in V_j. Then*

$$(L_1 \oplus L_2)_h^* = (L_1)_h^* \oplus (L_2)_h^* \quad \text{and} \quad d_h(L_1 \oplus L_2) = d_h(L_1) d_h(L_2).$$

Proof. This is clear.

THEOREM 2.11. *Let $\mathfrak{p}$ be a prime ideal in R such that $\mathfrak{p}^\sigma = \mathfrak{p}$. For $j = 1, 2$, let L_j be a lattice in V_j which is integral with respect to h_j and such that $d_h(L_j) = \mathfrak{p}\mathfrak{a}_j$ for some ideal $\mathfrak{a}_j$ of R which is prime to $\mathfrak{p}$.*

(i) *$\mathfrak{p}^{-1} L_j \cap (L_j)_h^* = \langle v_j, L_j \rangle$ for some vector v_j. If $c_j = h(v_j, v_j)$ then $c_j \in \mathfrak{p}^{-1}$, $c_j \notin R$.*

(ii) *There exists a lattice L which is integral with respect to h such that $L_1 \oplus L_2 \subseteq L$ and $[L : L_1 \oplus L_2] = \mathfrak{p}$ if and only if there exists $a \in R$ with $c_1 + c_2 a a^\sigma \in R$. When L exists, $L = \langle L_1 \oplus L_2, v_1 + a v_2 \rangle$ for some $a \in R$ with $c_1 + c_2 a a^\sigma \in R$.*

(iii) *If $\sigma \neq 1$, the lattice L of* (ii) *exists.*

(iv) *Suppose that $\sigma = 1$. Let L, L' be lattices which contain $L_1 \oplus L_2$ and are integral with respect to h. Suppose that $[L : L_1 \oplus L_2] = [L' : L_1 \oplus L_2] = \mathfrak{p}$. Then (L, h) is isometric to (L', h).*

Proof. (i) $(\mathfrak{p}^{-1} L_j \cap (L_j)_h^* / L_j) \approx R/\mathfrak{p}$ is a cyclic R-module. Clearly $c_j \in \mathfrak{p}^{-1}$. If $c_j \in R$ then $\mathfrak{p}^{-1} L_j \cap (L_j)_h^*$ is integral with respect to h. By Lemma 2.3(iii), $d_h(\mathfrak{p}^{-1} L_j \cap (L_j)_h^*) = \mathfrak{p}^{-1}\mathfrak{a}_j$. contrary to Lemma 2.4(ii).

(ii) Suppose that $a \in R$ with $c_1 + c_2 a a^\sigma \in R$. Let $L = \langle L_1 \oplus L_2, v_1 + a v_2 \rangle$. Then L satisfies all the required conditions. Conversely, suppose that L exists. Then $a_1 v_1 + a_2 v_2$ is in L but not in $L_1 \oplus L_2$ for some $a_1, a_2 \in R$. If $a_1 \in \mathfrak{p}$ then $a_1 v_1 \in L_1$. Thus $a_2 v_2 \in L$ and $c_2 a_2 a_2^\sigma = h(a_2 v_2, a_2 v_2) \in R$. Hence $a_2 \in \mathfrak{p}$ and so $a_2 v_2 \in L_2$, contrary to the choice of a_1, a_2. Therefore $a_1 \notin \mathfrak{p}$ and so there exists $a_1' \in R$ with $a_1 a_1' \equiv 1 \pmod{\mathfrak{p}}$. Thus $a_1' a_1 v_1 + a_1' a_2 v_2 \in L$. This implies that $v_1 + a v_2 \in L$ for some $a \in R$. Clearly $v_1 + a v_2 \notin L_1 \oplus L_2$. Furthermore,

$$c_1 + c_2 a a^\sigma = h(v_1 + a v_2, v_1 + a v_2) \in R.$$

(iii) If $\sigma \neq 1$ then every element of $\mathfrak{p}^{-1}/R$ which is fixed by σ is of the form $b b^\sigma$. (Every element of a finite field is the norm in a finite extension.) Thus the element a of (ii) exists. Hence L exists.

(iv) $L = \langle L_1 \oplus L_2, v_1 + a v_2 \rangle$ and $L' = \langle L_1 \oplus L_2, v_1 + a' v_2 \rangle$ with $c_1 + c_2 a^2$, $c_1 + c_2 (a')^2 \in R$ by (ii). Hence $a^2 \equiv (a')^2 \pmod{\mathfrak{p}}$. Therefore

$$a \equiv \pm a' \pmod{\mathfrak{p}}.$$

If $a \equiv a' \pmod{\mathfrak{p}}$ then $L = L'$. If $a \equiv -a' \pmod{\mathfrak{p}}$ define $f: V \to V$ by $f(w_1 + w_2) = w_1 - w_2$ for $w_j \in V_j$. Then clearly f is an isometry which maps L onto L'.

LEMMA 2.12. *Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ be distinct prime ideals in R such that $\mathfrak{p}_i^\sigma = \mathfrak{p}_i$ for each i. For $j = 1, 2$, let L_j be a lattice in V_j which is integral with respect to h_j such that $d_h(L_j) = \mathfrak{a}_j \prod \mathfrak{p}_i$ for some ideal $\mathfrak{a}_j$ of R which is prime to each $\mathfrak{p}_i$. There exists a lattice L which is integral with respect to h such that $L_1 \oplus L_2 \subseteq L$ and $[L : L_1 \oplus L_2] = \prod \mathfrak{p}_i$ if and only if for each i there exists a lattice M_i which is integral with respect to h such that $L_1 \oplus L_2 \subseteq M_i$ and $[M_i : L_1 \oplus L_2] = \mathfrak{p}_i$.*

Proof. If L exists, let $M_i = L \cap \mathfrak{p}_i^{-1}(L_1 \oplus L_2)$. If each M_i exists, let $L = \sum M_i$. By Lemma 2.9, L is integral with respect to h.

It should be noted that the analogue of Theorem 2.11(iv) does not hold under the assumptions of Lemma 2.12. That is to say that even if $\sigma = 1$, L is not necessarily unique up to isometry.

3. G-Invariant lattices

Let G be a finite group.

Let K be an algebraic number field and let V be a $K[G]$-module on which G acts faithfully. Let $n = \dim_K V$.

Let $\nu_1, \nu_2, \ldots$ be all the (pairwise inequivalent) archimedean valuations of K. Let K_j be the completion of K with respect to ν_j. Then K can be identified with a subfield of K_j. For each j, K_j is isomorphic to the field

of real numbers or the field of complex numbers. Let σ_j denote complex conjugation on K_j.

Suppose that $\sigma_j(K) = K \subseteq K_j$ for some j. There exist non-zero G-invariant hermitian symmetric forms on V with respect to σ_j whose extension to $V \otimes_K K_j$ is definite. Hence such a form is either positive definite or negative definite.

Throughout this section it is assumed that there exists some j with $\sigma_j(K) = K$. For $c \in K$, write $\bar{c} = \sigma_j(c)$. In general h will denote a G-invariant hermitian symmetric form on V with respect to σ_j whose extension to $V \otimes_K K_j$ is either positive definite or negative definite.

Let R be the ring of integers in K. A *G-invariant lattice* is a lattice in V which is also an $R[G]$-module.

$\mathscr{L}_h$ is the set of all G-invariant lattices in V which are integral with respect to h. $\mathscr{L}_h$ is non-empty. By Lemma 2.3, $\mathscr{L}_h$ satisfies the maximum condition with respect to inclusion and so in particular $\mathscr{L}_h$ contains maximal elements.

LEMMA 3.1. *Let L, M be G-invariant lattices. Let $\mathfrak{a}$ be an ideal of K. Then $L+M$, $L \cap M$, $\mathfrak{a}L$, and L_h^* are G-invariant lattices.*

The proof is clear.

THEOREM 3.2. *Let $L \in \mathscr{L}_h$. Let $\mathfrak{p}$ be a prime ideal in R. Let $d_h(L) = \mathfrak{p}^m\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in R which is not divisible by $\mathfrak{p}$. Assume that $\mathfrak{p} \nmid [L_h^* : \mathfrak{p}^{-1}L \cap L_h^*]$. Then*

(i) $0 \leqslant m \leqslant n$;

(ii) *m is the dimension of a constituent of the $R[G]$-module $\mathfrak{p}^{-1}L/L$;*

(iii) *if V is absolutely irreducible and $0 < m < n$ then $p \mid\mid |G|$, where p is the rational prime with $\mathfrak{p} \mid p$.*

Proof. Since $\mathfrak{p}^n = [\mathfrak{p}^{-1}L : L]$ and $\mathfrak{p}^{-1}L$ is an $R[G]$-module, (i) and (ii) are clear. If $0 < m < n$ then, by (ii), $\mathfrak{p}^{-1}L/L$ is a reducible $R[G]$-module. As V is absolutely irreducible, this implies that $p \mid\mid |G|$.

THEOREM 3.3. *Let L be a maximal element of $\mathscr{L}_h$. Let $\mathfrak{p}$ be a prime ideal in R with $\mathfrak{p} \neq \bar{\mathfrak{p}}$. Then $\mathfrak{p} \nmid d_h(L)$.*

Proof. By Lemma 2.5, $(\bar{\mathfrak{p}}L_h^* \cap \mathfrak{p}^{-1}L) + L \in \mathscr{L}_h$. The maximality of L implies that $\bar{\mathfrak{p}}L_h^* \cap \mathfrak{p}^{-1}L \subseteq L$. Multiplying through by $\bar{\mathfrak{p}}^{-1}$ and using the fact that $\mathfrak{p}^{-1}L \subseteq \bar{\mathfrak{p}}^{-1}\mathfrak{p}^{-1}L$, we obtain $L_h^* \cap \mathfrak{p}^{-1}L \subseteq \bar{\mathfrak{p}}^{-1}L$. Since

$$\mathfrak{p}^{-1}L \cap \bar{\mathfrak{p}}^{-1}L = L,$$

this implies that

$$L_h^* \cap \mathfrak{p}^{-1}L = L_h^* \cap \mathfrak{p}^{-1}L \cap \bar{\mathfrak{p}}^{-1}L = L_h^* \cap L = L.$$

Thus $\mathfrak{p} \nmid d_h(L)$ as required.

THEOREM 3.4. *Let L be a maximal element in $\mathscr{L}_h$. Let $\mathfrak{p}$ be a prime ideal in R. Then $\mathfrak{p} \nmid [L_h^* : \mathfrak{p}^{-1}L \cap L_h^*]$.*

Proof. Suppose that $\mathfrak{p} \mid [L_h^* : \mathfrak{p}^{-1}L \cap L_h^*]$. Then there exists an element $v \in L_h^*$ and an element $a \in \mathfrak{p}$ such that $av \notin L$, $\mathfrak{p}^2 v \subseteq L$. Let

$$M = L + \langle avx \mid a \in \mathfrak{p},\ x \in G \rangle.$$

Then M is a G-invariant lattice and $L \subset M \subseteq L_h^*$. If $x, y \in G$, $a, b \in \mathfrak{p}$ then $\bar{b} \in \mathfrak{p}$ by Theorem 3.3 and

$$h(avx, bvy) = h(a\bar{b}vx, vy) \in R$$

since $a\bar{b}vx \in \mathfrak{p}^2 vx \subseteq L$ and $vy \in L_h^*$. If $u \in L$ then $h(u, avx) \in R$ for all $x \in G$, $a \in \mathfrak{p}$ as $avx \in L_h^*$. Thus $M \in \mathscr{L}_h$. This contradicts the maximality of L and proves the result.

COROLLARY 3.5. *Let L be a maximal element in $\mathscr{L}_h$. There exist distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ in R such that $L_h^* \subseteq (\prod \mathfrak{p}_i)^{-1}L$. In particular L_h^*/L has square-free exponent.*

Proof. This is an immediate corollary of Theorem 3.4.

Theorem 3.3 has the following curious consequence which, however, seems to be difficult to use.

THEOREM 3.6. *Let L be a maximal element in $\mathscr{L}_h$. Let K' be a finite extension field of K which is closed under complex conjugation and let R' be the ring of integers in K'. Assume that if $\mathfrak{p}$ is any prime ideal in R with $\mathfrak{p} \mid d_h(L)$ then $\mathfrak{p}R' = \mathfrak{A}\overline{\mathfrak{A}}$, where $\mathfrak{A}, \overline{\mathfrak{A}}$ are ideals in R' with $(\mathfrak{A}, \overline{\mathfrak{A}}) = (1)$. Let $V' = V \otimes_K K'$. Let h' be the unique extension of h to a non-degenerate hermitian symmetric form V' with respect to complex conjugation. Then h' is positive definite and G-invariant. Let $\mathscr{L}'_{h'}$ be the set of all G-invariant lattices in V' which are integral with respect to h'. Then there exists $M \in \mathscr{L}'_{h'}$ with $d_{h'}(M) = (1)$.*

Proof. Clearly h' is G-invariant and positive definite. Let M be a maximal element of $\mathscr{L}'_{h'}$ which contains $L' = L \otimes_R R'$. By Lemma 2.6, $d_{h'}(M) \mid d_{h'}(L') = d_h(L)R'$. Thus if $\mathfrak{p}'$ is any prime ideal in R' which divides $d_{h'}(M)$ then $\mathfrak{p}' \neq \bar{\mathfrak{p}}'$. Hence $d_{h'}(M) = (1)$ by Theorem 3.3.

It is easy to construct fields K' which satisfy the hypotheses of Theorem 3.6. For instance, let m be a positive rational integer such that $\left(\frac{-m}{p}\right) = 1$ for all odd rational primes p with $(p, d_h(L)) \neq (1)$, where $\left(\frac{-m}{p}\right)$ is the Legendre symbol. Assume further that $-m \equiv 1 \pmod 8$

if $(2, d_h(L)) \neq (1)$. Then the field $K' = K(\sqrt{(-m)})$ satisfies the hypotheses of Theorem 3.6. Dirichlet's theorem on primes in an arithmetic progression implies that m can even be chosen to be a rational prime.

Let $L \in \mathscr{L}_h$. The *pair* (L, h) *has minimal discriminant* if for any positive definite or negative definite G-invariant hermitian symmetric form h' and $M \in \mathscr{L}_{h'}$, $d_{h'}(M) \mid d_h(L)$ implies that $d_{h'}(M) = d_h(L)$.

LEMMA 3.7. *If (L, h) has minimal discriminant then L is maximal in $\mathscr{L}_h$.*

Proof. This result is clear by Lemma 2.3(iii).

THEOREM 3.8. *Let $L \in \mathscr{L}_h$. Assume that if $\mathfrak{p}$ is any prime ideal in R then $\mathfrak{p} \nmid [L_h^* : \mathfrak{p}^{-1}L \cap L_h^*]$. Suppose that $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ are distinct prime ideals in R such that $\mathfrak{p}_i = \bar{\mathfrak{p}}_i$ for all i and $\prod \mathfrak{p}_i = c_0 \mathfrak{a}\bar{\mathfrak{a}}$ for some ideal $\mathfrak{a}$ of K and some $c_0 = \bar{c}_0$ in K. Let $d_h(L) = \mathfrak{b} \prod \mathfrak{p}_i^{m_i}$ where $\mathfrak{b}$ is an ideal in R which is not divisible by any $\mathfrak{p}_i$. Then there exists $c \in K$ with $c = \bar{c}$ and $M \in \mathscr{L}_{ch}$ such that $d_{ch}(M) = \mathfrak{b} \prod \mathfrak{p}_i^{n-m_i}$.*

Proof. Replacing c_0 by $-c_0$ if necessary, it may be assumed that $c_0 > 0$. Any ideal class of K contains infinitely prime ideals. Thus $\mathfrak{a} = a\mathfrak{q}^{-1}$ for some prime ideal $\mathfrak{q}$ such that $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ are distinct from all $\mathfrak{p}_i$ and neither divides $d_h(L)$. Thus $c_0 \mathfrak{a}\bar{\mathfrak{a}} = c_0 a\bar{a}\mathfrak{q}^{-1}\bar{\mathfrak{q}}^{-1}$.

Let $c = c_0 a\bar{a}$. Hence $(c) = \mathfrak{q}\bar{\mathfrak{q}} \prod \mathfrak{p}_i$.

Let $M = \bar{\mathfrak{q}}c^{-1}L \cap \mathfrak{q}^{-1}L_h^*$. Clearly M is a G-invariant lattice. If $v, w \in M$ then $ch(v, w) = h(cv, w) \in R$ as $cv \in \bar{\mathfrak{q}}L$ and $w \in \mathfrak{q}^{-1}L_h^* = (\bar{\mathfrak{q}}L)_h^*$. Thus $M \in \mathrm{L}_{ch}$.

Since $\bar{\mathfrak{q}}c^{-1} = \mathfrak{q}^{-1} \prod \mathfrak{p}_i^{-1}$, it follows that $[M : L] = \mathfrak{q}^n \prod \mathfrak{p}_i^{m_i}$. Hence Lemma 2.3 implies that

$$d_{ch}(M) = c^n d_h(M) = c^n d_h(L)[L : M]\overline{[M : L]} = c^n \mathfrak{b}\mathfrak{q}^{-n}\bar{\mathfrak{q}}^{-n} \prod \mathfrak{p}_i^{-m_i}$$
$$= \mathfrak{b} \prod \mathfrak{p}_i^{n-m_i}.$$

COROLLARY 3.9. *Let $K_0 = \{a \mid a \in K, \bar{a} = a\}$. Let $\{\mathfrak{p}_i\}$ be a finite set of prime ideals in K, none of which is ramified in K over K_0. There exist infinitely many prime ideals $\mathfrak{q}$ of K_0 which satisfy the following conditions:*

(i) *$\mathfrak{q} \neq \mathfrak{p}_i$ for all i;*

(ii) *There exists $c = c(\mathfrak{q}) \in K_0$ and a G-invariant lattice $M \in \mathscr{L}_{ch}$ depending on $\mathfrak{q}$, such that $d_{ch}(M) = \mathfrak{b}(\mathfrak{q}R)^n \prod \mathfrak{p}_i^{m_i}$, where $\mathfrak{b}$ is an ideal in R which is not divisible by $\mathfrak{q}$ or $\mathfrak{p}_i$ for any i and $2m_i \leqslant n$ for all i.*

Proof. Let L be a maximal element in $\mathscr{L}_h$. Let A be the set of all $\mathfrak{p}_i$ such that $\mathfrak{p}_i^{[\frac{1}{2}n]+1} \mid d_h(L)$. Let $d_h(L) = \mathfrak{b}\mathfrak{c} \prod_{\mathfrak{p}_i \in A} \mathfrak{p}_i^{m_i}$, where $\mathfrak{b}$ an ideal of R which is relatively prime to all $\mathfrak{p}_i$ and $\mathfrak{c}$ is a product of powers of $\mathfrak{p}_j$,

with $\mathfrak{p}_j \notin A$. By Theorem 3.3, $\mathfrak{p}_i = \bar{\mathfrak{p}}_i$ for all $\mathfrak{p}_i \in A$. Since no $\mathfrak{p}_i$ in A is ramified in K over K_0, this implies that if $\mathfrak{p}_i \in A$ then there exists a prime ideal $\mathfrak{p}_i^0$ of K_0 such that $\mathfrak{p}_i = \mathfrak{p}_i^0 R$. There exist infinitely many prime ideals $\mathfrak{q}$ of K_0 in the class containing $\{\prod_{\mathfrak{p}_i \in A} \mathfrak{p}_i\}^{-1}$. Thus $\mathfrak{q} \prod_{\mathfrak{p}_i \in A} \mathfrak{p}_i = (c_0)$ for some $c_0 \in K_0$. Hence there exist infinitely many such prime ideals $\mathfrak{q}$ distinctive from all $\mathfrak{p}_i$ and not dividing $d_h(L)$. The result now follows from Theorem 3.8.

COROLLARY 3.10. *Suppose that (L, h) has minimal discriminant. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ be distinct prime ideals in R such that $\prod \mathfrak{p}_i = c_0 \mathfrak{a}\bar{\mathfrak{a}}$ for some ideal $\mathfrak{a}$ of K and some $c_0 = \bar{c}_0 \in K$. Then there exists i with $\mathfrak{p}_i^{[\frac{1}{2}n]+1} \nmid d_h(L)$.*

Proof. If $\mathfrak{p}_i \neq \bar{\mathfrak{p}}_i$ for some i, the result follows from Theorem 3.3 and Lemma 3.7. If $\mathfrak{p}_i = \bar{\mathfrak{p}}_i$ for all i then Theorem 3.8 implies the result as (L, h) has minimal discriminant.

COROLLARY 3.11. *Suppose that (L, h) has minimal discriminant. Let $c_0 \in R$ with $c_0 = \bar{c}_0$ such that $(c_0) = \mathfrak{p}$ is a prime ideal in R. Then $\mathfrak{p}^{[\frac{1}{2}n]+1} \nmid d_h(L)$.*

Proof. This is a special case of Corollary 3.10.

COROLLARY 3.12. *Let $K_0 = \{a \mid a \in K, \bar{a} = a\}$. Suppose that K_0 has class number 1. Let (L, h) have minimal discriminant. If $\mathfrak{p}$ is a prime in K which is not ramified in the extension of K over K_0 then $\mathfrak{p}^{[\frac{1}{2}n]+1} \nmid d_h(L)$.*

Proof. This is immediate by Corollaries 3.9 and 3.11.

COROLLARY 3.13. *Suppose that (L, h) has minimal discriminant. Let $\mathfrak{p}$ be a prime in K.*

(i) *If $K = Q$ then $\mathfrak{p}^{[\frac{1}{2}n]+1} \nmid d_h(L)$.*

(ii) *If K is an imaginary quadratic extension of Q and $\mathfrak{p}$ does not ramify in K then $\mathfrak{p}^{[\frac{1}{2}n]+1} \nmid d_h(L)$.*

Proof. This is clear by Corollary 3.12.

