JOURNAL OF ALGEBRA 97, 286–312 (1985)

Finite Unimodular Groups of Prime Degree and Circulants

W. PLESKEN*,†

RWTH Aachen, Lehrstuhl D für Mathematik,
Templergraben 64, 51 Aachen, West Germany

Communicated by Walter Feit

Received December 2, 1983

I. INTRODUCTION

In the present paper the maximal finite irreducible subgroups of $GL_p(\mathbb{Z})$ are classified up to conjugacy for odd prime dimensions $p \leqslant 23$. Unlike in [PlP 77, 80], part I, where this task is solved for $p=5$ and $p=7$, no use of classification results of finite primitive subgroups of $GL_p(\mathbb{C})$ will be made. Inspired by [Fei 74], algebraic number theory will be applied to investigate the geometry of the lattices on which the groups act. The starting point of the classification is Theorem (II.4). Circulants, i.e., integral polynomials in the standard p-cycle

$$z_p = \begin{pmatrix} 0 & & \\ \vdots & I_{p-1} & \\ 0 & & \\ 1 & 0 \cdots & 0 \end{pmatrix} \in \mathbb{Z}^{p \times p}$$

(I_n denotes the $n \times n$-unit matrix), cf. [New 72], come into the game as Gram matrices of bilinear forms fixed by certain of the irreducible subgroups G of $GL_p(\mathbb{Z})$. As a consequence of (II.4) and the fact that the pth cyclotomic fields $\mathbb{Q}(\zeta_p)$ have classnumber 1 for $p \leqslant 19$, each irreducible finite subgroup of $GL_p(\mathbb{Z})$, $p \leqslant 19$ prime, is conjugate to a unimodular group which fixes a bilinear form with circulant Gram matrix.

Section III has two main results, namely, Theorems (III.3) and (III.7). Generalizing results by Burnside [Bur 12] and Bannai [Ban 73] Theorem (III.3) states that the finite subgroups of $GL_n(\mathbb{Q})$ ($n \in \mathbb{N}$ not necessarily prime) containing certain 2-transitive groups of permutation matrices are contained in automorphism groups of root systems.

* Supported by the Deutsche Forschungsgemeinschaft.

† Present address: School of Mathematical Sciences, Queen Mary College, London E1 4NS, Great Britain.

0021-8693/85 $3.00

Theorem (III.7) implies, e.g., that the maximal finite irreducible subgroups of $GL_p(\mathbb{Z})$ for odd prime dimensions $p \leqslant 11$ are essentially reflection groups, cf. Corollary (III.9).

The last three sections are devoted to describing a method of finding the maximal finite irreducible subgroups of $GL_p(\mathbb{Z})$ for bigger p and to carrying out the method for $p = 13$, 17, 19, and 23, cf. Theorems (V.2)–(V.5), and (VI.3). Fortunately the two main phenomena responsible for the existence of other maximal finite irreducible subgroups of $GL_p(\mathbb{Z})$ than automorphism groups of root systems occur separately in these dimensions p, namely, the existence of prime numbers $q < p$ for which q or $-q$ is not a primitive root modulo p on the one hand and the class number of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ not being 1 on the other hand. For dimensions 13 to 19 it was necessary to compute automorphism groups of some lattices by machine. For this the original implementation of the algorithm developed in [PlP 85] was used, the calculations were carried out on the Cyber 175 of the Rechenzentrum of the RWTH Aachen.

It might be worth mentioning that the proof of Theorem (II.4)(i) can easily be modified to obtain, e.g., the following result:

Let L be an irreducible $\mathbb{Z}G$-lattice on which the finite group G acts faithfully and let $U = \langle g \rangle$ be a subgroup of G of prime order $p > 2$. Assume $n_1 = \dim_{\mathbb{Z}}\{x \in L \mid gx = x\}$ and $n_2 = \dim_{\mathbb{Z}} L - n_1$ are relatively prime, then the restriction $L|_U$ has a projective $\mathbb{Z}U$-lattice as direct summand.