In general, Corollary 3.12 and Corollary 3.13(ii) cannot be strengthened. For instance, let G be the quaternion group of order 8 and let $K = Q(\sqrt{-3})$. There exists a 2-dimensional faithful $K[G]$-module. Let $\mathfrak{p} = (\sqrt{-3})$. It can be shown that if the pair (L, h) has minimal discriminant then $\mathfrak{p}^2 \mid d_h(L)$.

For the remainder of this section the following situation will be considered.

K_0 is a subfield of K. R_0 is the ring of integers in K_0. T and N respectively denote the trace and norm from K to K_0. Let V_0 be V considered as a $K_0[G]$-module. Thus V_0 has dimension $[K : K_0]n$ over K_0.

If L is a lattice in V, let L_0 be L, considered as a lattice in V_0. If L is G-invariant then clearly L_0 is G-invariant. Let h be a G-invariant positive definite hermitian symmetric form on V. Define $h_0(v,w) = \mathrm{T}(h(v,w))$ for all $v, w \in V_0$. Clearly h_0 is a G-invariant K_0-bilinear form on V_0. Assume that

(i) $\bar{K}_0 = K_0$.

(ii) $\overline{h_0(v,w)} = h_0(w,v)$ for v, w in V_0 and h_0 is positive definite.

If, for instance, $K_0 = \{c \mid c \in K, \bar{c} = c\}$ then these conditions are satisfied since $h_0 = h + \bar{h}$ and $h_0(v,v) = 2h(v,v)$ for $v \in V$. In fact $h_0(v,v)$ is always even in this case.

Let $\mathfrak{d}$ be the different of K over K_0. Let $\mathfrak{d} = \mathfrak{a}^2\mathfrak{d}_1$, where $\mathfrak{a}$ is an integral ideal in R and $\mathfrak{d}_1$ is the product of distinct prime ideals of R.

LEMMA 3.14. *Suppose that if* $\mathfrak{p}$ *is any prime ideal in* R *then*

$$\mathfrak{p} \nmid [L_h^* : \mathfrak{p}^{-1}L \cap L_h^*].$$

Then

(i) $(\mathfrak{a}^{-1}L)_0$ *is a* G*-invariant lattice in* V_0 *which is integral with respect to* h_0*;*

(ii) $((\mathfrak{a}^{-1}L)_0)_{h_0}^* = \{\mathfrak{a}^{-1}\mathfrak{d}_1^{-1}(L_h^*)\}_0 . d_{h_0}((\mathfrak{a}^{-1}L)_0) = \mathrm{N}(\mathfrak{d}_1)^n \mathrm{N}(d_h(L))$*;*

(iii) *if* $\mathfrak{p}_0$ *is any prime ideal in* R_0 *then*

$$\mathfrak{p}_0 \nmid [((\mathfrak{a}^{-1}L)_0)_{h_0}^* : \mathfrak{p}_0^{-1}(\mathfrak{a}^{-1})L)_0 \cap ((\mathfrak{a}^{-1}L)_0)_{h_0}^*].$$

Proof. Clearly $(\mathfrak{a}^{-1}L)_0$ is G-invariant. By definition,

$$(L_0)_{h_0}^* = \{v \mid v \in V_0,\ h(v,w) \in \mathfrak{d}^{-1} \text{ for all } w \in L_0\}$$

$$= \{v \mid v \in V_0,\ \mathfrak{d}v \subseteq L_h^*\} = (\mathfrak{d}^{-1}L_h^*)_0.$$

Thus (ii) follows from Lemma 2.2 as $\mathfrak{d} = \bar{\mathfrak{d}}$. By (ii) $(\mathfrak{a}^{-1}L)_0 \subseteq ((\mathfrak{a}^{-1}L)_0)_{h_0}^*$ and so (i) is proved.

Suppose that (iii) is false for the prime ideal $\mathfrak{p}_0$ in R_0. Then there exists $v \in \mathfrak{a}\mathfrak{d}^{-1}(L_h^*)$ such that $\mathfrak{p}_0 v \notin \mathfrak{a}^{-1}L$ but $\mathfrak{p}_0^2 v \subseteq \mathfrak{a}^{-1}L$. Suppose first that $\mathfrak{p}_0 R$ is prime to $\mathfrak{d}_1$. Then $[\mathfrak{a}\mathfrak{d}^{-1}L_h^* : \mathfrak{a}^{-1}L_h^*]$ is prime to $\mathfrak{p}_0$. Thus $v \in \mathfrak{a}^{-1}L_h^*$ and so $\mathfrak{a}v \subseteq L_h^*$. Let $\mathfrak{p}$ be a prime divisor of $\mathfrak{p}_0$ in R. Then $\mathfrak{p}\mathfrak{a}v \subseteq L$ and so $\mathfrak{p}v \subseteq \mathfrak{a}^{-1}L$. Thus $\mathfrak{p}_0 v \subseteq \mathfrak{a}^{-1}L$, contrary to assumption. Suppose that the greatest common divisor $\mathfrak{b}$ of $\mathfrak{p}_0 R$ and $\mathfrak{d}_1$ is not (1). Then $\mathfrak{b}^2 \mid \mathfrak{p}_0 R$. Since $[\mathfrak{a}\mathfrak{d}^{-1}L_h^* : \mathfrak{b}^{-1}L_h^*]$ is prime to $\mathfrak{p}_0 R$, it follows that $v \in \mathfrak{b}^{-1}L_h^*$. Thus $\mathfrak{b}v \subseteq L_h^*$ and so $\mathfrak{b}^2 v \in L$. Thus $\mathfrak{p}_0 v \subseteq L$, contrary to assumption. This contradiction establishes the result.

THEOREM 3.15. *Suppose that if* $\mathfrak{p}$ *is any prime in* R *then*

$$\mathfrak{p} \nmid [L_h^* : \mathfrak{p}^{-1}L \cap L_h^*].$$

Let $\mathfrak{d}_1 = \prod_{i=1}^{k} \mathfrak{p}_i$. *Assume that* $[K : K_0] = 2$ *and* $\mathfrak{d}_1^2 = (c)$ *with* $c = \bar{c}$ *in* K_0. *Let* $d_h(L) = (\prod_{i=1}^{k} \mathfrak{p}_i^{m_i})\mathfrak{b}$, *where* $0 \leqslant m_i \leqslant n$ *and* $\mathfrak{b}$ *is an integral ideal of* K *which is not divisible by any* $\mathfrak{p}_i$. *Then there exist prime ideals* $\mathfrak{p}_{0i}$ *of* R_0 *such that* $\mathfrak{p}_i^2 = \mathfrak{p}_{0i}R$ *for* $i = 1, \ldots, k$. *Furthermore, there exist a* G*-invariant lattice* M *in* V_0 *and an element* c *in* K_0 *such that* M *is integral with respect to* ch_0 *and* $d_{ch_0}(M) = (\prod_{i=1}^{k} \mathfrak{p}_{0i}^{n-m_i})\mathrm{N}(\mathfrak{b})$.

Proof. The existence of the $\mathfrak{p}_{0i}$ follows from the definition of $\mathfrak{d}$. By Lemmas 3.3 and 3.13,

$$d_{h_0}((\mathfrak{a}^{-1}L)_0) = \mathrm{N}(\mathfrak{d}_1)^n \mathrm{N}(d_h(L)) = \left(\prod_{i=1}^{k} \mathfrak{p}_{0i}^{n+m_i}\right)\mathrm{N}(\mathfrak{b}).$$

By Theorem 3.8 there exist c and M having the required properties.

COROLLARY 3.16. *Let* $K_0 = \{c \mid c \in K, \bar{c} = c\}$. *Assume that* $[K : K_0] = 2$ *and* K_0 *has class number* 1. *Suppose that if* $\mathfrak{p}$ *is any prime in* R *then* $\mathfrak{p} \nmid [L_h^* : \mathfrak{p}^{-1}L \cap L_h^*]$. *If* $d_h(L) = \mathfrak{d}_1^n$, *there exist a* G*-invariant lattice* M *in* V_0 *and an element* c *in* K_0 *such that* $M_{ch_0}^* = M$.

Proof. This is a special case of Theorem 3.15.

COROLLARY 3.17. *Let* $K_0 = \{c \mid c \in K, \bar{c} = c\}$. *Assume that* $[K : K_0] = 2$, K_0 *has class number* 1, *and only one prime ramifies in* K *over* K_0. *Suppose that* (L, h) *has minimal discriminant and* $L/\mathfrak{p}L$ *is an irreducible* $R[G]$*-module for every prime* $\mathfrak{p}$ *in* K. *Then either* $d_h(L) = (1)$ *or there exist a* G*-invariant lattice* M *in* V_0 *and an element* c *in* K_0 *such that* $M_{ch_0}^* = M$.

Proof. By Theorems 3.2 and 3.8, either $d_h(L) = (1)$ or $d_h(L) = \mathfrak{d}_1^n$. The result follows from Corollary 3.16.

If, for example, $K = Q(\sqrt{-3})$ then the Suzuki group satisfies the hypotheses of Corollary 3.17 with $n = 12$ and a suitably chosen pair (L, h). It can be shown that $d_h(L) \neq (1)$. Thus by Theorem 2.8, the Suzuki group must act on an even rational unimodular lattice in dimension 24. It is of course known that it acts on the Leech lattice.

As another example, let $G : \widetilde{HaJ}$. Then if $K_1 = Q(\sqrt{5})$ and $K = K_1\sqrt{(-m)}$ for any positive rational integer, it follows that there is a faithful 6-dimensional $K[G]$-module V. It is easily seen that for any G-invariant lattice in V and any prime $\mathfrak{p}$ in K that $L/\mathfrak{p}L$ is an irreducible $R[G]$-module. Thus if $m = 3$ then Theorems 3.3 and 3.8 imply the existence of a pair (L, h) with $d_h(L) = (1)$ or $\sqrt{(-3)^6}$. It can be shown that $d_h(L) \neq (1)$. Thus by Theorem 3.8, there exists a pair (L, h) with $d_h(L) = (\sqrt{5})^6(\sqrt{(-3)})^6$. Let σ be the automorphism of K of order 2 whose fixed field is $Q(\sqrt{(-3)})$. If h^σ is not positive definite replace h by $\frac{1}{2}(1+\sqrt{5})h$. This does not change the discriminant as $\frac{1}{2}(1+\sqrt{5})$ is a unit. Thus it may be assumed that

h and h^σ are both positive definite. Theorem 3.15, with $K_0 = Q(\sqrt{(-3)})$, implies the existence of a pair (L_1, h_1), where L_1 is a G-invariant lattice in 12 dimensions over K_0 and $d_{h_1}(L_1) = (\sqrt{(-3)})^{12}$. Thus Corollary 3.16 and Theorem 2.8 imply that G acts on an even rational unimodular lattice.

More generally, all even unimodular lattices in 24 dimensions over Q have been classified ([**20**]). Thus some of these results can be used to classify groups which act on special lattices in special fields as subgroups of known groups.

4. Unitary reflection groups

Let F be a field of characteristic 0. Let V be a vector space over F and let $n = \dim_F V$. A *unitary reflection on* V is a linear transformation of finite order of V which has exactly one characteristic root unequal to 1. A finite group of linear transformations on V which is generated by unitary reflections is called an *n-dimensional finite unitary reflection group over F.*

Let G be an n-dimensional finite unitary reflection group over F. Since G is a finite group there exists an algebraic number field $K \subseteq F$ and a vector space W over K such that W is a $K[G]$-module and $V = W \otimes_K F$ is the given $F[G]$-module. If W is tensored with the complex number, it follows that G is an n-dimensional finite unitary complex reflection group.

The finite unitary complex reflection groups have been completely classified ([**22**]). The following two lemmas summarize the results that are relevant to this paper. These results can be found in [**22**], see especially Table VII on p. 301.

LEMMA 4.1. *Let H be a complex finite unitary reflection group. Then $H = H_1 \times \ldots \times H_m$, where each H_j is an irreducible complex finite unitary reflection group.*

LEMMA 4.2. *Let H be an irreducible complex n-dimensional finite unitary reflection group with $n \geqslant 8$. Then one of the following occurs:*

(i) *there exists a normal abelian subgroup H_1 of H such that $H/H_1 \approx \mathrm{S}_n$ or S_{n+1};*

(ii) *$n = 8$ and $H \approx \mathrm{W}(E_8)$, the Weyl group of type E_8.*

THEOREM 4.3. *Let p be a prime, $p \geqslant 7$. Let ζ be a primitive pth root of 1 and let F be an algebraic number field with $[F(\zeta) : F] = p-1$. Let G be a finite group and let V be an absolutely irreducible $F[G]$-module such that $\dim_F V = n$ with $8 \leqslant n \leqslant 2p-3$. Assume that G contains a unitary reflection. Then one of the following occurs:*

(i) *there exists a normal p'-subgroup G_1 of G such that G/G_1 is isomorphic to a subgroup of S_{n+1};*

(ii) $p = 7$, $n = 8$. $G \approx H\mathbf{Z}(G)$, *where* $H \approx W(E_8)$.

Proof. Since $[F(\zeta) : F] = p-1$, the character afforded by V is rational-valued on p-elements. Let P be a Sylow p-group of G. Thus $|P| = 1$ or p. If $|P| = 1$ then (i) holds with $G_1 = G$. Thus it may be assumed that $|P| = p$. Hence, in particular, $n \geqslant p-1$.

Let H be the subgroup of G generated by all the unitary reflections in G. Then $\langle 1\rangle \neq H \lhd G$. By Lemma 4.1, $V = \bigoplus_{i=1}^{m} V_i$ and $H = H_1 \times \ldots \times H_m$, where H_i is an irreducible finite unitary reflection group on V_i for $i = 1, \ldots, m$. Since $H \lhd G$, G acts as a transitive permutation group on the set $\{H_i\}$. Thus $H_i \approx H_j$ for all i, j and $\dim V_i = n/m$ for all i.

Suppose that $m > 1$. If P normalizes H_i for all i then PH_j has a faithful representation on V_j for some j. This cannot be the case as

$$\dim V_j = n/m < p-1.$$

Hence if G_1 is the kernel of the action of G on $\{H_i\}$ then G_1 is a p'-group and G/G_1 is a permutation group on m ($\leqslant n$) objects and (i) holds.

Suppose that $m = 1$. Let H_0 be the maximal normal abelian subgroup of H. Then Lemma 4.2 implies that either $H/H_0 \approx S_n$ or S_{n+1} or $H \approx W(E_8)$. The group $W(E_8)$ does not have any outer automorphisms. Hence (ii) holds in the latter cases. The group S_n has no outer automorphisms for $n \neq 6$. Thus in the former cases there exists $G_1 \lhd G$ with $G/G_1 \approx S_n$ or S_{n+1}. If $p \| G : G_1|$ then (i) holds. Suppose that $p \nmid |G : G_1|$. Then $n = p-1$ and $G/G_1 \approx S_{p-1}$. Since $P \subseteq G_1$, the Frattini argument implies that $\mathbf{N}_G(P)$ has a homomorphic image isomorphic to S_{p-1}. This is impossible as $\mathbf{C}_G(P)$ is cyclic by Schur's lemma as P acts irreducibly on V.

A result analogous to Theorem 4.3 could be proved for dimension $n \leqslant 7$. Since the finite groups which have a faithful complex representation of degree $n \leqslant 7$ are known ([2], [5], [18], and [25]), there is no point in doing this here.

I am indebted to A. Rudvalis who has informed me of the following result.

THEOREM 4.4 (Rudvalis). *Let G be a subgroup of $W(E_8)$ with $7 \| G|$. Then either G contains a normal abelian subgroup G_1 such that G/G_1 is isomorphic to a subgroup of A_9 or G' is isomorphic to one of the following:* $W(E_8)'$, $W(E_7)'$, $\widetilde{W(E_7)}'$, *or* $SU_3(3) \approx G_2(2)'$.

5. Some special G-invariant lattices

Let $K, G, V, h, \mathscr{L}_h$ be defined as in § 3. Assume in addition that V is an absolutely irreducible $K[G]$-module and K is a Galois extension of Q with the property that the map sending c to $\bar{c}$ is in the centre of the Galois group of K over Q.

Let $K_0 = \{c \mid c \in K, c = \bar{c}\}$. Then K_0 is a Galois extension of Q such that the completion of K with respect to any archimedean valuation is the field of real numbers. Choose a fixed ordering in K_0. This is equivalent to choosing a completion of K_0 with respect to a fixed archimedean valuation.

LEMMA 5.1. *Let τ be an automorphism of K. Then either $h^\tau(v,v) > 0$ for all $v \in V, v \neq 0$ or $h^\tau(v,v) < 0$ for all $v \in V, v \neq 0$. Furthermore, $|h^\tau(v,w)|^2 \leqslant |h^\tau(v,v)|\,|h^\tau(w,w)|$ for all $v, w \in V$.*

Proof. Define the $K[G]$-module V_τ as follows. $V_\tau = \{v_\tau \mid v \in V\}$, and

$$av_\tau + bw_\tau = (a^\tau v + b^\tau w)_\tau \quad \text{for all } a, b \in K,$$

$$v_\tau x = (vx)_\tau \quad \text{for all } x \in G.$$

Define $h_\tau(v_\tau, w_\tau) = h^\tau(v,w)$. Since $\bar{a}^\tau = \overline{a^\tau}$ for $a \in K$, h_τ is a G-invariant hermitian symmetric form on V_τ with respect to complex conjugation. Since V_τ is an absolutely irreducible $K[G]$-module, h_τ is either positive definite or negative definite. This implies the result.

LEMMA 5.2. *Let L be a G-invariant lattice in V. Let $c \in K$. There exist only finitely many $v \in L$ with $h(v,v) = c$.*

Proof. Let $v_0 \in V, v_0 \neq 0$ and let $a_0 = h(v_0, v_0)$. For $v, w \in V$ define $h_0(v,w) = a_0 h(v,w)$. Let $H(v,w) = \sum_\tau h_0^\tau(v,w)$, where τ ranges over all automorphisms of K. Then H is a G-invariant symmetric Q-bilinear form. By Lemma 5.1, H is positive definite. If $h(v,v) = c$ then $H(v,v) = \sum_\tau (a_0 c)^\tau$. Since L is a finitely generated module over the rational integers, there are only finitely many w in L with $H(w,w) = \sum_\tau (a_0 c)^\tau$. The result follows.

THEOREM 5.3. *Let L be a G-invariant lattice. Then* $\mathrm{Aut}((L,h))$ *is a finite group.*

Proof. Let $G_0 = \mathrm{Aut}((L,h))$. Then $G \subseteq G_0$ and so V is an irreducible $K[G_0]$-module. Choose $v_0 \in L, v_0 \neq 0$. Let $A = \{v \mid v \in L, h(v,v) = h(v_0, v_0)\}$. G_0 acts as a permutation group on A. Since V is an irreducible $K[G_0]$-module, it follows that A generates V as a vector space. Therefore G_0 acts faithfully on A. By Lemma 5.2, A is a finite set. Thus G_0 is finite.

LEMMA 5.4. *Let $L \in \mathscr{L}_h$. Let v be an element in L with $ch(v,v) = 2$ for some c in R. Define r_v by $vr_v = w - ch(w,v)v$. Then r_v is a unitary reflection and $r_v \in \mathrm{Aut}((L,h))$.*

Proof. $vr_v = -v$ and if $h(w,v) = 0$ then $wr_v = w$. Thus r_v is a unitary reflection and an isometry on V. If $w \in L$ then $ch(w,v) \in R$. Therefore $wr_v = w - ch(w,v)v \in L$. Thus $r_v \in \mathrm{Aut}((L,h))$.

THEOREM 5.5. *Let p be a prime, $p \geqslant 7$. Let ζ be a primitive pth root of 1. Suppose that $[K(\zeta) : K] = p-1$. Let $L \in \mathscr{L}_h$. Assume that $8 \leqslant n \leqslant 2p-3$ and L contains v with $ch(v,v) = 2$ for some c in R. Then one of the following occurs:*

(i) *there exists a normal p'-subgroup G_1 of G such that G/G_1 is isomorphic to a subgroup of S_{n+1};*

(ii) *$p = 7$, $n = 8$, $G \approx G_1\mathbf{Z}(G)$, where G_1 is isomorphic to a subgroup of $\mathrm{W}(E_8)$.*

Proof. Let $G_0 = \mathrm{Aut}((L,h))$. By Theorem 5.3, G_0 is finite. By Lemma 5.4, G_0 contains a unitary reflection. The result follows directly from Theorem 4.3.

6. Some results from algebraic number theory

This section contains a variety of results which will be needed in the sequel. These results are probably all known but are included here for convenience.

THEOREM 6.1. *Let K be an algebraic number field which is a subfield of the complex numbers such that $\bar{K} = K$. Let p be a prime such that $[K(\zeta) : K] = p-1$, where ζ is a primitive pth root of 1 in the complex numbers. Let h be a positive definite hermitian symmetric form on the K-vector space $K(\zeta)$ such that $h(\alpha\zeta, \beta\zeta) = h(\alpha,\beta)$ for all α,β in $K(\zeta)$. Then there exists $\eta \in K(\zeta)$ such that η^τ is real and positive for every τ in the Galois group of $K(\zeta)$ over K and $h(\alpha,\beta) = \mathrm{T}(\alpha\eta\bar{\beta})$ for $\alpha,\beta \in K(\zeta)$, where T denotes the trace from $K(\zeta)$ to K.*

Proof. For $\gamma \in K(\zeta)$ let $f_\gamma(\alpha) = \mathrm{T}(\alpha\gamma)$. Each f_γ is a linear functional on the K-space $K(\zeta)$. Thus the set of all f_γ forms a subspace W of the dual space of $K(\zeta)$. Since $K(\zeta)$ is a separable extension of K, it follows that W has a dimension $p-1$ over K. Hence W is the dual space of $K(\zeta)$. Consequently every linear functional on $K(\zeta)$ is of the form f_γ for some γ in $K(\zeta)$.