It is a pleasure for me to thank R. Parker for informing me about certain decomposition numbers of $Co.2$ and $Co.3$ before (VI.2) was available to me, M. Pohst for computing the vectors of minimum length of one of the lattices in (V.4)(v), and O. Taussky for informing me about the literature on circulants.

II. The Irreducible Unimodular Group of Prime Degree and Its Natural Lattice

In odd prime (p) dimensions $\mathbb{Q}$- and $\mathbb{C}$-irreducibility are equivalent for a finite irreducible unimodular group (f.i.u.g.), cf. [PlP 77, 80], which has some easy, but important consequences.

(II.1) *Remark.* Let $G \leqslant GL_p(\mathbb{Z})$ be a f.i.u.g. Then

(i) G is uniform, and hence contained in a unique maximal f.i.u.g. $G^{\max}$. More precisely, there is an—up to scalar multiples—unique symmetric matrix $F \in \mathbb{Q}^{p \times p}$, $F \neq 0$, with $g^{\text{tr}} F g = F$ for all $g \in G$. (det F) F is positive definite and $G^{\max} = \text{Aut}_{\mathbb{Z}}(F) := \{g \in GL_p(\mathbb{Z}) \mid g^{\text{tr}} F g = F\}$.

(ii) $p \mid |G|$, but $p^2 \nmid |G|$.

(iii) (cf. [Min 11]) $|G| \mid \prod_q q^{v(q)}$ with q running over all primes ($\leqslant p$) and

$$v(q)=\left[\frac{p}{q-1}\right]+\left[\frac{p}{(q-1)q}\right]+\left[\frac{p}{(q-1)q^2}\right]+\cdots.$$

Proof. (i) cf. [PlP 77, 80]; (ii) the natural character of G is $\mathbb{C}$-irreducible and of degree p, hence $p \mid |G|$. The rest follows from part (iii). Q.E.D.

Hence the natural $\mathbb{Z}G$-lattice $L=L_G:=\mathbb{Z}^{p\times 1}$ of a f.i.u.g. $G\leqslant GL_p(\mathbb{Z})$ is equipped with a unique positive definite, surjective, G-invariant bilinear form $\phi=\phi_G$: $L\times L\to\mathbb{Z}$. The Gram matrix $F_G\in\mathbb{Z}^{p\times p}$ (with respect to the standard basis of $\mathbb{Z}^{p\times 1}$) of ϕ_G is a multiple of F in (II.1.i), and $G^{\max}$ can be identified with $\mathrm{Aut}(L,\phi)$. ϕ induces a G-invariant $\mathbb{Q}$-bilinear form on the natural $\mathbb{Q}G$-module $V=V_G:=\mathbb{Q}^{p\times 1}=\mathbb{Q}L$; which will also be denoted by ϕ or ϕ_G. The notation V_G, L_G, ϕ_G, F_G will be used without further comment. Note, any $\mathbb{Z}G$-lattice L with faithful G-action and $\mathbb{Z}$-rank n defines a conjugacy class of subgroups of $GL_n(\mathbb{Z})$ isomorphic to G (via the various choices of $\mathbb{Z}$-bases of L); other $\mathbb{Z}G$-lattices L' in $\mathbb{Q}L:=\mathbb{Q}\otimes_{\mathbb{Z}}L$ with $\mathbb{Q}L'=\mathbb{Q}L$ define subgroups of $GL_n(\mathbb{Z})$ which are conjugate under $GL_n(\mathbb{Q})$ to those defined by L; finally L defines a unique ϕ_G, if $\mathbb{C}\otimes_{\mathbb{Z}}L$ is irreducible $\mathbb{C}G$-module. The group theoretical structure of f.i.u.g. of degree p is best distinguished by the behaviour of the maximal normal 2-subgroup $O_2(G)$. Note, with $G\leqslant GL_p(\mathbb{Z})$ also $G^+=G\cap SL_p(\mathbb{Z})$ is irreducible.