$h(\alpha, 1)$ is a linear functional on $K(\zeta)$. Therefore there exists η in $K(\zeta)$ with $h(\alpha, 1) = \mathrm{T}(\alpha\eta)$ for all $\alpha \in K(\zeta)$. Thus

$$h(\alpha, \zeta^j) = h(\alpha\zeta^{-j}, 1) = \mathrm{T}(\alpha\eta\zeta^{-j}) = \mathrm{T}(\alpha\eta\bar{\zeta}^j).$$

Let $\beta \in K(\zeta)$. Then $\beta = \sum_{j=0}^{p-2} a_j\zeta^j$ with $a_j \in K$. Hence

$$h(\alpha, \beta) = h(\alpha, \sum a_j\zeta^j) = \sum \bar{a}_j h(\alpha, \zeta^j) = \sum \bar{a}_j \mathrm{T}(\alpha\eta\bar{\zeta}^i) = \mathrm{T}(\alpha\eta\overline{\sum a_j\zeta^i}) = \mathrm{T}(\alpha\eta\bar{\beta}).$$

For $\alpha \in K(\zeta)$,

$$T(\overline{\alpha\eta}) = \overline{\mathrm{T}(\alpha\eta)} = \overline{h(\alpha, 1)} = h(1, \alpha) = \mathrm{T}(\bar{\alpha}\eta).$$

Thus $\mathrm{T}(\bar{\alpha}(\eta - \bar{\eta})) = 0$ for all $\alpha \in K(\zeta)$. Hence $\eta = \bar{\eta}$. Thus $\eta^\tau = \overline{\eta^\tau}$ for every τ in the Galois group of $K(\zeta)$ over K. Suppose that $\eta^\tau < 0$ for some τ. The weak approximation theorem at the infinite primes in $Q(\zeta)$ implies the existence of an element $\alpha \in Q(\zeta)$ such that $|\alpha^\tau|^2 > p|\eta^\tau|^{-1}$ and $|\alpha^\sigma|^2 < |\eta^\sigma|^{-1}$ for every automorphism σ of $Q(\zeta)$, $\sigma \neq \tau$. Therefore

$$0 \leqslant h(\alpha, \alpha) = \sum_\sigma |\alpha^\sigma|^2\eta^\sigma < (p-2) + |\alpha^\tau|^2\eta^\tau < (p-2) - p < 0.$$

This contradiction shows that $\eta^\tau > 0$ and completes the proof.

THEOREM 6.2. *Let F, K $(F \subseteq K)$ be number fields with $[K : F] = 2$. Let $\langle\sigma\rangle$ be the Galois group of K over F. Assume that at most one finite prime of F ramifies in K. Let $\alpha \in F$ with $(\alpha) = \mathfrak{a}\mathfrak{a}^\sigma$ for some ideal $\mathfrak{a}$ of F. Suppose further that α is positive at every real completion of F. Then $\alpha = \gamma\gamma^\sigma$ for some γ in K.*

Proof. For any valuation ν of F, let F_ν denote the completion of F at ν. By the Hasse norm theorem ([6], p. 185) it suffices to show that α is a norm in F_ν for all valuations ν.

Suppose that ν is archimedean. If F_ν is the field of complex numbers then $F_\nu = K_\nu$ and α is obviously a norm. If F_ν is the field of real numbers then α is positive in F_ν, hence α is a norm as either $F_\nu = K_\nu$ or K_ν is the field of complex numbers.

Suppose that ν is non-archimedean. Let $\mathfrak{p}$ be the prime ideal of F corresponding to ν. Suppose that $\mathfrak{p}$ does not ramify in K. If $\mathfrak{p} \neq \mathfrak{p}^\sigma$ then $K_\nu = F_\nu$ and α is clearly a norm. If $\mathfrak{p} = \mathfrak{p}^\sigma$ then since $(\alpha) = \mathfrak{a}\mathfrak{a}^\sigma$ it follows that $(\alpha) = \mathfrak{p}^{2m}\mathfrak{b}$ for some integer m and some ideal $\mathfrak{b}$ of F whose numerator and denominator are prime to $\mathfrak{p}$. Thus α is a norm in the unramified extension of K_ν over F_ν.

Since at most one finite prime ramifies in K over F it follows that (up to equivalence) there is at most one valuation ν such that α is not a norm in F_ν. The Artin reciprocity law ([1], p. 66) now implies that α is a norm in F_ν for all ν, as required.

At various points in this paper it will be convenient to use the following known results. See, for example, [19], p. 413.

THEOREM 6.3 (Kummer). *If $p = 23$ then $Q(\zeta)$ has odd class number.*

THEOREM 6.4 (Kummer, Minkowski, and Wolfskehl). *If $p \leqslant 19$ then $Q(\zeta)$ has class number* 1.

It will also be necessary to use the following result which is essentially due to Gauss and can be found in any list of tables of class numbers.

LEMMA 6.5. *$Q\sqrt{(-23)}$ has class number* 3.

THEOREM 6.6. *Let p be a prime with $p \leqslant 23$. Let ζ be a primitive pth root of* 1. *Let u be a real unit in $Q(\zeta)$ such that $u^\tau > 0$ for every automorphism τ of $Q(\zeta)$. Then there exists a real unit v in $Q(\zeta)$ with $u = v^2 = v\bar{v}$.*

Proof. Let $K = Q(\zeta)$, $F = Q(\zeta + \zeta^{-1})$. The only prime in F which ramifies in K is the unique prime of F which divides (p). Thus by Theorem 6.2, $u = \gamma\bar{\gamma}$ for some $\gamma \in K$.

Suppose first that $p \leqslant 19$. By Theorem 6.4, the class number of K is 1. In other words, the ring R of integers in K is a unique factorization domain. Hence $\gamma = \alpha/\beta$ with $(\alpha, \beta) = 1$. Thus $\beta\bar{\beta}u = \alpha\bar{\alpha}$. By unique factorization this implies that $\alpha \mid \bar{\beta}$. Hence $\bar{\beta} = \alpha w$ for some $w \in R$. Thus $\beta = \bar{\alpha}\bar{w}$ and so $u^{-1} = w\bar{w}$. Hence w is a unit in R. Thus $w = \pm\zeta^j v$ for some real unit v in R ([3], p. 158). Therefore $u = v\bar{v} = v^2$.

Suppose that $p = 23$. Let U be the group of units in F. Let U^+ be the set of all units of the form $\pm u$, where $u^\tau > 0$ is positive for every automorphism τ of $Q(\zeta)$. Let $U^{(2)}$ be the group of all units of the form $\pm u^2$ for some unit u. Then $U^{(2)} \subseteq U^+ \subseteq U$. The Dirichlet unit theorem implies that $U/U^{(2)}$ is an elementary abelian group of order 2^{10}. Let $\langle\sigma\rangle$ be the Galois group of F over Q. Then σ preserves U, U^+, and $U^{(2)}$. Since σ has order 11 and 2 is a primitive root modulo 11, it follows that σ acts irreducibly on $U/U^{(2)}$. As $U^+/U^{(2)}$ is an invariant subspace of $U/U^{(2)}$, the only possibilities are that $U = U^+$ or $U^+ = U^{(2)}$. It is easily verified that $\zeta + \zeta^{-1} \in U$, $\zeta + \zeta^{-1} \notin U^+$. Thus $U \neq U^+$ and so $U^+ = U^{(2)}$. This yields the desired result.

LEMMA 6.7. *Let p be a prime and let ζ be a primitive pth root of* 1. *Let $\alpha = \sum_{j=0}^{p-1} a_j\zeta^j$. Then*

$$T_{Q(\zeta)/Q}(\alpha\bar{\alpha}) = p\sum_{j=0}^{p-1} a_j^2 - (\sum a_j)^2.$$

Proof. By definition,

$$\alpha\bar{\alpha} = \sum_{ij=0}^{p-1} a_i a_j \zeta^{i-j} = \sum_{i=0}^{p-1} a_i^2 + \sum_{i \neq j} a_i a_j \zeta^{i-j}.$$

Since $T_{Q(\zeta^j)/Q}(\zeta^j) = -1$ for $j \not\equiv 0 \pmod{p}$, this implies that

$$T_{Q(\zeta)/Q}(\alpha\bar{\alpha}) = (p-1)\sum_{j=0}^{p-1} a_j^2 - \sum_{i \neq j} a_i a_j = p\sum_{j=0}^{p-1} a_j^2 - \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_i a_j.$$

The result follows from this.

LEMMA 6.8. *Let p be a prime, $p \equiv 7 \pmod 8$. Let ζ be a primitive pth root of 1. Let $\alpha = \sum a_j \zeta^j$, where each a_j is a rational integer. Let $\mathfrak{A}$ be the ideal in the ring of integers which is generated by a prime divisor of 2 in $Q(\sqrt{(-p)})$. Let m be the number of a_j which are odd. If $\alpha \in \mathfrak{A}$ then $m \equiv 0$ or $-1 \pmod 4$. Furthermore, $m = 0$ or $2(m-1)^2 \geqslant p-1$.*

Proof. As $\alpha \in \mathfrak{A}$, it follows that $\bar{\alpha} \in \bar{\mathfrak{A}}$ and so $\alpha\bar{\alpha} \in (2)$. Since $\alpha\bar{\alpha}$ is real this implies that $T_{Q(\zeta)/Q}(\alpha\bar{\alpha}) \equiv 0 \pmod 4$. By Lemma 6.4,

$$-m - m^2 \equiv -\sum a_j^2 - (\sum a_j)^2 \equiv p\sum a_j^2 - (\sum a_j)^2 \equiv T_{Q(\zeta)/Q}(\alpha\bar{\alpha}) \equiv 0 \pmod 4.$$

Hence $m \equiv 0$ or $-1 \pmod 4$.

Suppose that $m \neq 0$ and $2(m-1)^2 < p-1$. By multiplying α by a root of unity if necessary, it may be assumed that a_0 is odd. Let

$$M = \{j : 1 \leqslant j \leqslant p-1,\ a_j \text{ is odd}\}.$$

Let $\alpha_0 = 1 + \sum_{j \in M} \zeta^j$. Thus $\alpha - \alpha_0 \in \mathfrak{A}$ and so it may be assumed that $\alpha = \alpha_0$. Since $2(m-1)^2 < p-1$, there exists $s \not\equiv 0 \pmod p$ such that $s \not\equiv \pm j/k \pmod p$ for any $j, k \in M$. Furthermore, $-s$ has the same property. Thus it may be assumed that $\left(\frac{s}{p}\right) = 1$. Let τ be the automorphism of $Q(\zeta)$ which sends ζ to ζ^s. Then $\mathfrak{A}^\tau = \mathfrak{A}$. Hence $\bar{\alpha}\alpha^\tau \in \mathfrak{A}\bar{\mathfrak{A}} = (2)$. Therefore the coefficient of any ζ^j in $\bar{\alpha}\alpha^\tau$ is congruent modulo 2 to the coefficient of 1. Since $m^2 < p$, the coefficient of ζ^j is 0 for some j. Thus the coefficient of 1 in $\bar{\alpha}\alpha^\tau$ is even. However,

$$\bar{\alpha}\alpha^\tau = 1 + \sum_{j \in M} \zeta^{-j} + \sum_{j \in M} \zeta^{sj} + \sum_{j,k \in M} \zeta^{j-sk}.$$

Thus the coefficient of 1 is odd. This contradition establishes the result.

7. Groups of type $L_2(p)$

A finite group G is of *type* $L_2(p)$ if every composition factor of G is either a p-group, a p'-group, or isomorphic to $\mathrm{PSL}_2(p)$.

LEMMA 7.1. *Suppose that G is a group of type $L_2(p)$. Assume that $p||G|$ and $p^2 \nmid |G|$. Then either G has a subgroup of index p or a homomorphic image of G contains $p+1$ Sylow p-groups.*

Proof. If G is p-solvable then G contains a p-complement which has index p. Suppose that G is not p-solvable. Let H be the maximal normal p-solvable subgroup of G. It suffices to prove the result for G/H. Thus by changing notation, it may be assumed that G has no normal p-solvable subgroup of order greater than 1. Thus there exists $G_0 \lhd G$, $G_0 \simeq \mathrm{PSL}_2(p)$. Since $p^2 \nmid |G|$, G_0 is the subgroup of G generated by all p-elements in G. Thus G_0 contains all Sylow p-groups of G. Since $\mathrm{PSL}_2(p)$ contains exactly $p+1$ Sylow p-groups, so does G.

LEMMA 7.2. *Suppose that G is of type $L_2(p)$ with $p > 2$ and $p||G|$. Assume that G has a faithful rational valued character χ with $\chi(1) \leqslant 2p-3$. Then p is the largest prime which divides $|G|$ and $p^2 \nmid |G|$.*

Proof. A group of order p^2 does not have a rational-valued faithful character of degree less than $2(p-1)$. Thus $p^2 \nmid |G|$.

Suppose that q is a prime with $p < q$ and $q||G|$. Thus $q^2 \nmid |G|$ by the previous paragraph. Furthermore, $q \nmid |\mathrm{PSL}_2(p)|$. Since G is of type $\mathrm{L}_2(p)$, this implies the existence of a normal subgroup H of G such that either $p||H|$ and $q \nmid |H|$ or $q||H|$ and $p \nmid |H|$. In either case the Frattini argument implies that G contains a subgroup G_0 of order pq. If G_0 is cyclic, a faithful rational-valued character of G_0 has degree at least $(p-1)+(q-1) > \chi(1)$. If G_0 is not cyclic then $q \equiv 1 \pmod{p}$. Thus a faithful rational valued character of a group of order q has degree at least $q-1 \geqslant 2p > \chi(1)$. This contradiction proves the result.

8. Some local results

This section contains some results from the theory of modular characters. For general references, see [**9**], [**12**], or the papers of R. Brauer.

Throughout this section, p is a fixed prime, $p \geqslant 7$.

G is a finite group.

P is a Sylow p-group of G, $|P| = p$, $P = \langle x \rangle$.

$N = \mathbf{N}_G(P)$. $C = \mathbf{C}_G(P) = P \times H$.

Q_p is the field of p-adic numbers. F is a finite extension field of Q_p. S is the ring of integers in F and π is a prime element in S.

$\tilde{S} = S/(\pi)$, and if X is an S-module then $\tilde{X} = X/\pi X$. For any non-negative integer k, kX denotes the direct sum of k copies of X. If Y is an $\tilde{S}[G]$-module, let Y^* denote the contragredient module.

For $1 \leqslant j \leqslant p$, let V_j denote the indecomposable $\tilde{S}[P]$-module of dimension j.

LEMMA 8.1. *Let Y be an indecomposable $\tilde{S}[G]$-module on which P acts faithfully such that $Y(x-1)^{p-1} = (0)$. Then*

(i) *Y_N is indecomposable;*

(ii) *$Y_C \simeq V_d \otimes Y_1$, where d is the smallest integer such that $Y(x-1)^d = (0)$ and Y_1 is a sum of irreducible $\tilde{S}[H]$-modules which are conjugate under the action of N;*

(iii) $Y_C^* \otimes Y_C$

$$= \left(\sum_{i=1}^{d} V_{2i-1}\right) \otimes (Y_1^* \otimes Y_1) \quad \text{if } d \leqslant \tfrac{1}{2}(p-1)$$

$$= \left\{\sum_{i=1}^{s} V_{2i-1} \oplus (p-2s)V_p\right\} \otimes (Y_1^* \otimes Y_1) \quad \text{if } d = p-s,\ s \leqslant \tfrac{1}{2}(p-1).$$

Proof. By assumption, Y_N has no projective direct summand. Thus (i) follows from the Green correspondence and (ii) is an immediate consequence of (i). The formulas in (iii) are consequences of [**11**], Lemma 3.8.

THEOREM 8.2. *Suppose that G is not of type $L_2(p)$ and G is generated by its elements of order p. Let Y be an indecomposable $\tilde{S}[G]$-module on which P acts faithfully. Suppose that $Y(x-1)^d = (0)$ and $\dim Y \geqslant d+1$. Then $d \geqslant \frac{1}{3}(2p-1)$.*

Proof. Choose Y so that d is as small as possible. Let

$$Y_1^* \otimes Y_1 = \sum_{i=1}^{k} \sum_{j} Y_{ij},$$

where, for each i, $\{Y_{ij}\}$ is a set of irreducible $\tilde{S}[H]$-modules which form an orbit for the action of N. Since $\dim Y_1 > 1$ by assumption, it follows that $k \geqslant 2$. Furthermore, some Y_{ij} does not afford the trivial Brauer character.

If $d \leqslant \frac{1}{2}(p-1)$, Lemma 8.1(iii) and the Green correspondence imply that G has a representation of dimension 3 in which P is faithfully represented. This is impossible as G is not of type $\mathrm{L}_2(p)$ ([**11**], Theorem 1).

Suppose that $\frac{1}{2}(p+1) \leqslant d \leqslant \frac{2}{3}(p-1)$. Then Lemma 8.1(iii) implies that $(Y^* \otimes Y)_N$ has k direct summands whose restriction to P is a multiple of V_{2i-1} $(i = 1, \ldots, p-d)$ and $2d-p$ projective direct summands. Since G is generated by its elements of order p the only indecomposable $\tilde{S}[G]$-module on which P acts trivially is the 1-dimensional trivial module. Thus the minimality of d and the Green correspondence imply that

$$\tfrac{1}{2}(d-2)k+1 \leqslant k(2d-p) \quad \text{if } d \text{ is even,}$$

$$\tfrac{1}{2}(d-3)k+1 \leqslant k(2d-p) \quad \text{if } d \text{ is odd.}$$

If d is even, this yields $2p < 3d+2$ and so $2p \leqslant 3d+1$, as required. If d is odd, this implies that $2p < 3d+3$ and so $2p \leqslant 3d+1$, as required.

LEMMA 8.3. *Suppose that F is an unramified extension of Q_p. Let Y be an S-free $S[P]$-module on which P acts faithfully. If $\tilde{Y}(x-1)^k = (0)$ then $k \geqslant p-1$.*

Proof. Let χ be the character afforded by $Y \otimes_S F$. Since F is unramified over Q_p, it is linearly disjoint from the field of pth roots of 1 over Q_p. Thus $\chi = a\theta + b1$, where θ is the faithful rational-valued character of P of degree $p-1$ and a is some positive integer. Let $Y \otimes_S F = W_1 \oplus W_2$, where W_2 affords the character θ. Let $Y_2 = Y \cap W_2$. Then Y_2 is a pure submodule of Y and $\tilde{Y}_2 \subseteq \tilde{Y}$. Thus it suffices to prove the result in the case when $Y_2 = Y$. (An argument of this type was first used by Thompson in [**23**].) Since $\tilde{Y}(x-1)^k = (0)$, it follows that $Y(x-1)^k \subseteq pY$. Thus $\det(x-1)^k \equiv 0 \pmod{p^{p-1}}$. The characteristic values of x acting on Y are the distinct primitive pth roots of 1, namely ζ^j $(j = 1, \ldots, p-1)$. Thus $\det(x-1)^k = \{\prod_{j=1}^{p-1}(1-\zeta^j)\}^k = p^k$. Therefore $p^k \equiv 0 \pmod{p^{p-1}}$ and so $k \geqslant p-1$, as required.

THEOREM 8.4. *Suppose that F is unramified over Q_p. Let X be an S-free $S[G]$-module on which P acts faithfully such that $W = X \otimes_S F$ is absolutely irreducible and $\dim_F W = n \leqslant 2p-3$. Then one of the following holds:*

(i) *G is of type $L_2(p)$;*

(ii) *$\tilde{X}$ is an irreducible $\tilde{S}[G]$-module;*

(iii) *$n = p-1$ and $\tilde{X}$ has irreducible constituents of dimensions 1 and $p-2$ respectively.*

Proof. Let χ be the character afforded by W. Let μ be a faithful irreducible character of P. Let $\mu_0 = \mu^p$ be the principal character of P. Since F is unramified over Q_p and $\chi(1) < 2(p-1)$, it follows that

$$\chi_P = \sum_{j=1}^{p-1} \mu_j + \{\chi(1) - (p-1)\}\mu_0.$$

Suppose that neither (i) nor (ii) holds.

Let $A \lhd G$ with $P \subseteq A$. Suppose that χ_A is reducible. Then $\chi_A = \sum \theta_j$, where $\{\theta_j\}$ is a set of irreducible characters of A which are algebraically conjugate in the field $F(\zeta)$, where ζ is a primitive pth root of 1. Since $\theta_j(1) < p-1$ for all j, it follows that μ_0 occurs with multiplicity at most 1 as a constituent of θ_{jP} ([**4**]). Since each μ^j $(1 \leqslant j \leqslant p-1)$ occurs with multiplicity 1 in χ_P, μ_0 is the only common irreducible constituent of θ_{iP} and θ_{jP} for $i \neq j$. Thus $\theta_j(1) \leqslant \frac{1}{2}(p+1)$. Hence G is of type $\mathrm{L}_2(p)$, contrary to assumption ([**4**], or [**11**] Theorem 1).

Let A be the subgroup of G generated by all elements of order p. Then $P \subseteq A \lhd G$. By the previous paragraph, χ_A is irreducible. Thus it may be assumed that $G = A$ is generated by the elements of order p. Thus $G = G'$.

Since $\tilde{X}$ is reducible, there is a composition factor of $\tilde{X}$ of dimension at most $\frac{1}{2}n < p$. Suppose that such a composition factor affords a non-principal Brauer character φ. Let A be the kernel of φ. Since $G = G'$ is generated by its p-elements, A is a p'-group. Thus χ_A contains the principal character of A as a constituent and so A is in the kernel of χ. Thus $A = \langle 1 \rangle$ and φ is faithful. Since $\varphi(1) < p$ it follows that

$$\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$$

([**11**], Theorem 1). Then $\chi(1) \equiv \pm 1 \pmod{p}$ ([**4**]). Therefore $\chi(1) \leqslant p+1$ and so $\varphi(1) \leqslant \frac{1}{2}(p+1)$. If $p \geqslant 11$ then $\varphi(1) < \frac{2}{3}(p-1)$, contrary to [**11**], Theorem 1.

Suppose that $p = 7$. Then $\varphi(1) \geqslant 4$ by [**11**], Theorem 1. Hence $\chi(1) = 8$ and every irreducible Brauer constituent of χ has degree 4. Thus χ has two distinct Brauer constituents φ_1, φ_2 of degree 4. Let Y_1, Y_2 be $\tilde{S}[G]$-modules which afford φ_1, φ_2 respectively. Then ([**11**], Lemma 3.8) $(Y_i \otimes Y_j)_P \approx V_1 \oplus V_3 \oplus V_5 \oplus V_7$. If $Y_1 \approx Y_1^*$ then $Y_1 \otimes Y_2$ has no invariants. If $Y_1 \not\approx Y_1^*$ then $Y_1 \otimes Y_1$ has no invariants. Thus in either case there exists an $\tilde{S}[G]$-module W which has no invariants such that $W_P \approx V_1 \oplus V_3 \oplus V_5 \oplus V_7$. Since $G = G'$, the Green correspondence implies the existence of a faithful 3-dimensional $\tilde{S}[G]$-module, contrary to [**11**], Theorem 1.

Consequently the principal Brauer character is the only irreducible Brauer constituent of dimension at most $\frac{1}{2}n$. Thus χ is in the principal block and so $\chi(1) \equiv \pm 1 \pmod{p}$. Since the principal Brauer character is a constituent of χ, it follows that $\chi(1) \equiv -1 \pmod{p}$ and so $\chi(1) = p-1$, as required.

THEOREM 8.5. *Suppose that G is not of type $L_2(p)$. Let χ be an irreducible character of G such that P is not in the kernel of χ. Assume that $p \leqslant \chi(1) \leqslant 2p-3$ and $Q_p(\chi)$ is unramified over Q_p. Let X be an S-free $S[G]$-module such that $X \otimes_S F$ affords χ. Then $\tilde{X}_P$ has a projective direct summand.*

Proof. Every division algebra over $Q_p(\chi)$ is split by an unramified extension. Thus there exists an unramified extension F_0 of Q_p and an $F_0[G]$-module W_0 which affords χ. Let S_0 be the ring of integers in F_0 and let X_0 be an S_0-free $S_0[G]$-module with $W_0 = X_0 \otimes_{S_0} F_0$. By Theorem 8.4, $\tilde{X}_0$ is an irreducible $\tilde{S}_0[G]$-module. Thus it suffices to prove the result for X_0 in place of X. Hence by changing the notation it may be assumed that

F is unramified over Q_p. If $\tilde{X}_N$ has no projective direct summand then, by Lemma 8.1, $\tilde{X}_C \simeq V_d \otimes Y_1$ for some integer $d \leqslant p-1$. By Lemma 8.3, $d \geqslant p-1$. Since $\chi(1) = d\,(\dim Y_1)$ and $\chi(1) < 2(p-1)$ it follows that $\chi(1) = d = p-1$, contrary to assumption.

THEOREM 8.6. *Suppose that χ is an irreducible faithful character of G with $\chi(1) = p+1$. Then one of the following occurs.*

(i) *G is of type $\mathrm{L}_2(p)$.*

(ii) *$\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$.*

(iii) *$p = 7$ and there exists a normal subgroup G_1 of index at most 2 in G such that $G_1 = A\mathbf{C}_G(A)$ with $A/\mathbf{Z}(A) \approx \mathrm{A}_7$ and $|\mathbf{Z}(A)| = 2$.*

(iv) *There exists an unramified extension F_0 of Q_p and an $F_0[G]$-module W_0 which affords χ. Furthermore, there exists a finite group G_0 of linear transformations on W_0 such that $G \subseteq G_0$ and G_0 contains a unitary reflection. In particular if $p \geqslant 11$ then G contains a normal p'-subgroup G_1 such that G/G_1 is isomorphic to a subgroup of S_{p+2}.*

Proof. Suppose that (i) and (ii) do not hold. Let A be the subgroup of G generated by all elements of order p in G. Then $A \lhd G$. Choose F so that χ is afforded by an $F[G]$-module.

Suppose that χ_A is reducible. Then A has an irreducible character of degree at most $\frac{1}{2}(p+1)$ which does not have P in its kernel. If $p \geqslant 11$ then $\frac{1}{2}(p+1) < \frac{2}{3}(p-1)$, contrary to [**11**], Theorem 1. If $p = 7$ then A has a character of degree at most 4 which does not have P in its kernel. An inspection of the finite linear groups of dimension at most 4 ([**2**]) implies that $\chi_A = \theta_1 + \theta_2$, where $\theta_i(1) = 4$. If $\theta_1 \neq \theta_2$, let G_1 be the inertia group of θ_1. Then (iii) follows from the list of 4-dimensional groups. If $\theta_1 = \theta_2$ then $A/\mathbf{Z}(A) \approx \mathrm{A}_7$. Since A_7 has no outer automorphism which fixes an element of order 7, this implies that (iii) holds also in this case.

Hence it may be assumed that χ_A is irreducible. There exists an S-free $S[A]$-module Y such that $W = Y \otimes_S F$ affords χ_A and $\tilde{Y}$ is indecomposable. If $\tilde{Y}_P$ does not have a projective direct summand then, by Lemma 8.1, $\tilde{Y}_{\mathbf{C}_A(P)} \approx V_d \otimes Y_1$ for some integer $d < p$. Since $d \mid (p+1)$, this implies that $d \leqslant \frac{1}{2}(p+1) < \frac{1}{3}(2p-1)$, contrary to Theorem 8.2. Therefore $\tilde{Y}_p$ has a projective direct summand. By Burnside's transfer theorem, $|\mathbf{N}_A(P) : \mathbf{C}_A(P)| \neq 1$. Therefore $Q_p(\chi_A)$ is unramified over Q_p. Hence by Theorem 8.4, $\tilde{Y}$ is irreducible. Let X be an S-free $S[G]$-module such that $X \otimes_S F$ affords χ. Then $\tilde{X}$ is irreducible and $\tilde{X}_P$ has a projective direct summand. Consequently $Q_p(\chi)$ is unramified over Q_p. As every division algebra over $Q_p(\chi)$ is split by an unramified extension, it follows that there exists an unramified extension F_0 of Q_p which is a splitting field for χ.

Let U be the group of all roots of 1 in $Q(\chi) \subseteq F_0$. Let G_0 be the group generated by G and all scalars μI with $\mu \in U$. Thus G_0 is a finite group. Since $Q_p(\chi)$ is unramified, $p \nmid |U|$ and so (iv) will follow once it is shown that G_0 contains a unitary reflection. Thus by changing the notation, it may be assumed that $G = G_0$ and $F = F_0$.

Let X_0 be an S-free $S[G]$-module such that $X_0 \otimes_S F$ affords χ. There exists a p'-element $y \in C$, $y \notin \mathbf{Z}(G)$. Since $\bar{X}_{0N}$ has a projective direct summand $\chi_{\langle y \rangle} = p\lambda_1 + \lambda_2$, where λ_1, λ_2 are linear characters of $\langle y \rangle$, $\lambda_1(y) \neq \lambda_2(y)$. Therefore $Q(\lambda_2) \subseteq Q(\chi)$ and so $Q(\lambda_1) \subseteq Q(\chi)$. Thus G contains the scalar $\lambda_1(y)^{-1}I$. Hence G contains an element with one characteristic root $\lambda_1^{-1}\lambda_2(y) \neq 1$ which has 1 as a characteristic root with multiplicity p. This is the required unitary reflection. The last statement follows from Theorem 4.3.

COROLLARY 8.7. *Suppose that $p \geqslant 11$ and G is not of type $\mathrm{L}_2(p)$. Assume that $\mathbf{Z}(G) = \langle 1 \rangle$ and $|G : G'| = 2$. Suppose that G has a faithful real-valued irreducible character χ of degree $p+1$. Then G has a normal p'-subgroup G_1 such that G/G_1 is isomorphic to a subgroup of S_{p+2}.*

Proof. By Theorem 8.6, it may be assumed that $\mathbf{C}_G(P) = P$. Let μ be the faithful linear character of G/G'. By Theorem 8.4, $\chi_{G'}$ is irreducible. Thus $\chi, \mu\chi$ ($\chi \neq \mu\chi$) are real characters of G which are in the principal p-block of G. By Theorem 8.4, both χ and $\mu\chi$ are irreducible as Brauer characters modulo p. Thus $\chi, \mu\chi$, and the principal character are all three end-points of the real stem of the tree corresponding to the principal block. This is clearly impossible.

9. Some structure theorems

Let K, R, G, V, n, h be defined as in § 3. In addition, the following notation and assumptions will be used throughout this section.

p is a prime which does not ramify in K.

ζ is a primitive pth root of 1. Thus $[K(\zeta) : K] = p-1$ and $R[\zeta] = \{\sum a_j \zeta^j \mid a_j \in R\}$ is the ring of integers in $K(\zeta)$. It is assumed that $K(\zeta)$ is contained in the fixed completion chosen in § 3.

x is an element of order p in G such that 1 occurs with multiplicity $n-(p-1)$ as a characteristic root of x acting on V. $P = \langle x \rangle$. Thus $|P| = p$.

Since p does not ramify in K, the character afforded by the $K[P]$-module V is rational-valued. Thus for $j = 1, \ldots, p-1$, ζ^j occurs as a characteristic root with multiplicity 1 in x acting on V.

If $p||G|$ and $n \leqslant 2p-3$ then any element x of order p satisfies these conditions. Furthermore, P is a Sylow p-group of G.

As was mentioned in the introduction, the results of this section were all proved by J. G. Thompson in the case when $K = Q$ and $d_h(L) = (1)$.

LEMMA 9.1. *Let* $u = \sum_{j=1}^{p-1} x^j \in R[P]$. *Then* $R[P]/uR[P] \approx R[\zeta]$ *and* $K[P]/uK[P] \approx K(\zeta)$. *If* M *is an* $R[P]$*-module such that* $vx \neq v$ *for all* $v \in M$, $v \neq 0$, *then* M *is an* $R[\zeta]$*-module.*

Proof. This is clear.

For $\gamma \in K(\zeta)$, define $x(\gamma)$ by $\alpha x(\gamma) = \alpha\gamma$. For τ in the Galois group of of $K(\zeta)$ over K, define y_τ by $\alpha y_\tau = \alpha^\tau$. Thus $x(\gamma)$ and y_τ are K-linear transformations on $K(\zeta)$ and $y_\tau^{-1}x(\gamma)y_\tau = x(\gamma^\tau)$. In this notation, $x = x(\zeta)$.

Let $\mathfrak{A}$ be a fractional ideal of $K(\zeta)$. Let η be an element of $K(\zeta)$ such that η^τ is real and positive for all τ in the Galois group of $K(\zeta)$ over K. Let T denote the trace from $K(\zeta)$ to K. Then $\mathfrak{A}$ is a lattice in $K(\zeta)$ which is an $R[P]$-module and $h_0(\alpha, \beta) = \mathrm{T}(\alpha\eta\bar{\beta})$ is a P-invariant positive definite hermitian symmetric form on $K(\zeta)$. Let $(\mathfrak{A}, \eta)$ denote the pair consisting of the lattice $\mathfrak{A}$ and the form h_0.

THEOREM 9.2. *Let* $(\mathfrak{A}, \eta)$ *be as above.*

(i) *If* τ *is in the Galois group of* $K(\zeta)$ *over* K *then* y_τ *is an isometry from* $(\mathfrak{A}, \eta)$ *onto* $(\mathfrak{A}^\tau, \eta^\tau)$.

(ii) *If* $\gamma \in K(\zeta)$, $\gamma \neq 0$, *then* $x(\gamma)$ *is an isometry from* $(\mathfrak{A}, \eta)$ *onto* $(\mathfrak{A}\gamma, \eta(\gamma\bar{\gamma})^{-1})$.

(iii) *Let* $y \in \mathrm{Aut}(\mathfrak{A}, \eta)$ *be such that* $y^{-1}xy = x^t$. *Let* τ *be the element of the Galois group of* $K(\zeta)$ *over* K *such that* $\zeta^\tau = \zeta^t$. *Then* $y = y_\tau x(\gamma)$ *for some* $\gamma \in K(\zeta)$.

Proof. (i) and (ii) are clear. It is easily seen that $y_\tau^{-1}y$ commutes with $x = x(\zeta)$. Thus by Schur's lemma, $y_\tau^{-1}y = x(\gamma)$ for some γ in $K(\zeta)$. This proves (iii).

THEOREM 9.3. *Let* M *be a finitely generated* $R[P]$*-module which is torsion free as an* R *module. Let* $W = M \otimes_R K$. *Assume that* x *acts non-trivially on* M *and* $\dim_K W = p-1$. *Let* h_0 *be a positive definite* P*-invariant hermitian symmetric form on* W. *Let* M^* *denote the dual of* M *with respect to* h_0. *Then the following hold.*

(i) $vx \neq v$ *for all* $v \in W$, $v \neq 0$, *and* $W \simeq K[\zeta]$ *as a* $K[P]$*-module.*

(ii) *There exists* $\eta \in K(\zeta) = W$ *such that* η^τ *is real and positive for every* τ *in the Galois group of* $K(\zeta)$ *over* K *and such that* $h_0(\alpha, \beta) = \mathrm{T}(\alpha\eta\bar{\beta})$, *where* T *denotes the trace from* $K(\zeta)$ *to* K.

(iii) *There exist a fractional ideal* $\mathfrak{A}$ *of* $K(\zeta)$ *and an isometry* f *from* (M, h_0) *onto* $(\mathfrak{A}, \eta)$ *which is an* $R[P]$*-homomorphism.*

(iv) *Let f be defined as in* (iii). *Then* $f(M^*) = \mathfrak{A}^{-1}\eta^{-1}(1-\zeta)^{-(p-2)}$.

(v) $M \subseteq M^*$ *if and only if* $\mathfrak{A}\mathfrak{A}\eta(1-\zeta)^{p-2}$ *is an integral ideal of* $K(\zeta)$. *In that case*

$$M^*/M \approx \frac{R[\zeta]}{\mathfrak{A}\mathfrak{A}\eta(1-\zeta)^{p-2}}.$$

(vi) $[M^* : M] = N_{K(\zeta)/K}(\mathfrak{A}\mathfrak{A}\eta(1-\zeta)^{p-2})$, *where* $N_{K(\zeta)/K}$ *denotes the norm from* $K(\zeta)$ *to* K.

Proof. (i) x acting on W does not have 1 as a characteristic root since $\dim_K W = p-1$ and K is linearly disjoint from $Q(\zeta)$ over Q. Thus $W \approx K(\zeta)$ by Lemma 8.1.

(ii) This follows from Theorem 6.1.

(iii) This is clear by (ii).

(iv) By definition,

$$f(M^*) = \{\beta \mid \beta \in K(\zeta),\ \mathrm{T}(\beta\eta\bar{\alpha}) \in R \quad \text{for all } \alpha \in \mathfrak{A}\}.$$

The different of the extension of $K(\zeta)$ over K is the ideal $(1-\zeta)^{p-2}$. Thus

$$\begin{aligned} f(M^*) &= \{\beta \mid \beta \in K(\zeta),\ \beta\eta\bar{\alpha} \in (1-\zeta)^{-(p-2)} \text{ for all } \alpha \in \mathfrak{A}\} \\ &= \{\beta \mid \beta \in K(\zeta),\ \beta \in \mathfrak{A}^{-1}\eta^{-1}(1-\zeta)^{-(p-2)}\} = \mathfrak{A}^{-1}\eta^{-1}(1-\zeta)^{-(p-2)} \end{aligned}$$

(v) By (iv), $M \subseteq M^*$ if and only if $\mathfrak{A} \subseteq \mathfrak{A}^{-1}\eta^{-1}(1-\zeta)^{-(p-2)}$. In that case,

$$M^*/M \approx \frac{\mathfrak{A}^{-1}\eta^{-1}(1-\zeta)^{-(p-2)}}{\mathfrak{A}} \approx \frac{R[\zeta]}{\mathfrak{A}\mathfrak{A}\eta(1-\zeta)^{p-2}}.$$

(vi) This is an immediate consequence of (v).

THEOREM 9.4. *Suppose that* $n \geqslant p$. *Let* $L \in \mathscr{L}_h$. *Let* $M = L(1-x)$ *and let* $L_1 = \{v \mid v \in L,\ vx = v\}$.

(i) M *is an* $R[P]$*-module,* $M \otimes_R K$ *has dimension* $p-1$ *over* K *and* $M \perp L_1$.

(ii) $M \oplus L_1 \subseteq M_h^* \oplus L_{1h}^*$.

(iii) $[L : M \oplus L_1] = pR$.

(iv) $d_h(M)d_h(L_1) = p^2 d_h(L)$.

Proof. (i) For $j = 1, \ldots, p-1$, ζ^j occurs as a characteristic root with multiplicity 1 in x acting on V. Thus $M \otimes_R K = V(1-x)$ has dimension $p-1$ over K. If $v \in L$ and $w \in L_1$ then

$$h(v, w) = h(vx, wx) = h(vx, w).$$

Therefore $h(v - vx, w) = 0$. Thus $M \perp L_1$.

(ii) This is clear.

(iii)
$$L/M \oplus L_1 \approx \frac{L(1-x)}{(M \oplus L_1)(1-x)} \approx \frac{M}{M(1-x)}.$$

The determinant of $1-x$ on M is $\prod_{j=1}^{p-1}(1-\zeta^j)=p$. Thus

$$[M : M(1-x)] = pR,$$

as required.

(iv) This follows from (iii) and Lemma 2.3.

THEOREM 9.5. *Suppose that $n=p-1$ and K is a real field. Let $L \in \mathscr{L}_h$.*

(i) *If $\mathfrak{p}$ is a prime divisor of p in R then an odd power of $\mathfrak{p}$ divides $d_h(L)$. Furthermore $(p)\,|\,d_h(L)$.*

(ii) *Assume that $p \geqslant 7$ and G is not of type $L_2(p)$. Suppose further that $\mathfrak{p}^{in+1} \nmid d_h(L)$ for any prime divisor $\mathfrak{p}$ of p in R. Then $d_h(L) = p\mathfrak{a}$ for some ideal $\mathfrak{a}$ of R which is prime to p.*

Proof. (i) Let $(p) = \prod \mathfrak{p}_j$, where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ are distinct prime ideals of R. Let $\mathfrak{p}_j = \mathfrak{P}_j^{p-1}$, where $\mathfrak{P}_j$ is a prime ideal in $R[\zeta]$. If $\mathfrak{B}$ is a fractional ideal of $K(\zeta)$ such that $\mathfrak{P}_j$ divides neither the numerator nor the denominator of $\mathfrak{B}$, let $\nu_j(\mathfrak{P}_j^s\mathfrak{B}) = s$ for any rational integer s.

By Theorem 9.3, the pair (L, h) is isometric to the pair $(\mathfrak{A}, \eta)$, where $\mathfrak{A}$ is a fractional ideal of $K(\zeta)$ and η is a suitable real element in $K(\zeta)$. Since $\overline{\mathfrak{P}}_j = \mathfrak{P}_j$ it follows that $\nu_j(\mathfrak{A}\overline{\mathfrak{A}})$ is even. As K is a real field, $K(\zeta+\zeta^{-1})$ is the real subfield of $K(\zeta)$. For each j, $\mathfrak{P}_j^2$ is a prime ideal in $R[\zeta+\zeta^{-1}]$. Thus $\nu_j((\eta))$ is even as $\eta \in K(\zeta+\zeta^{-1})$. Since $(1-\zeta) = \prod \mathfrak{P}_j$, it follows that $\nu_j((1-\zeta)^{p-2}) = p-2$ is odd. Consequently $\nu_j(\mathfrak{A}\overline{\mathfrak{A}}\eta(1-\zeta)^{p-2})$ is odd. As $\mathfrak{p}_j = N_{K(\zeta)/K}(\mathfrak{P}_j)$, Theorem 8.5 implies that $\mathfrak{p}_j\,|\,d_h(L)$ for each j. Hence $(p)\,|\,d_h(L)$.

(ii) By Theorems 3.2 and 8.4, $\mathfrak{p}^2 \nmid d_h(L)$ for any prime divisor $\mathfrak{p}$ of p in R. The result follows from (i).

In particular, Theorem 9.5 implies that if $p \geqslant 7$, G is not of type $L_2(p)$ and G has a faithful real representation of degree $p-1$ then this representation is reducible modulo every prime divisor of p in a real splitting field. This fact can be proved directly by local methods and will be exploited more fully elsewhere. It should be observed that if K is not a subfield of the field of real numbers then the conclusion of Theorem 9.5 is false. Numerous counter-examples exist. If $p=7$ then for instance $U_3(3)$ and $\widetilde{HaJ}$ are counter-examples.