(II.2) PROPOSITION. *Let $G\leqslant SL_p(\mathbb{Z})$ be a* f.i.u.g. *and let d be the multiplicative order of* 2 *modulo p. One of the following situations arises*:

(i) *$O_2(G)$ is elementary abelian of order 2^{dk} with $1\leqslant k\leqslant(p-1)/d$. In this case G is conjugate under $GL_p(\mathbb{Q})$ to a group of monomial matrices. Moreover, G contains an irreducible subgroup which is an extension of an elementary abelian* 2*-group of order 2^d by a cyclic group of order p.*

(ii) *$O_2(G)=1$. In this case G has a unique minimal normal subgroup $N\neq 1$ (possibly $N=G$). N is nonabelian simple, $C_G(N)=1$ and as a matrix group N is irreducible.*

Proof. Since $p\nmid|O_2(G)|$ the natural $\mathbb{Q}G$-module $V=V_G$ becomes reducible upon restriction to $O_2(G)$. Since $\dim_{\mathbb{Q}} V=p$, Clifford's theorem leads only to two possibilities for the decomposition of the $V_{O_2(G)}$: Either it is the direct sum of p G-conjugate one-dimensional nonisomorphic $\mathbb{Q}O_2(G)$-modules or it is the direct sum of p copies of a single one-dimensional $\mathbb{Q}O_2(G)$-module. The first case leads to (i) above by routine arguments, cf. part I of [PlP 77, 80]. In the second case $O_2(G)$ consists of scalar matrices of determinant 1 and is therefore trivial. By similar Clifford arguments as above, cf. [PlP 77, 80], one concludes that G has no abelian normal subgroup $\neq 1$ in this case. Hence a minimal normal subgroup of G is nonabelian, characteristically simple, and therefore simple, since the degree of a faithful irreducible character is a prime number. The rest follows. Q.E.D.

In the sequel P will denote a fixed Sylow p-subgroup of the f.i.u.g. G of degree p, z a fixed generator of P, and $\zeta = \zeta_p$, a fixed primitive pth root of unity. The group ring $\mathbb{Z}P$ of P is isomorphic to $\{(a, b) \mid a \in \mathbb{Z},\ b \in \mathbb{Z}[\zeta],\ \varphi(a) = \psi(b)\} \leqslant \mathbb{Z} \oplus \mathbb{Z}[\zeta_p]$, where φ and ψ are the ring epimorphisms of $\mathbb{Z}$ and $\mathbb{Z}[\zeta]$ onto $\mathbb{Z}/p\mathbb{Z}$. Clearly, the natural $\mathbb{Z}P$-lattice L_P (restriction of the $\mathbb{Z}G$-lattice L to $\mathbb{Z}P$) is isomorphic to an ideal of full $\mathbb{Z}$-rank in $\mathbb{Z}P$. Slightly extending the conventions of [Fei 74], one can describe the P-invariant rational quadratic forms of such an ideal as being induced by a generalized trace bilinear form

$$T_f\colon\quad \mathbb{Q}P \times \mathbb{Q}P \to \mathbb{Q}\colon\quad (x, y) \mapsto \frac{1}{p}\, tr_{\mathbb{Q}P/\mathbb{Q}}(\bar{x} f y)$$