THEOREM 9.6. *Suppose that $p \leqslant n \leqslant 2p-3$. Let $L \in \mathscr{L}_h$ be such that $d_h(L)$ is prime to p. Let $M = L(1-x)$ and let $L_1 = \{v \mid v \in L, vx = v\}$. Assume that one of the following holds:*

(i) *K is a real field;*

(ii) *for every prime divisor $\mathfrak{p}$ of p in R, $L/\mathfrak{p}L$ has a projective direct summand as an $R/\mathfrak{p}\,[P]$-module.*

Then $d_h(M) = p\mathfrak{a}$, $d_h(L_1) = p\mathfrak{b}$ for ideals $\mathfrak{a}, \mathfrak{b}$ of R which are prime to p.

Proof. Let $\mathfrak{p}$ be a prime divisor of p in R. By Theorem 9.4(iv), $\mathfrak{p}^3 \nmid d_h(M)$ and $\mathfrak{p}^3 \nmid d_h(L_1)$. Thus it suffices to show that $\mathfrak{p} \mid d_h(M)$ and $\mathfrak{p} \mid d_h(L_1)$.

If K is a real field then Theorem 9.5(i) applied to M implies that $\mathfrak{p} \mid d_h(M)$ and $\mathfrak{p}^2 \nmid d_h(M)$. Thus the result follows from Theorem 9.4(iii).

Suppose that assumption (ii) is satisfied. Let $R_\mathfrak{p}$ denote the completion of R at $\mathfrak{p}$. For any R-module X, let $X_\mathfrak{p} = X \otimes_R R_\mathfrak{p}$. If $\mathfrak{p} \nmid d_h(L_1)$ then $(L_{1h}^*)_\mathfrak{p} = L_{1\mathfrak{p}}$. Thus by Theorem 9.4(ii),

$$M_\mathfrak{p} \oplus L_{1\mathfrak{p}} \subseteq L_\mathfrak{p} \subseteq (M_h^*)_\mathfrak{p} \oplus L_{1\mathfrak{p}}.$$

This implies that $L_{1\mathfrak{p}}$ is a direct summand of $L_\mathfrak{p}$. Similarly, if $\mathfrak{p} \nmid d_h(M)$ then $M_\mathfrak{p}$ is a direct summand of $L_\mathfrak{p}$. In either case it follows that as an $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}[P]$-module $L_\mathfrak{p}/\mathfrak{p}L_\mathfrak{p}$ cannot have a projective direct summand contrary to assumption (ii).

10. Further structure theorems

Throughout this section, the hypotheses and notation of § 9 will be used. In addition, the following assumptions and notation will be used.

$p \geqslant 7$, G is not of type $\mathrm{L}_2(p)$.

V is an absolutely irreducible $K[G]$-module. $n \leqslant 2p-3$.

$|\mathbf{N}_G(P) : \mathbf{C}_G(P)| = e$.

τ is an element of order e in the Galois group of $K(\zeta)$ over K.

$\mathbf{N}_G(P)$ is said to be *split* if there exists $y \in \mathbf{N}_G(P)$ of order e such that $\mathbf{N}_G(P) = \langle y \rangle \mathbf{C}_G(P)$.

Suppose that the pair (L, h) has minimal discriminant. Define $M = M(L)$ as follows:

$$M = L \qquad \text{when } n = p-1,$$
$$M = L(1-x) \quad \text{when } n \geqslant p.$$

LEMMA 10.1. *Suppose that (p) is a prime ideal in R. Let $\pi = 1-\zeta$. Then $(\pi)^{p-1} = (p)$ and (π) is a prime ideal of $R[\zeta]$. Suppose that $\eta \in K$ with $\bar{\eta} = \eta^\tau = \eta$ such that neither the numerator nor the denominator of $(\eta)(\gamma\bar{\gamma})^{-1}$ is divisible by any prime divisor of p, where $(\gamma) = (\pi)^k$. Then there exists a unit u and an element η_0 in $K(\zeta)$ such that $\eta_0^\tau = \bar{\eta}_0 = \eta_0$ and $\eta = \eta_0 u\bar{u}\gamma\bar{\gamma}$.*

Proof. The first statement is clear by the Hilbert decomposition theorem. Since $\eta^\tau = \eta$, it follows that $(\eta) = \mathfrak{B}(\pi)^{em}$ for some ideal $\mathfrak{B}$ whose numerator and denominator are prime to p and for some integer m. Then $(\pi)^{em} = (\gamma\bar{\gamma}) = (\pi)^{2k}$ and so em is even. If e is odd, let

$$\beta = \prod_{i=1}^{e} \{\pi^{\frac{1}{2}m}\}^{\tau^i}.$$

Thus $\{\beta\bar{\beta}\}^\tau = \beta\bar{\beta}$. If e is even, let $\beta = \prod_{i=1}^{\frac{1}{2}e}\{\pi^m\}^{\tau^i}$. Thus $\{\beta\bar{\beta}\}^\tau = \beta\bar{\beta}$. In either case, $(\beta\bar{\beta}) = (\gamma\bar{\gamma})$. Let $\eta = \eta_0\beta\bar{\beta}$. Then ${\eta_0}^\tau = \bar{\eta}_0 = \eta_0$. Furthermore, $\beta\gamma^{-1} = u$ is a unit. Therefore $\beta\bar{\beta} = uu\gamma\bar{\gamma}$ as required.

THEOREM 10.2. *Suppose that the pair (L,h) has minimal discriminant and $\mathfrak{p}^{[\frac{1}{2}n]+1} \nmid d_h(L)$ for any prime divisor $\mathfrak{p}$ of (p) in K.*

(i) *If K is a real field then $\mathbf{N}_G(P)$ is split.*

(ii) *If $\mathbf{N}_G(P)$ is split then the pair (M,h) is isometric to $(\mathfrak{A},\eta)$ for some fractional ideal $\mathfrak{A}$ of $K(\zeta)$ and suitable $\eta \in K(\zeta)$ such that $\mathfrak{A}^\tau = \mathfrak{A}$ and $\eta^\tau = \eta$.*

(iii) *Suppose that $\mathbf{N}_G(P)$ is split and (p) is a prime ideal in K. Assume that either $n \geqslant p$ or K is a real field. Then the pair (M,h) is isometric to $(\mathfrak{A}(1-\zeta), \eta/p)$, where $\mathfrak{A}^\tau = \mathfrak{A}$, $\eta^\tau = \eta$, and the numerator and denominator of $\mathfrak{A}$ are both prime to p.*

Proof. By Theorem 9.3, the pair (M,h) is isometric to $(\mathfrak{A},\eta)$ for suitable $\mathfrak{A}$ and η. By abuse of language, (M,h) will be identified with $(\mathfrak{A},\eta)$. By Theorem 9.2, there exists $\gamma \in K$ such that $y_\tau x(\gamma) \in \mathbf{N}_G(P)$ and $\{y_\tau x(\gamma)\}^e \in \mathbf{C}_G(P)$. Thus $\{y_\tau x(\gamma)\}^e = x(\beta)$, where $\beta = \prod_{i=1}^{e}\gamma^{\tau^i}$.

(i) Since $x(\beta)$ has finite order, β is a root of unity in K. Thus $\beta = \pm 1$ as K is a real field. If $\beta = 1$, let $y = y_\tau x(\gamma)$. Suppose that $\beta = -1$. If e were even then some power of τ would be complex conjugation in $K(\zeta)$ as K is a real field. Hence $\beta > 0$, contrary to the fact that $\beta = -1$. Thus e is odd. Let $y = y_\tau x(-\gamma)$. Then $y^e = 1$, as required.

(ii) Let $y = y_\tau x(\gamma)$. Then $\prod_{i=0}^{e-1}\gamma^{\tau^i} = 1$. Hilbert's Theorem 90 implies that $\gamma = \alpha^{1-\tau}$ for some $\alpha \in K(\zeta)$. By Theorem 9.2, the map sending v to $v\alpha$ defines an isometry from $(\mathfrak{A},\eta)$ onto $(\mathfrak{A}\alpha, \eta(\alpha\bar{\alpha})^{-1})$. Furthermore, if $v \in K(\zeta)$ then

$$v\{\alpha y_\tau x(\gamma)\alpha^{-1}\} = v^\tau\alpha^\tau\gamma\alpha^{-1} = v^\tau.$$

Therefore $(\mathfrak{A}\alpha)^\tau = \mathfrak{A}\alpha$ and the map sending v to v^τ is an isometry of $(\mathfrak{A}\alpha, \eta(\alpha\bar{\alpha})^{-1})$. Consequently if T denotes the trace from $K(\zeta)$ to K and if $v, w \in K(\zeta)$ then

$$\mathrm{T}(v\bar{w}\eta(\alpha\bar{\alpha})^{-1}) = \mathrm{T}(v^\tau\bar{w}^\tau\eta(\alpha\bar{\alpha})^{-1}) = \mathrm{T}(v\bar{w}\{\eta(\alpha\bar{\alpha})^{-1}\}^{\tau^{-1}}).$$

Thus $\{\eta(\alpha\bar{\alpha})^{-1}\}^\tau = \eta(\alpha\bar{\alpha})^{-1}$. This yields the required result.

(iii) If either $n \geqslant p$ or K is a real field then Theorems 8.5, 9.5, and 9.6 imply that $d_h(M) = p\mathfrak{a}$ for some integral ideal $\mathfrak{a}$ of K which is relatively prime to p. By (ii), (M,h) may be identified with $(\mathfrak{A}\gamma(1-\zeta), \eta/p)$, where $\eta^\tau = \eta$, $\{\mathfrak{A}\gamma\}^\tau = \mathfrak{A}\gamma$, the numerator and denominator of $\mathfrak{A}$ are both prime to p, and (γ) is a product of powers of divisors of p in $K(\zeta)$. Thus $\mathfrak{A}^\tau = \mathfrak{A}$. Let $\pi = 1-\zeta$. By Lemma 10.1, $(\gamma) = (\pi)^k$ for some k. By Theorems 8.3,

8.5, and 8.6.

$$p\mathfrak{a} = d_h(M) = \mathrm{N}_{K(\zeta)/K}\left(\mathfrak{A}\bar{\mathfrak{A}}\gamma\bar{\gamma}\frac{(1-\zeta)^p}{p}\eta\right) = p\mathrm{N}_{K(\zeta)/K}(\mathfrak{A}\bar{\mathfrak{A}}\gamma\bar{\gamma}\eta).$$

Therefore $\mathfrak{A}\bar{\mathfrak{A}}\gamma\bar{\gamma}\eta$ is an integral ideal of $R[\zeta]$ which is prime to p. Thus Lemma 10.1 implies the existence of a unit u and an element $\eta_0 \in K$ with $\eta_0{}^\tau = \bar{\eta}_0 = \eta_0$ such that $n = \eta_0 u\bar{u}\gamma\bar{\gamma}$. By Theorem 9.2 the isometry $x(\gamma u)^{-1}$ sends $(\mathfrak{A}\gamma(1-\zeta), \eta/p)$ onto $(\mathfrak{A}u^{-1}(1-\zeta), \eta_0/p)$. Since u is a unit, $\mathfrak{A}u^{-1} = \mathfrak{A}$, and the result follows.

THEOREM 10.3. *Let $K_0 = \{c \mid c \in K, \bar{c} = c\}$. Let $L \in \mathscr{L}_h$ be such that (L, h) has minimal discriminant and $p^{[\frac{1}{2}n]+1} \nmid d_h(L)$ for any prime divisor $\mathfrak{p}$ of (p) in K. Assume that $\mathrm{N}_G(P)$ is split and one of the following assumptions is satisfied:*

(i) $e = p-1$, $K = K_0$;

(ii) $e = p-1$, $n \geqslant p$;

(iii) $p \equiv 3 \pmod 4$, $K = K_0$, *and* $e = \frac{1}{2}(p-1)$.

Then $d_h(M) = p\mathfrak{a}^{p-1}$ for some ideal $\mathfrak{a}$ in R which is not divisible by any prime that ramifies in K over K_0.

Proof. Let τ be an element of the Galois group of $K(\zeta)$ over K of order e. By Theorem 10.2(ii), (M, h) is isometric to $(\mathfrak{A}(1-\zeta), \eta/p)$, where $\mathfrak{A}$ is an ideal of $K(\zeta)$ with $\mathfrak{A}^\tau = \mathfrak{A}$ and $\eta^\tau = \eta = \bar{\eta}$. By Theorem 9.3(vi), $d_h(M) = p\mathfrak{b}$, where $\mathfrak{b} = N_{K(\zeta)/K}(\mathfrak{A}\bar{\mathfrak{A}}\eta)$ and $N_{K(\zeta)/K}$ is the norm from $K(\zeta)$ to K. In all cases $\mathfrak{b}$ is an ideal of R which is not divisible by any prime divisor of (p). In case (i), this follows from Theorem 9.5. In case (ii), it follows from Theorems 8.4, 8.5, and 9.6. In case (iii) it follows from Theorems 9.5 and 9.6.

In cases (i), (ii), and (iii), $\mathfrak{A}\bar{\mathfrak{A}}\eta$ is an ideal of $K(\zeta)$ which is prime to (p) and is fixed by every element of the Galois group of $K(\zeta)$ over K. Thus $\mathfrak{A}\bar{\mathfrak{A}}\eta = \mathfrak{a}$ is an ideal of K. Suppose that $\mathfrak{a}$ is divisible by a prime $\mathfrak{q}$ of K which ramifies in K over K_0. Then we must be in case (ii) as $K \neq K_0$. Hence by Theorem 10.2(ii), it may be assumed that $\eta \in K_0$ and $\mathfrak{A} = \mathfrak{a}_0\mathfrak{B}$ where $\mathfrak{a}_0$ is an ideal of K and $\mathfrak{B}$ is an ideal of $K(\zeta)$ whose numerator and denominator are products of divisors of (p). Thus $\mathfrak{A}\bar{\mathfrak{A}}\eta = \mathfrak{a}_0\bar{\mathfrak{a}}_0\mathfrak{B}\bar{\mathfrak{B}}\eta$. Hence $\mathfrak{q}$ divides η to an even power and $\mathfrak{q}$ divides $\mathfrak{a}_0\bar{\mathfrak{a}}_0$ to an even power. Then $\mathfrak{q}^2 \mid \mathfrak{a}$. Hence $\mathfrak{q}^{2(p-1)} \mid \mathfrak{b} = \mathfrak{a}^{p-1}$. Consequently $\mathfrak{q}^{2(p-1)} \mid d_h(L)$, which is impossible as $2(p-1) > n$ by Theorems 3.2 and 3.4. Thus $\mathfrak{b} = \mathfrak{a}^{p-1}$, and the result is proved for these cases.

COROLLARY 10.4. *Let $K_0 = \{c \mid c \in K, \bar{c} = c\}$. Assume that $\mathrm{N}_G(P)$ is split and $e = p-1$. Suppose that either $K = K_0$ or $n \geqslant p$. Then there exists a pair (L, h) with $L \in \mathscr{L}_h$ of minimal discriminant such that either $d_h(M) = (p)$*

or $d_h(M) = p\mathfrak{q}^{p-1}$ *for some prime ideal* $\mathfrak{q}$ *of* K *which is a non-principal prime ideal of* K_0. *If, furthermore,* K_0 *has class number* 1 *and* (p) *is a prime ideal of* K *then there exists* (L', h') *with* $L' \in \mathscr{L}_{h'}$ *such that* $(M(L'), h')$ *is isometric to* $((1-\zeta), 1/p)$ *and* $\mathrm{Aut}((L', h'))$ *contains a unitary reflection.*

Proof. By Corollary 3.9, there exists $L \in \mathscr{L}_h$ such that (L, h) has minimal discriminant and $\mathfrak{p}^{[\frac{1}{2}n]+1} \nmid d_h(L)$ for any prime divisor $\mathfrak{p}$ of (p) in K. If for some prime ideal $\mathfrak{q}$ of K, $\mathfrak{q}^{[\frac{1}{2}n]+1} \mid d_h(L)$ then $\mathfrak{q} \mid d_h(M)$ as $p-1 > \frac{1}{2}n$. Thus by Theorem 10.3, $d_h(M) = p\mathfrak{a}^{p-1}$, where $\mathfrak{a}$ is the product of all the distinct prime ideals $\mathfrak{q}$ in K with $\mathfrak{q}^{[\frac{1}{2}n]+1} \mid d_h(L)$. The first statement now follows from Corollary 3.9.

If K_0 has class number 1 then the first statement implies that $d_h(M) = (p)$. If (p) is a prime ideal of K then Theorem 10.2(iii) implies that (M, h) is isometric to $(\mathfrak{a}(1-\zeta), \eta/p)$, where $\mathfrak{a}$ is an ideal of $K, \eta \in K_0$ and $\mathfrak{a}\bar{\mathfrak{a}}\eta = (1)$. Let $(L', h') = (\mathfrak{a}^{-1}L, \eta^{-1}h)$. Then h' is clearly G-invariant and $\mathfrak{a}^{-1}L \in \mathscr{L}_{\eta^{-1}h}$ by Lemma 2.2. Furthermore $(M(L'), h')$ is isometric to $((1-\zeta), 1/p)$. Since

$$\mathrm{T}_{K(\zeta)/K}\frac{(|1-\zeta|^2)}{p} = 2.$$

Lemma 5.4 implies that $\mathrm{Aut}(L', h')$ contains a unitary reflection.

COROLLARY 10.5. *Suppose that* $p \equiv 3 \pmod 4$, K *is a real field and* $e = \frac{1}{2}(p-1)$. *Then there exists a pair* (L, h) *with* $L \in \mathscr{L}_h$ *of minimal discriminant such that either* $d_h(M) = (p)$ *or* $d_h(M) = p\mathfrak{q}^{p-1}$ *for some non-principal prime ideal* $\mathfrak{q}$ *of* K.

Proof. By Corollary 3.9, there exists $L \in \mathscr{L}_h$ such that (L, h) has minimal discriminant and $\mathfrak{p}^{[\frac{1}{2}n]+1} \nmid d_h(L)$ for any prime divisor $\mathfrak{p}$ of (p) in K. Thus by Theorem 10.3, $d_h(M) = p\mathfrak{a}^{p-1}$, where $\mathfrak{a}$ is the product of all the distinct prime ideals $\mathfrak{q}$ in K with $\mathfrak{q}^{[\frac{1}{2}n]+1} \mid d_h(L)$. The result follows from Corollary 3.9.

THEOREM 10.6. *Suppose that* $p \equiv 3 \pmod 4$ *and* $n = p+1$. *Let* (L, h) *have minimal discriminant such that* $\mathfrak{p}^{\frac{1}{2}n+1} \nmid d_h(L)$ *for any prime divisor* $\mathfrak{p}$ *of* p *in* K. *Suppose that* G *acts on* V *as a group of unimodular linear transformations and* $\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$. *Assume that* K *is a Galois extension of* Q *with an abelian Galois group and one of the following hypotheses is satisfied:*

(i) (p) *is a prime in* K *and there exists* y *of order* 2 *in* $\mathbf{N}_G(P) \setminus \mathbf{C}_G(P)$;

(ii) $K = Q(i)$ *and there exists an element of order* 4 *in* $\mathbf{N}_G(P) \setminus \mathbf{C}_G(P)$.

Then $\mathrm{Aut}((L, h))$ *contains a unitary reflection.*

Proof. Since $p \equiv 3 \pmod 4$, (p) is a prime in K in both cases. Let G_1 be the group generated by G and all scalars of determinant 1. Without

loss of generality it may be assumed that $G = G_1$. Thus if (ii) holds then $iI \in G$ and so also (i) is satisfied. Therefore it suffices to prove the conclusion if (i) holds. Assume now that (i) holds.

Let σ be the element of order 2 in the Galois group of $K(\zeta)$ over K. By Theorems 9.3 and 10.2(iii), (M, h) is isometric to $(\mathfrak{A}(1-\zeta), \eta/p)$, where $\mathfrak{A}^\sigma = \mathfrak{A}$, $\eta^\sigma = \eta$, and the numerator and denominator of $\mathfrak{A}$ are prime to p. Thus, in particular, if $\alpha \in \mathfrak{A}$ then $\alpha^\sigma \equiv \alpha \pmod{\mathfrak{A}(1-\zeta)}$. Furthermore, $(M_h^* \cap p^{-1}M, h)$ is isometric to $(\mathfrak{A}, \eta)$. By Theorem 9.2, there exists $\gamma \in Q(\zeta)$ such that $\alpha y = \alpha^\sigma \gamma$ or, equivalently, $y = y_\sigma x(\gamma)$. Since $y_\sigma \in \mathrm{Aut}((L, h))$, this implies that $x(\gamma) \in \mathrm{Aut}((L, h))$. Thus by Theorem 5.3, γ is a root of unity. Hence $\gamma = \varepsilon\zeta^j$, where $\varepsilon^k = 1$ and $p \nmid k$. Since y has order 2, $1 = \gamma\gamma^\sigma = \varepsilon^2$ and so $\varepsilon = \pm 1$. Consequently, if $\alpha \in \mathfrak{A}$ then $\alpha y = \varepsilon\zeta^j\alpha^\sigma$. This implies that $\alpha y \equiv \varepsilon\alpha \pmod{\mathfrak{A}(1-\zeta)}$ for all $\alpha \in \mathfrak{A}$.