of $\mathbb{Q}P$ (note $V_P \cong_{\mathbb{Q}P} \mathbb{Q}P$). Here $tr_{\mathbb{Q}P/\mathbb{Q}}\colon \mathbb{Q}P \to \mathbb{Q}$ denotes the regular trace, $f \in \mathbb{Q}[z + z^{-1}] \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta + \zeta^{-1})$ and $\overline{}\colon \mathbb{Q}P \to \mathbb{Q}P$ is the involution $\sum_{i=0}^{p-1} \alpha_i z^i \mapsto \sum_{i=0}^{p-1} \alpha_i z^{-i}$. Clearly T_f is positive definite if and only if f is totally positive, i.e., if f is mapped onto positive real numbers by each of the $(p+1)/2$ homomorphisms of $\mathbb{Q}[z + z^{-1}]$ into $\mathbb{R}$. As a shorthand notation for the $\mathbb{Z}P$-ideal $\mathfrak{a}$ with the bilinear form induced by T_f, the symbol $(\mathfrak{a}, f)$ will be used. $\mathrm{Aut}(\mathfrak{a}, f)$ consists of all isometries of $(\mathfrak{a}, f)$ with itself disregarding the action of P. In particular, if $(\mathfrak{a}, f)$ is isometric to (L, ϕ_G) for some f.i.u.g. G, then $G^{\max}$ can be identified with $\mathrm{Aut}(\mathfrak{a}, f)$. However, the kind of mappings between the various $(\mathfrak{a}, f)$ usually used to make to a convenient choice of $(\mathfrak{a}, f)$ will not be arbitrary isometries but additionally respect the P-action, in the sense of the following easily verified remark, which also follows from [Fei 74] Theorem 9.2.

(II.3) *Remark.* Let $\mathfrak{a}, \mathfrak{a}'$ be $\mathbb{Z}P$-ideals of full $\mathbb{Z}$-rank in $\mathbb{Q}P$ and f, f' invertible elements of $\mathbb{Q}[z + z^{-1}]$.

(i) The multiplication by an invertible element a of $\mathbb{Q}P$ induces an isometry of $(\mathfrak{a}, f)$ onto $(a\mathfrak{a}, a\bar{a}f)$, which is a $\mathbb{Z}P$-isomorphism.

(ii) Each automorphism α of the $\mathbb{Q}$-algebra $\mathbb{Q}P$ is induced by an automorphism of P and induces an isometry of $(\mathfrak{a}, f)$ onto $(\alpha(\mathfrak{a}), \alpha(f))$.

(iii) Each isometry $\beta\colon (\mathfrak{a}, f) \to (\mathfrak{a}', f')$ satisfying $\beta z = z^i \beta$ for some $i \in \mathbb{Z}$ can be factored into a product of isometries just described in (i) and (ii) above.

The well-known concept of the dual lattice will be used in the next theorem: For a $\mathbb{Z}$-lattice L in the $\mathbb{Q}$-vector space $V=\mathbb{Q}L$ with positive definite scalar product $\phi\colon V\times V\to\mathbb{Q}$ the dual lattice of L (with respect to ϕ) is given by $L^{\#}:=\{x\in V\mid\phi(x,L)\subseteq\mathbb{Z}\}$.

Clearly $L^{\#}$ is again a $\mathbb{Z}$-lattice in V, it is $\mathbb{Z}G$-lattice if L is $\mathbb{Z}G$-lattice and ϕ G-invariant. ϕ takes integral values on $L\times L$ iff $L\subseteq L^{\#}$; in this case $[L^{\#}:L]=|\det(\phi(e_i,e_j))|$ for some $\mathbb{Z}$-basis $(e_1,\ldots,e_n)$ of L is the discriminant of (L,ϕ). Frequently the isomorphism type of $L^{\#}/L$ (as abelian group) presented in the form of the elementary divisors of the Gram matrix $(\phi(e_i,e_j))$ will be used as an invariant of (L,ϕ) which usually contains more information than just the discriminant.

(II.4) Theorem. *Let $G\leqslant GL_p(\mathbb{Z})$ be a* f.i.u.g. *with natural lattice $L=L_G$ and, associated G-invariant scalar product $\phi=\phi_G$ and Sylow p-subgroup $P=\langle z\rangle$. There exists an ideal $\mathfrak{a}$ of $\mathbb{Z}P$, a totally positive $f\in\mathbb{Q}[z+z^{-1}]$ and an isometry $\alpha\colon(L,\phi)\to(\mathfrak{a},f)$ satisfying $\alpha z=z^i\alpha$ for some $i\in\mathbb{Z}$. For any such $(\mathfrak{a},f)$ the following holds:*

(i) *$\mathfrak{a}$ is an invertible ideal of $\mathbb{Z}P$, i.e., as $\mathbb{Z}P$-module $\mathfrak{a}$ is projective indecomposable;*

(ii) *$(|G|/p)\,\mathbb{Z}P\subseteq f\mathfrak{a}\bar{\mathfrak{a}}\subseteq\mathbb{Z}P$;*

(iii) *$L^{\#}/L\cong\mathbb{Z}P/f\mathfrak{a}\bar{\mathfrak{a}}$ as abelian groups.*

Proof. The existence of $(\mathfrak{a},f)$ was already established above.

(i) Clearly, the following properties of a $\mathbb{Z}P$-ideal $\mathfrak{a}'$ of full $\mathbb{Z}$-rank are equivalent: $\mathfrak{a}'$ is indecomposable as $\mathbb{Z}P$-lattice; $\mathfrak{a}'/p\mathfrak{a}'\cong\mathbb{Z}P/p\mathbb{Z}P$; $\mathfrak{a}'$ is a projective $\mathbb{Z}P$-lattice; upon localization at p, $\mathfrak{a}'$ becomes a principal ideal; $\mathfrak{a}'$ is invertible $\mathbb{Z}P$-ideal (in this case $\mathfrak{a}'^{-1}$ is given by the dual of $\mathfrak{a}'$ with respect to T_1); cf. also [CuR 62, Sect. 74 ff]. Hence it suffices to prove that L_P is an indecomposable $\mathbb{Z}P$-lattice. Assume L_P is decomposable. Then $L_P=L_1\oplus L_2$ where $L_1=\{v\in L\mid zv=v\}$ is of $\mathbb{Z}$-rank 1 and L_2 is isomorphic to some ideal of $\mathbb{Z}[\zeta]$. With respect to ϕ the sublattices L_1 and L_2 are orthogonal to each other. According to a theorem by Eichler, cf. [Kne 54], (L,ϕ) decomposes uniquely into the direct sum of pairwise orthogonal $\mathbb{Z}$-sublattices $\neq 0$, each of which cannot be decomposed any further. Because of the uniqueness of this decomposition L_1 is one of these components and the others are contained in L_2. Since G acts irreducibly, the components are transitively permuted by G. Hence there are $p-1$ one-dimensional components in L_2. These are also permuted by P. But $\alpha\nmid p$ for $\alpha=2,3,\ldots,p-1$, hence P leaves each component invariant. But this contradicts the irreducibility of L_2 as $\mathbb{Z}P$-lattice.

(ii) The surjectivity of $\phi\colon L\times L\to\mathbb{Z}$ implies $L\nsubseteq kL^{\#}$ for any $k\in\mathbb{N}$, $k\geqslant 2$. Hence $(|G|/p)\,L^{\#}\subseteq L$ by Theorem 2.8 of [Ple 77]. The continuation of the isometry $(L, \phi) \to (\mathfrak{a}, f)$ to $(V, \phi) \to (\mathbb{Q}P, f)$ maps $L^{\#}$ onto $f^{-1}\bar{\mathfrak{a}}^{-1}$. Hence $(|G|/p)\, f^{-1}\bar{\mathfrak{a}}^{-1} \subseteq \mathfrak{a}$, or $(|G|/p)\, \mathbb{Z}P \subseteq f\mathfrak{a}\bar{\mathfrak{a}}$, which establishes the first inclusion. To obtain the second inclusion, note the $\mathbb{Z}P$ is equal to its dual lattice with respect to T_1. But $T_1(\mathbb{Z}P, f\mathfrak{a}\bar{\mathfrak{a}}) = T_f(\mathfrak{a}, \mathfrak{a}) \subseteq \mathbb{Z}$. Hence $f\mathfrak{a}\bar{\mathfrak{a}} \subseteq \mathbb{Z}P$. (iii) From the proof of (ii) one gets $L^{\#}/L \cong f^{-1}\bar{\mathfrak{a}}^{-1}/\mathfrak{a}$. Multiplication with $f\bar{\mathfrak{a}}$ yields $L^{\#}/L \cong \mathbb{Z}P/f\mathfrak{a}\bar{\mathfrak{a}}$ (note $f\bar{\mathfrak{a}}$ becomes principal, if localized at primes).