Let z be the linear transformation of V defined as follows. If $v \in M \otimes_R K$ then $vz = vy$, if $v \in L_1 \otimes_R K$ then $vz = \varepsilon v$. Clearly z is an isometry of V. Furthermore, $(M \oplus L_1)z = M \oplus L_1$ and if $v \in (M_h^* \cap p^{-1}M) \oplus (L_{1h}^* \cap p^{-1}L_1)$ then $vz - \varepsilon v \in M \oplus L_1$. By Theorems 8.4 and 9.6,

$$L \subseteq (M_h^* \cap p^{-1}M) \oplus (L_{1h}^* \cap p^{-1}L).$$

Thus by Theorem 2.9(ii), $L = \langle M \oplus L_1, \alpha + w \rangle$ for suitable $\alpha \in \mathfrak{A}$, $w \in L_{1h}^* \cap p^{-1}L$. Hence $Lz = L$ and so $z \in \mathrm{Aut}((L, h))$. Therefore

$$y_1 = yz \in \mathrm{Aut}((L, h)) \quad \text{and} \quad {y_1}^2 = 1.$$

Furthermore, $vy_1 = v$ for $v \in M \otimes_R K$ and so y_1 has 1 as a characteristic value with multiplicity at least $p-1$. Thus if it can be shown that $\det y_1 = -1$ then y_1 is the required unitary reflection.

The group $\langle y \rangle P$ is a Frobenius group. Therefore the characteristic values of y, and hence of z, acting on $M \otimes_R K$ are $+1$ and -1, each with multiplicity $\frac{1}{2}(p-1)$. The characteristic values of z on $L_1 \otimes_R K$ are both ε. Thus $\det z = (-1)^{\frac{1}{2}(p-1)}\varepsilon^2 = -1$. Therefore

$$\det y_1 = \det y \det z = \det z = -1,$$

as was to be shown.

11. Some results in the case when $K = Q$

Throughout this section the notation and assumptions of § 9 will be used with $K = Q$.

If $L \in \mathrm{L}_h$ is such that (L, h) has minimal discriminant define $M = M(L)$ as follows:

$$M = \begin{cases} L & \text{when } n = p-1, \\ L(1-x) & \text{when } n \geqslant p. \end{cases}$$

LEMMA 11.1. *Suppose that $L \in \mathscr{L}_h$ such that (L,h) has minimal discriminant. Assume that if q is a prime with $q \geqslant 2p-1$ then $(q) \nmid d_h(L)$. Assume further that $(p)^2 \nmid d_h(M)$. If $\frac{1}{2}(p-1)$ is a prime then $d_h(M) = (pa^{p-1})$ for some integer a which is prime to p.*

Proof. By Theorems 9.3 and 9.4, (M,h) is isometric to $(\mathfrak{A}(1-\zeta), \eta/p)$ for suitable $\mathfrak{A}, \eta$, where $pN_{Q(\zeta)/Q}(\mathfrak{A}\overline{\mathfrak{A}}\eta) = d_h(M)$. If $(1-\zeta) \mid \mathfrak{A}\overline{\mathfrak{A}}\eta$ then $(1-\zeta)^2 \mid \mathfrak{A}\overline{\mathfrak{A}}\eta$ as $(\overline{1-\zeta}) = (1-\zeta)$ and $\eta \in Q(\zeta+\zeta^{-1})$. Thus an odd power of p divides $d_h(M)$. Hence by assumption, $d_h(M) = (pb)$ for some positive integer b which is prime to p. Let $\mathfrak{Q}$ be a prime ideal in $Q(\zeta)$ which divides $\mathfrak{A}\overline{\mathfrak{A}}\eta$. Let q be the rational prime with $\mathfrak{Q} \mid q$. Let f be the residue-class degree of q in $Q(\zeta)$ over Q. Thus $f = 1, 2, \frac{1}{2}(p-1)$, or $p-1$. If $f = 1$ or 2 then $q^2 \equiv 1 \pmod{p}$ and so $q \geqslant 2p-1$. By assumption, $(q) \nmid d_h(M)$. If $f = p-1$ then $(q) = \mathfrak{Q}$ and so $q^{p-1} \mid b$. If $f = \frac{1}{2}(p-1)$ then $\mathfrak{Q} \neq \overline{\mathfrak{Q}}$. Thus $\mathfrak{Q}\overline{\mathfrak{Q}} \mid \mathfrak{A}\overline{\mathfrak{A}}\eta$ and so $(q)^{p-1} = \mathrm{N}_{Q(\zeta)/Q}(\mathfrak{Q}\overline{\mathfrak{Q}}) \mid \mathfrak{b}$. By Theorem 3.4, this implies that q^{p-1} is the exact power of q which divides b, as was to be shown.

LEMMA 11.2. *Suppose that $7 \leqslant p \leqslant 19$. Let $L \in \mathscr{L}_h$ be such that (L,h) has minimal discriminant. Assume that $d_h(M) = (p)$. Then L contains a vector w with $h(w,w) = 2$.*

Proof. By Theorems 9.3 and 9.4, (M,h) is isometric to $(\mathfrak{A}(1-\zeta), \eta/p)$ for suitable $\mathfrak{A}, \eta$. By Theorem 6.4, $Q(\zeta)$ has class number 1. Then by Theorem 9.2, (M,h) is isometric to $((1-\zeta), \eta/p)$. By Theorem 9.3, $\mathrm{N}_{Q(\zeta)/Q}(\eta) = (1)$. Thus η is a unit in $Q(\zeta+\zeta^{-1})$ such that every conjugate of η is positive. By Theorem 6.5, $\eta = u\bar{u}$ for some unit u in $Q(\zeta)$. Thus by Theorem 9.2, (M,h) is isometric to $((1-\zeta)u, 1/p) = ((1-\zeta), 1/p)$. Since

$$\mathrm{T}_{Q(\zeta)/Q}\left(\frac{|1-\zeta|^2}{p}\right) = 2$$

by Lemma 6.7, the result is proved.

12. Proofs of Theorems A, B, and C

Proof of Theorem A. If G of type $\mathrm{L}_2(p)$, the result follows from Lemma 7.1. Suppose that G is not of type $\mathrm{L}_2(p)$. Let V be the $Q[G]$-module of dimension $n < 2(p-1)$ over Q. By Theorem 10.2(i), $\mathrm{N}_G(P)$ is split. By Corollary 10.4, there exists a G-invariant quadratic form h on V and $L \in \mathscr{L}_h$ such that $\mathrm{Aut}((L,h))$ contains a unitary reflection. By Lemma 5.3, $\mathrm{Aut}((L,h))$ is finite. Thus by Theorem 4.3, either the result is proved or $G = \mathbf{Z}(G)H$, where H is an irreducible subgroup of $\mathrm{W}(E_8)$. The character table of $\mathrm{W}(E_7)$ shows that $\mathrm{W}(E_7)$ does not have an irreducible character of degree 8 ([**16**]). Similarly the character table

of $SU_3(3)$ shows that $SU_3(3)$ does not have an irreducible character of degree 8. The result is then an immediate consequence of Theorem 4.4.

LEMMA 12.1. *Let p be a prime and let G be a finite group whose Sylow p group P has order p. Assume that $|\mathbf{N}_G(P):\mathbf{C}_G(P)| = 2$ and $G = G' \subseteq S_{p+2}$. Then $p = 2^k - 1$ and $G \simeq SL_2(2^k)$.*

Proof. The group G acts as a permutation group on a set Ω consisting of $p+2$ elements. Let a, b be the elements of Ω which are fixed by P. Let $G_{a,b}$ be the subgroup of G consisting of all permutations on $\Omega \setminus \{a, b\}$. By a result of Ito (see [**17**] or [**13**], I, Theorem 4) $P \lhd G$ as $p \equiv 3 \pmod 4$. Thus $G_{a,b} = P$ or $|G_{a\,b}| = 2p$. Since $G' = G$, $G_{a,b}$ cannot contain an odd permutation. Thus $|G_{a,b}| \neq 2p$. Therefore $G_{a,b} = P$.

If G is not transitive on Ω then either G has two orbits of sizes 2 and p or of sizes 1 and $p+1$ respectively. In the first case $|G| = 2p$, contrary to the fact that $G = G'$. In the second case $|G| = (p+1)p$ and G is a Frobenius group, contrary to $G = G'$. Thus it may be assumed that G is transitive on Ω. Hence $|G| = (p+2)pm$, where $m \mid p+1$. If G contains a transposition then $G \approx S_{p+2}$ contrary to $|\mathbf{N}_G(P):\mathbf{C}_G(P)| = 2$. Thus $\mathbf{C}_G(P) = P$. Therefore $m \equiv 1 \pmod p$ by Sylow's theorem. Thus $m = 1$ or $m = p+1$. If $m = 1$ then $|G| = p(p+2)$ is odd, which is impossible. Thus $m = p+1$. Hence G is a triply transitive permutation group on $p+2$ letters and no element of $G \setminus \{1\}$ fixes three points of Ω. The result follows from a theorem of Zassenhaus ([**26**]).

Proof of Theorem B. Let G be a minimal counter-example to Theorem B. If $G \neq G'$ then the minimality of G implies that $p = 2^k - 1$ and $G' \approx SL_2(2^k)$. No outer automorphism of $SL_2(2^k)$ centralizes P. Since $\mathbf{Z}(G) = \langle 1 \rangle$, this implies that $G = G'$, and the result is proved. Thus it may be assumed that $G = G'$.

Suppose that $G \subseteq G_0$, where G_0 contains a unitary reflection and G_0 is a finite linear group in dimension $p+1$. Since $|\mathbf{N}_G(P):\mathbf{C}_G(P)| = 2$, it follows from Theorems 4.3 and 4.4 that there exists a normal p'-subgroup G_1 of G such that G/G_1 is isomorphic to a subgroup of S_{p+2}. Hence by Lemma 11.1, $p = 2^k - 1$ and $G/G_1 \approx SL_2(2^k)$ as required.

Thus it may be assumed that G is not contained in a $(p+1)$-dimensional finite linear group which contains a unitary reflection. Since

$$|\mathbf{N}_G(P):\mathbf{C}_G(P)| = 2$$

and G is not p-solvable it follows that G is not of type $L_2(p)$. Thus by Theorem 8.6, $\mathbf{C}_G(P) = P$ as $\mathbf{Z}(G) = \langle 1 \rangle$ by assumption. Therefore χ is in the principal p-block. Consequently χ is the only character of degree $p+1$ in the principal p-block and so χ is rational-valued. By the Brauer–

Speiser theorem, the Schur index of χ is at most 2 (see, for example, [**10**]). There exist a finite set of primes $\{q_i\}$ such that χ is not split at Q_{q_i}. Let m be a positive rational integer such that $\left(\frac{-m}{q_i}\right) = -1$ for all i and $\left(\frac{-m}{p}\right) = -1$. Then $K = Q(\sqrt{(-m)})$ is a splitting field for χ and (p) is a prime in K. Since $\mathbf{C}_G(P) = P$, it follows that there exists y of order 2 in $\mathbf{N}_G(P)$. By Corollary 3.9, there exists a G-invariant hermitian symmetric form h and $L \in \mathscr{L}_h$ such that (L, h) has minimal discriminant and $(p)^{\frac{1}{2}(p+1)+1} \nmid d_h(L)$. Thus $G \subseteq \mathrm{Aut}((L, h))$. By Theorem 10.6, $\mathrm{Aut}((L, h))$ contains a unitary reflection contrary to hypothesis. The proof is complete.

Proof of Theorem C. Let V be the $Q[G]$-module of dimension n over Q. There exists a G-invariant symmetric form h on V and $L \in \mathscr{L}_h$ such that (L, h) has minimal discriminant. By Corollary 3.9, $(q)^{[\frac{1}{2}n]+1} \nmid d_h(L)$ for any prime q. Let M, L_1 be defined as in § 10. Since V is a $Q[G]$-module, no prime $q \geqslant 2p-1$ divides $|G|$. If G is of type $\mathrm{L}_2(p)$ the result follows from Lemma 7.1. If G is not of type $\mathrm{L}_2(p)$ then Theorems 9.5 and 9.6 imply that $(p)^2 \nmid d_h(M)$. Hence by Lemma 11.1, $d_h(M) = (p)$. By Lemma 11.2, L contains a vector w with $h(w, w) = 2$. By Lemma 5.4, $\mathrm{Aut}((L, h)$ contains a unitary reflection. The result now follows from Theorems 4.3 and 4.4.

13. The case when $K = Q$ and $p \leqslant 19$

Throughout this section the hypotheses and notation of § 9 will be used. In addition it is assumed that

$$K = Q, \quad n = p - 1.$$

LEMMA 13.1. *Suppose that* $p = 13$, 17, *or* 19 *and* G *is not of type* $L_2(p)$. *Let* $L \in \mathrm{L}_h$ *so that* (L, h) *has minimal discriminant. Then* V *is absolutely irreducible. Either* G *has a subgroup of index* p *or* (L, h) *is isometric to* $((1-\zeta), \eta/p)$, *where one of the following holds:*

(i) $p = 13$ *and* $\eta = \frac{1}{2}(5+\sqrt{13})$;

(ii) $p = 17$ *and* $\eta = \frac{1}{2}(5+\sqrt{17})$;

(iii) $p = 19$ *and* (η) *is a prime divisor of* 7 *in* $Q(\zeta+\zeta^{-1})$. *Furthermore,*

$$|\mathbf{N}_{\mathrm{Aut}((L,h))}(P) : \mathbf{C}_{\mathrm{Aut}((L,h))}(P)| = 6 \text{ and } \mathrm{Aut}((L, h))' \cap \mathbf{Z}(\mathrm{Aut}((L, h))) = \langle 1 \rangle.$$

Proof. If V is not absolutely irreducible then G has a faithful character of degree at most $\frac{1}{2}(p-1)$ and so is of type $\mathrm{L}_2(p)$ ([**11**], Theorem 1), contrary to assumption.

By Theorem 5.3, $\mathrm{Aut}((L,h))$ is finite. Thus it clearly suffices to prove the result in the case when $G = \mathrm{Aut}((L,h))$.

Since $\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$ ([**11**], Theorem 1), it follows that if G_1 is the subgroup of G generated by all elements of order p in G then $G_1 = G_1'$ and G/G_1 is abelian. Thus $G_1 = G'$. Let χ be the character afforded by the $Q[G]$-module V. Since G is not of type $\mathrm{L}_2(p)$, Theorem 8.4 implies that $\chi_{G'}$ is in the principal p-block of G'. Thus G' has no normal p'-subgroup other than $\langle 1\rangle$. Hence $G' \cap \mathbf{Z}(G) = \langle 1\rangle$.

By Theorem 9.3, (L,h) is isometric to $(\mathfrak{A}(1-\zeta), \lambda/p)$ for suitable $\mathfrak{A}, \lambda$. By Theorem 6.4, $Q(\zeta)$ has class number 1. Thus Theorem 9.2 implies that (L,h) is isometric to $((1-\zeta), \eta/p)$ for a suitable real η in $Q(\zeta)$ all of whose conjugates are positive.

By Corollary 3.13, $(q)^{\frac{1}{2}n+1} \nmid d_h(L)$ for any prime q. By Theorem 9.5, $d_h(L) = (pa)$ for some positive integer a which is not divisible by p. By Theorem 9.3, $a = \mathrm{N}_{Q(\zeta)/Q}(\eta)$.

Let λ be an element of $Q(\zeta+\zeta^{-1})$ all of whose conjugates are positive such that $(\eta) = (\lambda)$. Then $\lambda = \eta\mu$ for some unit u in $Q(\zeta+\zeta^{-1})$ all of whose conjugates are positive. By Theorem 6.2, $u = v\bar{v}$ for some unit v in $Q(\zeta)$. Thus by Theorem 9.2, $((1-\zeta), \eta/p) = ((1-\zeta)v, \eta/p)$ is isometric to $((1-\zeta), \eta u/p) = ((1-\zeta), \lambda/p)$.

Suppose that $a = 1$. By Lemma 11.2, L contains a vector w with $h(w,w) = 2$.

It follows from Lemma 5.4 that G contains a unitary reflection. Hence Theorem 4.3 implies that G has a subgroup of index p. Thus it may be assumed that $a \neq 1$.

Let $e = |\mathrm{N}_G(P) : \mathbf{C}_G(P)|$. Since $\bar{\eta} = \eta$ and $(\overline{1-\zeta}) = (1-\zeta)$, it follows that e is even.

Let q be a prime which divides a. Since G has a rational-valued faithful character of degree $p-1$, one sees that $q < p$. If $q \geqslant 11$ then G is not of type $\mathrm{L}_2(q)$ by Lemma 7.2. Hence by Theorems 3.2 and 8.4, $q \nmid d_h(L)$. Thus $q \leqslant 7$. If, furthermore, q^m is the exact power of q which divides a then $q^m \equiv 1 \pmod{p}$, $e \mid m$, and by Theorem 3.2, $0 < m \leqslant \frac{1}{2}(p-1)$. Thus, in particular, $e \neq p-1$.

Suppose that $p = 17$. Then 3, 5, and 7 are primitive roots (mod 17). Hence a is a power of 2. Since 2 has order 8 (mod 17), this implies that $a = 2^8$. Hence (η) is a prime divisor of 2 in $Q(\zeta)$. Hence $(\eta) = (\frac{1}{2}(5 \pm \sqrt{17}))$, and the result follows in this case by applying a field automorphism if necessary.

Suppose that $p = 19$. The order of 2, 3, and 5 (mod 19) is divisible by 9. Thus if $q = 2$, 3, or 5 and $q^m \mid a$ then m is even and $9 \mid m$. Since $m \leqslant 9$ this implies that $m = 0$. Therefore $a = 7^m$. The order of 7 (mod 19) is 3.

Thus $6 \mid m$ and $m \leqslant 9$. Hence $m = 6$. Therefore $7^6 = a = \mathrm{N}_{Q(\zeta)Q}(\eta)$. Since $\eta = \bar{\eta}$, (η) is a prime divisor of 7 in $Q(\zeta + \zeta^{-1})$. Let $\gamma = \zeta + \zeta^7 + \zeta^{11}$. Let $\lambda = (\gamma + \bar{\gamma}) + (\gamma + \bar{\gamma})^2$. Then it may be verified that (λ) is a prime divisor of 7 in $Q(\zeta + \zeta^{-1})$. Hence $(\eta) = (\lambda^\sigma)$ for some automorphism σ of $Q(\zeta)$. Thus (L, h) is isometric to $((1-\zeta), \lambda^\sigma/p)$. Since λ is fixed by the automorphism of $Q(\zeta)$ of order 3, it follows that $3 \mid e$. Thus $e = 6$, and the result is proved in this case.

Suppose that $p = 13$. Assume that $e \mid 4$. Let $e_1 = |\mathrm{N}_{G'}(P) : P|$. By Theorem 10.2, $\mathrm{N}_G(P)$ is split. Thus if $e = 4$ then $\mathrm{N}_G(P)$ contains an element with determinant -1. Thus $e_1 \mid 2$. Since G is not p-solvable, $e_1 \neq 1$ by Burnside's transfer theorem. If $e_1 = 2$ then the principal p-block of G' contains a character of degree $p-2$. By [**13**], I, Theorem 2, $p \neq 13$. Thus $e \nmid 4$ and so $3 \mid e$. As e is even, this implies that $e = 6$.

Let q be a prime dividing a. Let q^m be the exact power of q dividing a. Then $m = 6$. Thus $q^6 \equiv 1 \pmod{13}$. Hence $q \neq 2$, 5, or 7. Therefore $a = 3^6$. Since $\eta = \bar{\eta}$, this implies that (η) is a prime divisor of 3 in $Q(\zeta + \zeta^{-1})$. Thus $\eta = (\frac{1}{2}(5 \pm \sqrt{13}))$, and the result follows by applying a field automorphism if necessary.

LEMMA 13.2. *Suppose that $p = 13$, 17, or 19 and G is not of type $L_2(p)$. Assume that G does not have a subgroup of index p. Let $G_0 = \mathrm{Aut}((L, h))$, where (L, h) is one of the lattices listed in Lemma* 13.1. *Then G_0 does not have a subgroup of index p and G_0 is not contained in a finite group of linear transformations of dimension $p-1$ which contains a unitary reflection.*

Proof. Choose $L \in \mathscr{L}_h$ so that (L, h) has minimal discriminant. By Lemma 13.1, $G \subseteq G_0$. Then clearly G_0 does not have a subgroup of index p. The last statement follows directly from Theorem 4.3.

LEMMA 13.3. *Suppose that $p = 19$ and G is not of type $L_2(p)$. Then G has a subgroup of index* 19.

Proof. By Lemma 13.2, it may be assumed that $G = \mathrm{Aut}((L, h))$, where (L, h) is as in Lemma 13.1(iii). By [**11**], Theorem 1,

$$\mathbf{C}_G(P) = P \times \mathbf{Z}(G).$$

Suppose that $17 \mid |G|$. By Theorem 10.2, there exists $y \in \mathrm{N}_G(P)$, $y \notin \mathbf{C}_G(P)$, with $y^2 = 1$. Thus $y \notin G'$ as y has determinant -1. Let $H = \langle G', y \rangle$. Then $|H : H'| = 2$ and $\mathbf{Z}(H) = \langle 1 \rangle$. Corollary 8.7 implies the existence of a normal $17'$-subgroup H_1 such that H/H_1 is isomorphic to a subgroup of S_{19}. If $19 \mid |H_1|$ then the Frattini argument implies the existence of a subgroup of order 19.17, which is impossible as G has a faithful 18-dimensional rational-valued character. Thus $19 \mid |H : H_1|$ and

so H has a subgroup of index 19, as required. Thus it may be assumed that $17 \nmid |G|$.