Q.E.D.

(II.5) Corollary. *Under the hypothesis of* (II.4) *one has*

(i) $C_G(P) = P \times Z(G)$ *and*

(ii) (*cf.* [Fei 74] *Theorem* 10.2.6) *$N_G(P)$ is a split extension of $C_G(P)$ by a cyclic group of order $e \mid p-1$.*

Proof. (i) Since the ideal $\mathfrak{a}$ of (II.4) is invertible one has $\mathrm{End}_{\mathbb{Z}P}(L_P) \cong \mathrm{End}_{\mathbb{Z}P}(\mathfrak{a}) \cong \mathbb{Z}P$. But $C_G(P) = G \cap \mathrm{End}_{\mathbb{Z}P}(L_P)$ after obvious identifications and the units of finite order in $\mathbb{Z}P$ are up to sign the elements of P, since the projection of $\mathbb{Z}P$ onto $\mathbb{Z}[\zeta]$ induces a monomorphism of the unit groups by the description of $\mathbb{Z}P$ given earlier.

(ii) This follows from the more general result in [Fei 74] or from part (i): It is obvious, if $Z(G) = 1$ and via the determinant the case $Z(G) \neq 1$ can be reduced to the earlier case. Q.E.D.

For the further discussion of consequences of Theorem (II.4) a few comments on the unit group of $\mathbb{Z}P$ will be helpful. In view of later applications the group ring $\mathbb{Z}P$ will be identified with the ring $\mathbb{Z}[z_p]$ of circulants of degree p, where

$$z_p = \begin{pmatrix} 0 & & \\ \vdots & & I_{p-1} \\ 0 & & \\ 1 & 0 \cdots 0 & \end{pmatrix}$$

is the standard p-cycle of degree p in matrix form (I_n denotes the $n \times n$-unit matrix), cf. [New 72]. The involution now becomes transposing of matrices, totally positive elements of $\mathbb{Z}[z_p + z_p^{-1}] = \{x \in \mathbb{Z}[z_p] \mid x^{\mathrm{tr}} = x\}$ can be interpreted as positive definite symmetric matrices. Since the unit group $U(\mathbb{Z}[z_p])$ is given by $U(\mathbb{Z}[z_p + z_p^{-1}]) \times \langle z_p \rangle$, only the unit group $U(\mathbb{Z}[z_p + z_p^{-1}])$ of the subring $\mathbb{Z}[z_p + z_p^{-1}]$ is of interest.

(II.6) *Remark.* The epimorphism $\varepsilon\colon \mathbb{Z}[z_p + z_p^{-1}] \to \mathbb{Z}[\zeta + \zeta^{-1}]$ projecting $z_p + z_p^{-1}$ onto its eigenvalue $\zeta + \zeta^{-1}$ maps the unit group $E_p = U(\mathbb{Z}[z_p + z_p^{-1}])$ onto the subgroup $\tilde{U}_p = \{x \in U(\mathbb{Z}[\zeta + \zeta^{-1}]) \mid x \equiv \pm 1 \bmod \mathfrak{p}\}$ of $U_p = U(\mathbb{Z}[\zeta + \zeta^{-1}])$, where $\mathfrak{p}$ is the prime ideal of

$\mathbb{Z}[\zeta+\zeta^{-1}]$ containing p. The elements $\xi_i=\zeta^{(1-i)/2}(1-\zeta^i)/(1-\zeta)$ for $i=1,\ldots,(p-1)/2$ form representatives of the coset of $\tilde{U}_p$ in U_p. Let $U_p^+=\{x\in U_p \mid x \text{ totally positive}\}$ and $E_p^+=\{X\in E_p \mid X \text{ positive definite}\}$. Then $U_p^+/U_p^2\cong E_p^+/E_p^2$.

Proof. Clearly $\mathbb{Z}[z_p+z_p^{-1}]\cong\{(a,b)\in\mathbb{Z}\oplus\mathbb{Z}[\zeta_p+\zeta_p^{-1}] \mid a\equiv b \bmod \mathfrak{p}\}$. Hence $\varepsilon(E_p)=\tilde{U}_p$. Since $\xi_i\equiv i (\bmod\ \mathfrak{p})$, $1=\xi_1,\xi_2,\ldots,\xi_{(p-1)/2}$ form representatives of $\tilde{U}_p$-cosets in U_p. From the structure of the unit group U_p one concludes $U_p^2\cap\tilde{U}_p=\tilde{U}_p^2$ and $U_p/U_p^2\cong\tilde{U}_p/\tilde{U}_p^2$. Since the ξ_i^2 also form a full set $\tilde{U}_p^2$-coset representatives in U_p^2, one has $\tilde{U}_pU_p^2=U_p$, $\varepsilon(E_p^+)=U_p^+\cap\tilde{U}_p$, and $U_p^+/U_p^2\cong E_p^+/E_p^2$. Q.E.D.

It seems that frequently $U_p^+/U_p^2=1=E_p^+/E_p^2$ holds. In [Fei 74, Theorem 6.6] $U_p^+=U_p^2$ for $p\leqslant 23$ is proved, moreover Feit's argument for $p=23$ works for each prime number p of the form $2q+1$, where q is prime with 2 a primitive root mod q. According to [New 72, p. 191], Dade and Taussky have shown $E_p^+=E_p^2$ for all primes $p\leqslant 100$ except for $p=29$, cf. also [Dav 78]. Since by [Was 80, pp. 144 and 352], the ξ_i and -1 generate U_p for primes $p\leqslant 67$ one actually does not only have a constructive way to prove this but also an algorithm to replace an element $a\in\mathbb{Z}[\zeta_p+\zeta_p^{-1}]$ by a totally positive element generating the same ideal (if it exists), for $p\leqslant 67$, namely by solving linear equations over the field of 2 elements (representing signs).

Here is a rough sketch of the search for maximal f.i.u.g. of degree p based on Theorem (II.4) alone:

Step 1. Choice of the invertible ideal $\mathfrak{a}$ of $\mathbb{Z}[z_p]$. Clearly the ideal classes of $\mathbb{Z}[\zeta]$ are in 1–1 correspondence with the ideal classes of invertible $\mathbb{Z}[z_p]$-ideals. Choose from the set of representatives of the invertible $\mathbb{Z}[z_p]$-ideal classes modulo the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Tables of ideals of $\mathbb{Z}[\zeta]$ may be found in [Reu 75].

Step 2. Choice of a principal ideal $\mathfrak{f}$ of $\mathbb{Z}[z_p+z_p^{-1}]$ for given $\mathfrak{a}$. Because of (II.4)(ii) and (II.1)(iii) there are only finitely many principal ideal $\mathfrak{f}$ of $\mathbb{Z}[z_p+z_p^{-1}]$ with a generator f such that $(\mathfrak{a},f)$ is isometric to (L,ϕ_G) for some f.i.u.g. G. However, there are far too many possibilities for $\mathfrak{f}$ if one only applies (II.4)(ii) and (II.1)(iii). How this difficulty is overcome at least in dimensions $\leqslant 23$ will be discussed in the subsequent chapters.