Let $H = G'$. Thus $\mathbf{C}_H(P) = P$ and $|\mathbf{N}_H(P) : P| = 3$. Thus the principal block is the only p-block of H of positive defect. Let χ be the character afforded by the $Q[H]$-module V. By Theorems 8.4 and 9.5, $\chi \leftrightarrow \varphi_0 + \varphi_1$, where φ_0 is the principal Brauer character and φ_1 is an irreducible Brauer character. Let X be the irreducible $R/(p)\,[G]$-module which affords φ_1. Then the Green correspondence and [**11**], Lemma 3.8, imply that $X \otimes X$ has an indecomposable direct summand Y which has no invariants such that $\dim Y \equiv 3 \pmod{19}$ and $\dim Y \leqslant \frac{1}{2}(17)(17+1) = 9.17$, the dimension of the space of symmetric tensors. Thus Y cannot contain X as a constituent of multiplicity at least 16 and so Y has an irreducible constituent in the principal block which does not afford either of the Brauer characters φ_0 or φ_1. Therefore χ^2 has an irreducible constituent θ with $\theta \neq \chi$, $\theta(1) \neq 1$. Hence $\theta(1) \leqslant \frac{1}{2}\chi(1)(\chi(1)+1) = 171$. The tree corresponding to the principal block is one of

Thus if $\theta(1) \equiv 1$ or $-3 \pmod{19}$ then $\theta(1) - 17$ is a degree. If $\theta(1) \equiv -1$ or $3 \pmod{19}$ then $\theta(1) + 17$ is a degree. Hence the degree of every character in the principal block is at most 187. By using [**13**], II, Theorem 4, and the fact that $H = H'$ and $17 \nmid |G|$, it is straightforward to verify that there are no possible sets of degrees.

LEMMA 13.4. *Let $p = 13$ or 17. Let $\eta = \frac{1}{2}(5+\sqrt{p})$. Let α be an integer in $Q(\zeta)$ such that $\mathrm{T}_{Q(\zeta)/Q}(\alpha\bar{\alpha}\eta) = \frac{5}{2}(p-1)$. Then $\alpha = \pm\zeta^j$ for some j.*

Proof. Let T_0 denote the trace from $Q(\zeta)$ to $Q(\eta)$. Let T denote the trace from $Q(\zeta)$ to Q. Choose a complex primitive pth root ζ of 1 such that $\mathrm{T}_0(\zeta) = \frac{1}{2}(-1+\sqrt{p})$. If $0 < j < p$ then $\mathrm{T}_0(\zeta^j) = \frac{1}{2}\left(-1+\left(\frac{j}{p}\right)\sqrt{p}\right)$, where $\left(\frac{j}{p}\right)$ is the Legendre symbol. Since $\bar{\gamma} = \gamma$ for $\gamma \in Q(\eta)$ and (2) is a prime ideal in $Q(\eta)$, it follows that $\mathrm{T}_0(\alpha\bar{\alpha})$ is even for every integer α in $Q(\zeta)$.

Let α be an integer in $Q(\zeta)$ with $\mathrm{T}(\alpha\bar{\alpha}\eta) = \frac{5}{2}(p-1)$. Let $\alpha = \sum_{j=0}^{p-1} a_j\zeta^j$. Then each a_j is a rational integer. Since $\sum_{j=0}^{p-1}\zeta^j = 0$, it may be assumed that $|\sum_{j=0}^{p-1} a_j| \leqslant \frac{1}{2}(p-1)$. Since $\mathrm{T}_0(\alpha\bar{\alpha})$ is even it follows that $\mathrm{T}_0(\alpha\bar{\alpha}) = b + c\sqrt{p}$, where b, c are rational integers. As every conjugate of $\alpha\bar{\alpha}$ is real and positive, it follows that $b > |c|\sqrt{p}$. $\mathrm{T}_0(\alpha\bar{\alpha})\eta = \frac{1}{2}(5b+pc+(b+5c)\sqrt{p})$. Therefore

$$5b + pc = \mathrm{T}(\alpha\bar{\alpha}\eta) = \tfrac{5}{2}(p-1). \tag{13.5}$$

Hence

$$5b = \tfrac{5}{2}(p-1) - pc < \tfrac{5}{2}(p-1) + b\sqrt{p}.$$

Therefore $(5-\sqrt{p})b < \frac{5}{2}(p-1)$ and so

$$b < \frac{5(p-1)(5+\sqrt{p})}{2(25-p)}. \tag{13.6}$$

By Lemma 6.7,

$$2b = \mathrm{T}(\alpha\bar{\alpha}) = p\sum a_j^2 - (\sum a_j)^2.$$

By (13.5), $2b \equiv -1 \pmod{p}$. Thus $(\sum a_j)^2 \equiv 1 \pmod{p}$ and so

$$|\sum a_j| \equiv 1 \pmod{p}.$$

As $|\sum a_j| \leqslant \frac{1}{2}(p-1)$ this implies that

$$|\sum a_j| = 1, \quad 1 + 2b = p\sum a_j^2. \tag{13.7}$$

If $b = \frac{1}{2}(p-1)$ then (13.7) implies that $\sum a_j^2 = 1$. Hence $\alpha = \pm\zeta^i$ for some i, as required.

Suppose that $b = \frac{1}{2}(3p-1)$. Then (13.7) implies that $\sum a_j^2 = 3$. Hence if α is multiplied by a suitable root of 1 it may be assumed that $\alpha = 1 + \zeta^j - \zeta^k$ for j, k distinct and non-zero. Hence

$$\alpha\bar{\alpha} = 3 + (\zeta^j + \zeta^{-j}) - (\zeta^k + \zeta^{-k}) - (\zeta^{j-k} + \zeta^{k-j}).$$

Consequently

$$\mathrm{T}_0(\alpha\bar{\alpha}) = b + \left\{\left(\frac{j}{p}\right) - \left(\frac{k}{p}\right) - \left(\frac{j-k}{p}\right)\right\}\sqrt{p}.$$

Thus c is odd and $|c| \leqslant 3$. However (13.5) implies that $c \equiv 0 \pmod{5}$, so this case cannot occur. Thus it may be assumed that $b \geqslant \frac{1}{2}(5p-1)$.

Suppose that $p = 13$. By (13.6), $b < \frac{5}{2}(5+\sqrt{13}) < \frac{1}{2}(5p-1)$, contrary to assumption.

Suppose that $p = 17$. By (13.6), $b < 25 + 5\sqrt{17} < \frac{1}{2}(7p-1)$. Thus as $b \geqslant \frac{1}{2}(5p-1)$ and $2b \equiv -1 \pmod{p}$, it follows that $b = 42$. Hence $\sum a_j^2 = 5$. Thus after multiplying by a suitable root of unity, it may be assumed that either $\alpha = 2 - \zeta^j$ or $\alpha = 1 + \zeta^j + \zeta^k - \zeta^s - \zeta^t$ where j, k, s, t are all distinct and non-zero. If $\alpha = 2 - \zeta^j$ then $\alpha\bar{\alpha} = 5 - 2(\zeta^j + \zeta^{-j})$ and so $\mathrm{T}_0(\alpha\bar{\alpha}) = 42 \pm 2\sqrt{17}$. Hence $c = 2$, contrary to (13.5). Thus

$$\alpha = 1 + \zeta^j + \zeta^k - \zeta^s - \zeta^t.$$

By (13.5), $c = -10$. By considering the value of $\mathrm{T}_0(\alpha\bar{\alpha})$, this implies that j, k, $j-k$, and $s-t$ are not quadratic residues mod 17 and $j-s$, $k-s$, $j-t$, $k-t$, s, t are quadratic residues mod 17. By replacing α by a conjugate with respect to an automorphism which leaves η fixed, it may be assumed that $j = 3$. A straightforward verification shows that it is impossible to satisfy these conditions. Hence this case cannot occur and the proof is complete.

LEMMA 13.8. *Suppose that $p = 13$ or 17 and G is not of type $L_2(p)$. Then G has a subgroup of index p.*

Proof. By Lemma 13.2, it may be assumed that $G = \mathrm{Aut}((L,h))$, where (L,h) is as in Lemma 13.1(i) or (ii). Let $L_0 = (1/p)L \cap L_h^*$. Then L_0 is a G-invariant lattice (though L_0 is not integral with respect to h). (L_0,h) is isometric to $((1), (5+\sqrt{p})/p$. By Lemma 13.3, the only integers in $Q(\zeta)$ with $\mathrm{T}_{Q(\zeta)/Q}\{\alpha\bar{\alpha}(\frac{1}{2}(5+\sqrt{p})/p)\} = \frac{5}{2}(p-1)$ are the elements $\pm\zeta^j$ for $0 \leqslant j \leqslant p-1$. Since G acts linearly, this implies that G acts as a transitive permutation group on the collection of p sets $\{\pm\zeta^j\}$ $(0 \leqslant j \leqslant p-1)$. Hence G has a subgroup of index p, as required.

LEMMA 13.9. *Theorem* D *is true for $p \leqslant 19$.*

Proof. If $p \leqslant 5$, the result follows from a check of the known groups in dimension at most 4. If $p = 7$ or 11, the result follows from Theorem C. If $p = 13$, 17, or 19, the result follows from Lemmas 13.3 and 13.8.

14. The case when $p = 23$

Throughout this section, the hypotheses and notation of § 9 will be used with $K = Q$.

Let $|\mathbf{N}_G(P) : \mathbf{C}_G(P)| = e$.

If (L,h) has minimal discriminant with $L \in \mathscr{L}_h$, let $L_1 = \{v \mid v \in L, vx = v\}$. Define $M = M(L)$ as follows:

$$M = \begin{cases} L & \text{if } n = p-1, \\ L(1-x) & \text{if } n \geqslant p. \end{cases}$$

Let $L_1 = \{v \mid v \in L, vx = v\}$. Of course $L_1 = L_1(L)$ depends on L.

It will further be assumed that $p = 23$ and $n \leqslant 24$.

In view of Lemma 13.9, it is enough to handle these cases to prove Theorems D, E, and F.

LEMMA 14.1. *Suppose that G is not of type $L_2(p)$. Let $L \in \mathscr{L}_h$ such that (L,h) has minimal discriminant and L contains no vector w with $h(w,w) = 2$. Then (M,h) is isometric to $(\mathfrak{A}(1-\zeta), 1/(2p))$, where $\mathfrak{A}$ is a prime divisor of (2) in $Q(\zeta)$.*

Proof. Let τ be an automorphism of $Q(\zeta)$ of order e. By Theorem 10.2 (M,h) is isometric to $(\mathfrak{A}(1-\zeta), \eta/p)$, where $\mathfrak{A}^\tau = \mathfrak{A}$, $\eta^\tau = \eta$, and the numerator and denominator of $\mathfrak{A}$ are relatively prime to p. By Theorems 9.4 and 11.1, $\mathfrak{A}\bar{\mathfrak{A}}\eta = (1)$.

If $\mathfrak{A}$ is a principal ideal then by Theorem 9.2 (M,h) is isometric to $((1-\zeta), \lambda/p)$ for some $\lambda = \bar{\lambda}$ all of whose conjugates are positive. Furthermore $(\lambda) = (1)$. Thus λ is a unit. Thus by Theorem 6.6, $\lambda = v\bar{v}$ for some

unit v of $Q(\zeta)$. Hence by Theorem 9.2, (M, h) is isometric to

$$((1-\zeta)v, 1/p) = ((1-\zeta), 1/p)$$

and so M contains the element $1-\zeta$ with $T_{Q(\zeta)/Q}(|1-\zeta|^2/p) = 2$ contrary to assumption. Hence $\mathfrak{A}$ is not a principal ideal.

If e is even then $\mathfrak{A} = \overline{\mathfrak{A}}$ and so $\mathfrak{A}^2\eta = (1)$. Thus $\mathfrak{A}^2$ is a principal ideal. By Theorem 6.3 this implies that $\mathfrak{A}$ is a principal ideal. Hence e is odd. Since G is not p-solvable, $e \neq 1$ by Burnside's transfer theorem. Therefore $e = 11$.

Since $\mathfrak{A}^\tau = \mathfrak{A}$ and the numerator and denominator of $\overline{\mathfrak{A}}$ are prime to p, it follows that $\mathfrak{A}$ is generated by an ideal $\mathfrak{a}$ of $Q(\sqrt{(-23)})$. Let $\mathfrak{b}$ be a prime divisor of 2 in $Q(\sqrt{(-23)})$. Then $\mathfrak{b}^2 \neq (2)$. It is easily seen that $\frac{1}{4}(a^2+23b^2) = 4$ has no solutions in integers with $b \neq 0$. Thus $\mathfrak{b}^2$ is not a principal ideal in $Q(\sqrt{(-23)})$. By Theorem 6.5, every ideal in $Q(\sqrt{(-23)})$ is in the same class as (1), $\mathfrak{b}$, or $\mathfrak{b}^2$. Since $\mathfrak{b}\overline{\mathfrak{b}} = (2)$ it follows that every ideal in $Q(\sqrt{(-23)})$ is in the same class as (1), $\mathfrak{b}$, or $\overline{\mathfrak{b}}$. By applying a field of automorphism if necessary it may be assumed that either $\mathfrak{a}$ is principal or $\mathfrak{a} = c\mathfrak{b}$ for some c in $Q(\sqrt{(-23)})$. Since $\mathfrak{A}$ is not principal, $\mathfrak{a}$ cannot be principal. Therefore $\mathfrak{A} = c\mathfrak{B}$, where $\mathfrak{B}$ is a prime divisor of 2 in $Q(\zeta)$. Consequently Theorem 9.1 implies that (M, h) is isometric to $(\mathfrak{B}(1-\zeta), \lambda/p)$ for some $\lambda \in Q(\sqrt{(-23)})$, $\lambda = \bar{\lambda}$. Thus $\lambda \in Q$ and $(1) = \mathfrak{B}\overline{\mathfrak{B}}\lambda = (2\lambda)$. Since $\lambda > 0$ this implies that $\lambda = \frac{1}{2}$ as required.

LEMMA 14.2. *Let $\mathfrak{A}$ be a prime divisor of 2 in $Q(\zeta)$. Let $T = T_{Q(\zeta)/Q}$ denote the trace from $Q(\zeta)$ to Q. Let $\alpha \in \mathfrak{A}$ with $T(\alpha\bar{\alpha}) < 8p$, $\alpha \neq 0$. Then $4p - \frac{1}{2}T(\alpha\bar{\alpha})$ is one of the following set of numbers*

$$\{0, 2, 4, 6, 8, 12, 16, 18, 24, 32, 36, 48\}.$$

Furthermore,

(i) $T(\alpha\bar{\alpha}) = 88$ *if and only if* $\alpha = \pm 2\zeta^j$ *for some* j;

(ii) $4p - \frac{1}{2}T(\alpha\bar{\alpha}) = 18$ *if and only if* $\alpha = \pm\{\zeta^{k_1} - \sum_{j=2}^{8}\zeta^{k_j}\}$, *where* $k_1, \ldots, k_8$ *are distinct modulo* p;

(iii) $4p - \frac{1}{2}T(\alpha\bar{\alpha}) = 36$ *if and only if* $\alpha = \pm\sum_{j=1}^{7}\zeta^{k_j}$, *where* $k_1, \ldots, k_7$ *are distinct modulo* p;

(iv) $T(\alpha\bar{\alpha}) = 8p$ *if and only if either* $\alpha = \sum_{j=1}^{4}\zeta^{k_j} - \sum_{j=5}^{8}\zeta^{k_j}$, *where* $k_1, \ldots, k_8$ *are distinct modulo* p *or* $\alpha = 2(\zeta^j - \zeta^i)$ *when* $i \not\equiv j \pmod{p}$;

(v) $4p - \frac{1}{2}T(\alpha\bar{\alpha}) = 32$ *if and only if* $\alpha = \pm\sum_{j=1}^{8}\zeta^{k_j}$, *where* $k_1, \ldots, k_8$ *are distinct modulo* p.

Proof. Let $\alpha = \sum_{j=0}^{p-1} a_j\zeta^j$, where $a_0, a_1, \ldots$ are rational integers and $|\sum a_j| \leqslant \frac{1}{2}(p-1) = 11$. Let m be the number of odd a_j. By Lemma 6.8, $m = 7, 8, 11, 12$ or $m \geqslant 15$. By Lemma 6.7, $T(\alpha\bar{\alpha}) = p\sum a_j^2 - (\sum a_j)^2 \leqslant 8p$. Thus $p\sum a_j^2 \leqslant 8p + (\sum a_j)^2 \leqslant 8p + 121 < 14p$. Thus $\sum a_j^2 \leqslant 13$. If no a_j

is odd then the only possibilities are that $\alpha = \pm 2\zeta^i$ or $\pm 2(\zeta^i \pm \zeta^j)$. If some a_j is odd then a_j is odd for at least seven values of j. Hence any odd a_j is equal to ± 1. There are relatively few possibilities and the result follows from direct computation.

LEMMA 14.3. *The Mathieu group* M_{23} *acting as a permutation group on* $\{\zeta^j \mid 0 < j \leqslant p-1\}$ *acts as a group of automorphisms of* $(\mathfrak{A}, 1/(2p))$, *where* $\mathfrak{A}$ *is a prime divisor of* 2 *in* $Q(\zeta)$. *Let* Z_2 *be the group of order* 2 *generated by the map which sends* α *to* $-\alpha$. *Let* T *denote the trace from* $Q(\zeta)$ *to* Q. *Then the following hold:*

(i) *there are* 2.253 *elements* α *in* $\mathfrak{A}$ *such that* $4p - \frac{1}{2}\mathrm{T}(\alpha\bar{\alpha}) = 36$. *The group* $Z_2 \times \mathrm{M}_{23}$ *acts transitively on this set;*

(ii) *there are* 32.253 *elements* α *in* $\mathfrak{A}$ *such that* $4p - \frac{1}{2}\mathrm{T}(\alpha\bar{\alpha}) = 18$;

(iii) *there are* 140.253 *elements* $\alpha = \sum_{j=1}^{4} \zeta^{k_j} - \sum_{j=5}^{8} \zeta^k$ *in* $\mathfrak{A}$, *where* $k_1, \ldots, k_8$ *are distinct modulo* p;

(iv) *there are* 2.253 *elements* $\alpha = 2(\zeta^i - \zeta^j)$ *in* $\mathfrak{A}$ *with* $i \not\equiv j \pmod{p}$;

(v) *there are* 4.253 *elements* α *in* $\mathfrak{A}$ *such that* $4p - \frac{1}{2}\mathrm{T}(\alpha\bar{\alpha}) = 32$.

Proof. Let $\Omega = \mathrm{GF}(23) \cup \{\infty\}$. Let C_8 be the collection of all 8 element sets $\{k_j \mid 1 \leqslant j \leqslant 8,\ k_j \in \mathrm{GF}(23),\ \sum_{j=1}^{8} \zeta^{k_j} \in \mathfrak{A}\}$. Let C_7 be the collection of all 8-element sets $\{k_j \mid 1 \leqslant j \leqslant 7,\ k_j \in \mathrm{GF}(23),\ \sum_{j=1}^{7} \zeta^{k_j} \in \mathfrak{A}\} \cup \{\infty\}$. For the following results, see for instance, [**24**].

There are 2.253 sets in C_8 and 253 sets in C_7. The collection $C_7 \cup C_8$ is the set of all 8 element sets in the Steiner system $\mathrm{S}(5, 8, 24)$. This together with Lemma 14.2 establishes the cardinality of all the required sets in the statement of the lemma.

The Mathieu group M_{24}, which acts 5-transitively on Ω, acts as a transitive permutation group on $C_7 \cup C_8$. This is easily seen to imply that M_{23} acts transitively on C_7. In view of Lemma 14.2, this implies that $Z_2 \times \mathrm{M}_{23}$ acts transitively on the set of all elements $\alpha \in \mathfrak{A}$ with $4p - \frac{1}{2}\mathrm{T}(\alpha\bar{\alpha}) = 36$.

LEMMA 14.4. *Suppose that* $n = p = 23$. *Assume that* G *is not of type* $L_2(p)$. *Let* $L \in \mathscr{L}_h$ *be such that* (L, h) *has minimal discriminant and* L *contains no vector* v *with* $h(v, v) = 2$. *Then* (L, h) *is isometric to one of three lattices for which* $d_h(L_1) = (p)$, $(3p)$, $(6p)$ *respectively. Furthermore,* $d_h(L) = (1)$, (3), (6) *respectively.*

Proof. By Theorem 9.6, $d_h(L_1) = (d_1 p)$ for some positive integer d_1. Since $L_1 \otimes_R Q$ is 1-dimensional, there exists $w \in L_1$ with $h(w, w) = d_1 p$. Thus w generates L_1 and so d_1 is a square-free integer. The lattice L_1 is uniquely determined by d_1. By Lemma 14.1, (M, h) is isometric to $(\mathfrak{A}(1-\zeta), 1/(2p))$, where A is a prime divisor of 2 in $Q(\zeta)$. Thus by

Theorem 2.10, (L,h) is uniquely determined up to isometry by the value of d_1. Thus it suffices to show that $d_1 = 1$, 3, or 6.

By Theorem 10.2, every element in L is either in $M \oplus L_1$ or is of the form $\alpha + cw/p$ for some $\alpha \in \mathfrak{A}$ and some integer c. By Lemmas 14.2 and 14.3, there exist vectors $v \in M$ with $h(v,v) = 4$. Since $\mathrm{Aut}((L,h))$ acts irreducibly on V, there exists a vector $v \notin M$, $v \in L$ with $h(v,v) = 4$. Clearly $v \notin L_1$, otherwise $h(v,v)$ is divisible by p. Thus $v = \alpha + cw/p$ for $\alpha \in \mathfrak{A}$, $\alpha \neq 0$, and some non-zero integer c. Thus

$$c^2 d_1 p = h(cw, cw) = p\{4p - \tfrac{1}{2}\mathrm{T}_{Q(\zeta)/Q}(\alpha\bar{\alpha})\}.$$

Hence $c^2 d_1$ is equal to one of the values listed in Lemma 14.2. The only primes dividing any of these values (other than 0) are 2 and 3. Since d_1 is square-free this implies that $d_1 = 1$, 2, 3, or 6.

Suppose that $d_1 = 2$. By Theorem 2.10, (L,h) is isometric to $(\langle M \oplus L_1, 2\zeta + w/p\rangle, h)$.

$$\begin{aligned} h(2\zeta + w/p, 2\zeta + w/p) &= 1/(2p)\mathrm{T}_{Q(\zeta)/Q}(4) + h(w/p, w/p) \\ &= 2(p-1)/p + 2/p = 2. \end{aligned}$$

Thus L contains a vector v with $h(v,v) = 2$, contrary to assumption.

The last statement follows from Theorem 9.6 and Lemma 11.1.

LEMMA 14.5. *Suppose that* $n = p+1 = 24$. *Assume that* G *is not of type* $L_2(p)$ *and* $\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$. *Let* $L \in \mathscr{L}_h$ *be such that* (L,h) *has minimal discriminant and* L *contains no vector* v *with* $h(v,v) = 2$. *Let* d *be a positive integer such that* $d_h(L) = (d)$. *Then the following hold:*

(i) $d \mid 2.3^2.5.7.13$;

(ii) $d \neq 13$ *and* $d \neq 9$;

(iii) $11^2 \nmid |G|$.

Proof. By replacing G by the last term in the descending commutator series, it may be assumed without loss of generality that $G = G'$.

Let q be a prime which divides d. By Theorem 8.4, $q \leqslant 13$. By Corollary 3.9, $q^{13} \nmid d$. By Theorem 9.4 and Lemma 11.1, $q^3 \nmid d$. Thus $d \mid 2^2.3^2.5^2.7^2.11^2.13^2$. Furthermore, Theorem 9.6 implies that $d_h(L_1) = (pd)$.

Suppose that $q^2 \mid d$. Then $(1/q)L \cap L_h^*/L$ is a 2-dimensional module over $\mathrm{GF}(q)$. Let H be the kernel of the representation of G on this module. Since $q^2 \not\equiv 1 \pmod{p}$, it follows that $p \mid\mid H\mid$. As $\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$, this implies that G/H is abelian by the Frattini argument. Since $G = G'$, this implies that G acts trivially on $(1/q)L \cap L_h^*/L$. Thus G preserves every lattice L_0 with $L \subseteq L_0 \subseteq L_h^* \cap (1/q)L$. Since (L,h) has minimal discriminant, this implies that there exists no lattice L_0 which is integral with respect to h such that $L \subseteq L_0 \subseteq L_h^* \cap (1/q)L$. Let $L_2 = (L_1)_h^* \cap (1/q)L_1$.

Then there exists no lattice L_0 with $L_1 \subseteq L_0 \subseteq L_2$ such that L_0 is integral with respect to h. In other words, L_2/L_1 is a 2-dimensional space over GF(q) which contains no isotropic subspace with respect to the symmetric bilinear form induced on L_2/L_1 by h. This implies in particular that $q \neq 2$ as such an isotropic subspace always exists for $q = 2$.

Let $v \in L_1$. Then $(1/q)v \in L_2$. Thus $h((1/q)v, v)$ is an integer and so $h(v,v) = 0 \pmod q$ for all $v \in L_1$. By Lemma 14.1, (M,h) is isometric to $(\mathfrak{A}(1-\zeta), 1/(2p))$, where $\mathfrak{A}$ is a prime divisor of 2 in $Q(\zeta)$. Thus by Lemmas 14.2 and 14.3, there exist vectors $v \in M$ with $h(v,v) = 4$. As G acts irreducibly on L, this implies that there exists a vector $v \in L$, $v \notin M$ such that $h(v,v) = 4$. Since $q \neq 2$, $q \nmid h(v,v)$ and so $v \notin L_1$. Consequently $v = \alpha + w/p$ for some $\alpha \in \mathfrak{A}$ and some $w \in L_1$. Thus

$$h(w/p, w/p) = 4 - 1/(2p)\mathrm{T}_{Q(\zeta)/Q}(\alpha\bar{\alpha}).$$

Hence $h(w,w) = pc$, where c is one of the non-zero values listed in Lemma 14.2. Therefore the only primes which divide c are 2 or 3. Hence $q = 2$ or 3 and so $q = 3$. Thus $d \mid 2.3^2.5.7.11.13$.

Suppose that $d = 9$. Then $d_h(L_1) = (9p)$. Hence the quadratic form on L_2/L_1 induced by h has discriminant $23 \equiv -1 \pmod 3$. Thus this form is equivalent to $X^2 - Y^2$ and so has an isotropic subspace. Therefore $d \neq 9$. To complete the proof it is sufficient to show that $11 \nmid d$, $d \neq 13$, and $11^2 \nmid |G|$.

Let $q = 11$ or 13. Suppose that $q \mid d$. Thus the GF(q)[G]-module $(1/q)L$ has a 1-dimensional constituent $(1/q)L \cap L_h^*/L$. Since $G = G'$, this affords the principal character. Thus the $Q[G]$-module V is in the principal block. Since $n = 24 \not\equiv \pm 1 \pmod q$, this implies that a Sylow q-group of G has order at least q^2. Since G has a faithful rational representation of degree 24, this implies that a Sylow q-group of G is elementary abelian of order q^2. To complete the proof, it suffices to show that $q^2 \nmid |G|$. Assume that $q^2 \| |G|$. There exists an element z of order q which has 1 as a characteristic root with multiplicity $n-(q-1)$ on V. Thus Theorem 9.4 may be applied for the prime q.

Let $A = L(1-z)$ and let $B = \{v \in L, vz = v\}$. By Theorem 9.4, $d_h(A)d_h(B) = d_h(L)q^2$. Thus $(q)^3$ is the exact power of q which divides $d_h(A)d_h(B)$. By Theorem 9.5, (q) divides $d_h(A)$ to an odd power. Suppose that $(q)^3 \nmid d_h(A)$. If $d = 13$, this implies that $d_h(A) = (13)$. If $q = 11$, Lemma 11.1 implies that $d_h(A) = (11)$. Thus in any case $d_h(A) = (q)$ and Lemma 11.2 implies that there exists $v \in L$ with $h(v,v) = 2$, contrary to assumption. Suppose that $(q)^3 \mid d_h(A)$. Thus $(q) \nmid d_h(B)$. This implies that $L = B \oplus A_1$, where A_1 is the orthogonal complement of B. Thus (q) divides $d_h(A_1)$ to the first power and z acts on A_1 without fixed points.

If $d = 13$ then $d_h(A_1) = (q)$. If $q = 11$ then $d_h(A_1) = (q)$ by Lemma 11.1. Thus by Lemma 11.2, L contains a vector v with $h(v, v) = 2$ also in this case. This contradiction completes the proof.

LEMMA 14.6. *Suppose that G is not of type $L_2(p)$, $n = p+1 = 24$, and $\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$. Let $L \in \mathscr{L}_h$ be such that (L, h) has minimal discriminant and L contains no vector v with $h(v, v) = 2$. Then $d_h(L) = (1)$.*

Proof. Since G acts irreducibly on V and M contains a vector v with $h(v, v) = 4$ by Lemmas 14.1, 14.2, and 14.3, there exist vectors u, $w \in L$ such that u and w are linearly independent modulo M with

$$h(u, u) = h(w, w) = 4.$$

Let d be the positive integer such that $d_h(L) = (d)$. Thus $d_h(L_1) = (dp)$.

Let a be the minimum value of $h(v, v)$, $v \in L_1$, $v \neq 0$. Then there exists a basis v_1 and v_2 of L_1 such that $h(v_1, v_1) = a$, $h(v_2, v_2) = c$ $h(v_1, v_2) = b$, $|b| \leqslant \frac{1}{2}a$, and $pd = ac - b^2$. Furthermore, $a \leqslant c$. By assumption, $a \geqslant 3$. Furthermore,

$$(14.7)\quad h(sv_1 + tv_2, sv_1 + tv_2) = s^2a + 2stb + t^2c = (1/a)\{(sa + bt)^2 + pdt^2\}$$

If $L_2 \subseteq L_1$ then, by Lemma 2.3, $d_h(L_2) = (m^2dp)$ for some integer m.

Not both u and w are in L_1, otherwise the lattice spanned by u and w has discriminant at most $16 < p$. Suppose one of them, say u, is in L_1. Then L_1 cannot contain v with $h(v, v) < 4$ as otherwise L_1 would have discriminant at most $12 < p$. By Lemma 14.1, $w = \alpha + w_0/p$, where $\alpha \in \mathfrak{A}$, a prime divisor of 2 in $Q(\zeta)$ and $w_0 \in L_1$. Consequently $h(w_0, w_0) = mp$, where m is one of the non-zero values listed in Lemma 14.2. By (14.7), this implies that $d \leqslant 4.48 = 192$. By using (14.7) and Lemma 14.5, it follows that $d = 1$, 2, 3, 6, or 105. Since $pd = 4c - b^2$ it follows that $d \equiv 0$ or 1 (mod 4). Therefore $d = 1$ or $d = 105$. Suppose that $d = 105$. Then L_1 has a basis $\{u, u_1\}$ with $h(u, u) = 4$, $h(u_1, u_1) = 604$, and $h(u, u_1) = 1$. Thus the only vectors v in L with $h(v, v) = 4$ are either in M or of the form $\pm u$ or $\alpha \pm w_0/p$, where $w_0 = (6u - u_1)$. Thus by Lemma 14.3, there are $146.253 + 2 = 36{,}940$ vectors v in L with $h(v, v) = 4$. Furthermore, if $v \in L$ with $h(v, v) = 4$ and $v \notin (M + \langle w_0 \rangle) \otimes_R Q \cap L$ then $v = \pm u$. Since $\mathrm{Aut}((L, h))$ acts irreducibly on V, this implies that $\mathrm{Aut}((L, h))$ acts transitively on the set of 36,940 vectors v with $h(v, v) = 4$. This is impossible as 36,940 is divisible by a prime $q > 23$ which cannot divide $|\mathrm{Aut}((L, h))|$. Thus it may be assumed that neither u nor w is in L_1.

Let $u = \alpha + u_0/p$, $w = \beta + w_0/p$, where $\alpha, \beta \in \mathfrak{A}$ and $u_0, w_0 \in L_1$. Then $h(u_0, u_0)$ and $h(w_0, w_0)$ are both of the form pm, where m is one of the

numbers listed in Lemma 14.2. By using (14.7) and Lemma 14.5 and checking all non-zero possibilities (there are 66 of them), one gets either $d = 1$ or $d = 7$, $h(u_0, u_0) = 18p$, $h(w_0, w_0) = 36p$. A check of all possible lattices of discriminant 7.23 which take on the values $18p$ and $36p$ shows that there is a unique such lattice and $a = 11, b = 2, c = 15$. Furthermore, the only vectors of length $18p$ are $\pm(3v_1 - 5v_2)$ and the only vectors of length $36p$ are $\pm(8v_1 + 2v_2)$. Thus if $\alpha + u_0/p \in L$ then $\alpha - u_0/p \notin L$; similarly, if $\beta + w_0/p \in L$ then $\beta - w_0/p \notin L$. Therefore if $u_0 = 3v_1 - 5v_2$ and $w_0 = 8v_1 + 2v_2$, it follows that every vector v in L with $h(v, v) = 4$, $v \notin M$ is of the form $\pm(\alpha \pm u_0/p)$ or $\pm(\beta \pm w_0/p)$, where the inner sign depends on α and β respectively and $4p - \frac{1}{2}\mathrm{T}(\alpha\bar{\alpha}) = 18$, $4p - \frac{1}{2}\mathrm{T}(\beta\bar{\beta}) = 36$.

Let Z be the group of order 2 generated by the map sending v to $-v$ for v in L. By Lemmas 14.1 and 14.3, the group $\mathrm{M}_{23} \times Z$ acts as a group of automorphisms of L. Since $\mathrm{Aut}((L, h))$ acts irreducibly on V, it follows that if $v \in M$ with $h(v, v) = 4$ then some element of $\mathrm{Aut}((L, h))$ sends v into a vector not in $(M \oplus \langle w_0 \rangle) \otimes_R Q \cap L$, thus into a vector of the form $\pm(\beta \pm w_0/p)$. Since $\mathrm{M}_{23} \times Z \subseteq \mathrm{Aut}((L, h))$, it follows from Lemma 14.3(i) that $\mathrm{Aut}((L, h))$ is transitive on all such vectors. Thus $\mathrm{Aut}((L, h))$ acts transitively on the set of all vectors v in L with $h(v, v) = 4$. By Lemma 14.3, there are $253.(2 + 2 + 32 + 140) = 253.176$ such vectors. Consequently $11^2 \mid\mid \mathrm{Aut}((L, h))|$, contrary to Lemma 14.5. This finally shows that $d = 1$.

15. Proof of Theorems D, E, and F

Proof of Theorem D. As remarked above, Lemma 13.9 implies that only the case $p = 23$ needs to be considered. It may be assumed that G is not of type $\mathrm{L}_2(p)$ since a p-solvable group has a subgroup of index p. Let $L \in \mathscr{L}_h$ be such that (L, h) has minimal discriminant. If there exists $w \in L$ with $h(w, w) = 2$ then $\mathrm{Aut}((L, h))$ contains a unitary reflection and is finite by Theorem 5.3 and Lemma 5.4. Hence the result follows from Theorem 4.3 in this case. Thus it may be assumed that $h(w, w) \neq 2$ for all $w \in L$. By Lemma 13.1, (L, h) is isometric to $(\mathfrak{A}(1 - \zeta), 1/(2p))$, where $\mathfrak{A}$ is a prime divisor of 2 in $Q(\zeta)$. Let $L_0 = (1/p)L \cap L_h^*$. Then L_0 is a G-invariant lattice and (L_0, h) is isometric to $(\mathfrak{A}, 1(2p))$. By Lemma 14.2(i), $\{\pm 2\zeta^j \mid 0 \leqslant j \leqslant p - 1\}$ is the set of all elements in $\mathfrak{A}$ with

$$1/(2p)\mathrm{T}_{Q(\zeta)/Q}(\alpha\bar{\alpha}) = 44/23.$$

Since G acts linearly on V, this implies that G acts as a transitive permutation group on the collection of p sets $\{\pm 2\zeta^j\}$, $0 \leqslant j \leqslant p - 1$. Thus G has a subgroup of index p.

Proof of Theorem E. Consider the class of all pairs (L, h), where h is a positive definite quadratic form on a vector space V over Q of dimension

$n = p = 23$. L is a lattice which is integral with respect to h and is even. L contains no vector v with $h(v,v) = 2$, $23 \mid\mid |\mathrm{Aut}((L,h))|$, $\mathrm{Aut}((L,h))$ acts irreducibly on V, and $d_h(L) = (4)$, (6), or (12). Let L_0 be an $\mathrm{Aut}(L,h))$-invariant lattice such that $L \subseteq L_0$ and (L_0,h) has minimal discriminant. By Theorem 9.6 and Lemma 14.4, $d_h(L_0) = (1)$, (3), or (6). If $d_h(L_0) = (1)$ or (3) then the set of all vectors $v \in L_0$ with $h(v,v) \equiv 0 \pmod 2$ is a sublattice of index 2 by Lemma 2.7. If $d_h(L_0) = 6$ then it is easily seen that L_0 is an even lattice. Thus in any case, L is uniquely determined by L_0. By Lemma 14.4, (L,h) is isometric to one of three lattices which have discriminants (4), (6), or (12) respectively. In [7], Conway has described three such lattices and has shown that their automorphism groups are $Z_2 \times \mathrm{Co.2}$, $Z_2 \times \mathrm{Co.3}$, and $Z_2 \times \mathrm{M}_{24}$ respectively, where $|Z_2| = 2$. Since $8 \nmid [L_h^* : L]$, there are at most three integral lattices in L_h^* which contain L. Thus $Z_2 \times \mathrm{Co.2}$, $Z_2 \times \mathrm{Co.3}$, and $Z_2 \times \mathrm{M}_{24}$ are the automorphism groups of the above-mentioned lattices L_0 of discriminant (1), (6), or (3) respectively.

Let G be a group which has a faithful irreducible rational-valued character of degree 23. By a theorem of Speiser (see, for example, [**10**]), there exists a $Q[G]$-module V of dimension 23. If G is of type $\mathrm{L}_2(p)$, the result follows from Lemma 7.1. Suppose that G is not of type $\mathrm{L}_2(p)$. Let $L \in \mathscr{L}_h$ be such that (L,h) has minimal discriminant. If there exists $w \in L$ with $h(w,w) = 2$ then, by Lemma 5.4, $\mathrm{Aut}((L,h))$ contains a unitary reflection and the result follows from Theorem 4.3. If L contains no vector w with $h(w,w) = 2$ then, by Lemma 14.4, (L,h) is isometric to one of three lattices and the result follows from the previous paragraph.

Proof of Theorem F. Let V be an irreducible $Q[G]$-module of dimension $p+1 = 24$. If G is of type $\mathrm{L}_2(p)$, the result follows from Lemma 7.1. Let P be a Sylow p-group of G. If V is absolutely irreducible and $\mathbf{C}_G(P) \neq P \times \mathbf{Z}(G)$, the result follows from Theorem 8.6. Suppose that G is not of type $\mathrm{L}_2(p)$. Thus V is absolutely irreducible and so it may be assumed that $\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$. Let h be a G-invariant form on V and let $L \in \mathscr{L}_h$ be such that (L,h) has minimal discriminant. If there exists $w \in L$ with $h(w,w) = 2$ then, by Lemma 5.4, $\mathrm{Aut}((\mathrm{L},h))$ contains a unitary reflection. The result follows from Theorem 4.3 in this case.

Suppose that $h(w,w) \neq 2$ for all $w \in L$. By Lemma 14.6, $d_h(L) = (1)$. Thus by Theorem 2.8, there exists an even unimodular lattice L_0 such that $G' \subseteq \mathrm{Aut}((L_0,h))$. If L_0 contains w with $h(w,w) = 2$ then, as above, Lemma 5.4 and Theorem 4.3 imply the result. If L_0 contains no w with $h(w,w) = 2$ then L_0 is the Leech lattice ([8], Theorem 1). Hence $G' \subseteq \mathrm{Co.0}$, as was to be shown.

REFERENCES

1. E. ARTIN and J. TATE, *Class field theory* (Benjamin, New York, 1968).
2. H. F. BLICHFELDT, *Finite collineation groups* (University of Chicago Press, Chicago, 1917).
3. Z. I. BOREVICH and I. R. SHAFAREVICH, *Number theory* (Academic Press, New York and London, 1966).
4. R. BRAUER, 'On groups whose order contains a prime number to the first power, I, II', *Amer. J. Math.* 64 (1942) 401–20, 421–40.
5. —— 'Über endliche lineare Gruppen von Primzahlgrad', *Math. Ann.* 169 (1967) 73–96.
6. J. W. S. CASSELS and A. FRÖHLICH, *Algebraic number theory* (Thompson, Washington, 1967).
7. J. H. CONWAY, 'A group of order 8,315,553,613,086,720,000', *Bull. London Math. Soc.* 1 (1969) 79–88.
8. —— 'A characterization of Leech's lattice', *Invent. Math.* 7 (1969) 137–42.
9. L. DORNHOFF, *Group representation theory* (Dekker, New York, 1972).
10. B. FEIN, 'A note on the Brauer–Speiser theorem', *Proc. Amer. Math. Soc.* 25 (1970) 620–21.
11. W. FEIT, 'Groups with a cyclic Sylow subgroup', *Nagoya Math. J.* 27 (1966) 571–84.
12. —— Representations of finite groups, Part I; Lecture notes (Yale University, New Haven).
13. —— 'On finite linear groups, I, II', *J. Algebra* 5 (1967) 378–400, 30 (1974) 496–506.
14. —— 'The current situation in the theory of finite simple groups', *Actes du Congrès International des Mathématiciens* (1970) 55–93.
15. D. FENDEL, 'A characterization of Conway's group .3', *J. Algebra* 24 (1973) 159–96.
16. J. S. FRAME, 'The classes and representations of the groups of 27 lines and 28 bitangents', *Ann. Mat. Pura. Appl.* (IV) 32 (1951) 83–119.
17. N. ITO, 'Zur Theorie der Permutationsgruppen vom Grad p', *Math. Z.* 74 (1960) 299–301.
18. J. H. LINDSEY, II, 'Finite linear groups of degree six', *Canad. J. Math.* 23 (1971) 771–90.
19. J. MILNOR, 'Whitehead torsion', *Bull. Amer. Math. Soc.* 72 (1966) 358–426.
20. H. V. NIEMEIER, 'Definite quadratische Formen der Dimension 24 und Diskriminante 1', *J. Number Theory* 5 (1973) 142–78.
21. J. P. SERRE, *Cours d'arithmétique* (Presses Universitaires de France, Paris, 1970).
22. G. C. SHEPHARD and J. A. TODD, 'Finite unitary reflection groups', *Canad. J. Math.* 6 (1954) 274–304.
23. J. G. THOMPSON, 'Vertices and sources', *J. Algebra* 6 (1967) 1–6.
24. J. A. TODD, 'A representation of the Mathieu group M_{24} as a collineation group', *Ann. Mat. Pura Appl.* (IV) 71 (1966) 199–238.
25. D. B. WALES, 'Finite linear groups in seven variables', *Bull. Amer. Math. Soc.* 74 (1968) 197–98.
26. H. ZASSENHAUS, 'Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen', *Abh. Math. Sem. Univ. Hamburg* 11 (1936) 17–40.

Yale University