Step 3. Choice of generator f of $\mathfrak{f}$ for $\mathfrak{a}$ and $\mathfrak{f}$ given. This amounts to replace some generator of $\mathfrak{f}$ by a totally positive generator f. This is always posible, if $E_p^+=E_p^2$, in which case f is essentially unique cf. (II.6) and discussion of (II.6).

Step 4. Find $\mathrm{Aut}(\mathfrak{a},f)$. In the cases where this was really necessary it was done by means of a computer, cf. Section IV. Note: to decide that

$\mathrm{Aut}(\mathfrak{a}, f)$ is absolutely irreducible one only has to find one element of $\mathrm{Aut}(\mathfrak{a}, f)$ which does not have the eigenvector of z_p eigenvalue 1 as eigenvector. As a final point in this section it remains to mention that the order of the normalizer $N_G(P)$ of a Sylow p-subgroup P in a maximal f.i.u.g. of degree p can usually be relatively easy computed by means of (II.3) if $E_p^+ = E_p^2$, cf. (II.6) above.

(II.7) LEMMA. *Let G be a maximal* f.i.u.g. *of degree p and let $(\mathfrak{a}, f)$ be isometric to (L, ϕ_G). Let $\alpha: z \to z^i$ be an automorphism of $P = \langle z \rangle$ and denote the induced automorphism of $\mathbb{Z}P$ also by α. Then α is induced by $N_G(P)$ if and only if*

(i) $\mathfrak{a}\alpha(\mathfrak{a})^{-1}$ *is a principal ideal $a\mathbb{Z}[z+z^{-1}]$ in $\mathbb{Z}[z+z^{-1}]$ and*

(ii) $a\bar{a}\alpha(f)f^{-1} \in E_p^2$.

Proof. Apply (II.3)(iii) and note $\{u\bar{u} \mid u \in U(\mathbb{Z}P)\} = E_p^2$. Q.E.D.

Of course the most convenient case is, if $\mathfrak{a}$ is principal. In this case one may choose $\mathfrak{a} = \mathbb{Z}P$, $z_p \in G$ and the Gram matrix F_G of ϕ_G is a circulant, namely f itself. Moreover in (II.7) one may choose $a = 1$.

III. REFLECTION GROUPS

In each dimension n some of the maximal finite subgroups G of $GL_n(\mathbb{Z})$ are reflection groups or contain a reflection subgroup of index 2. Before discussing these groups in prime dimensions some results for arbitrary dimensions will be presented. Recall, a (real) reflection is an involution in $GL_n(\mathbb{R})$ fixing an $(n-1)$-dimensional hyperplane of $\mathbb{R}^{n \times 1}$ pointwise, a reflection group is a group generated by reflections, and each finite reflection group in $GL_n(\mathbb{Q})$ can be described by its associated root system, cf., e.g., [Wit 41] and [Hum 72]. The following remark is an easy consequence of basic properties of root systems.

(III.1) *Remark.* Let G be a finite, irreducible subgroup of $GL_n(\mathbb{Q})$ containing a reflection. Then G is absolutely irreducible and hence fixed an essentially unique positive definite quadratic form $\phi = \phi_G$. Let $R = \langle g \in G \mid g \text{ reflection} \rangle$ and Γ the root system associated with R. Then

(i) $R \trianglelefteq \mathrm{Aut}(\Gamma)$ with $\mathrm{Aut}(\Gamma)$ consisting of all (ϕ-)orthogonal transformations which map Γ onto itself, in particular $R \trianglelefteq G \subseteq \mathrm{Aut}(\Gamma)$,

(ii) Γ decomposes into the union of orthogonal root systems all isomorphic to the same irreducible root system Γ_0 of rank d dividing n. In case $d \neq n$, $\mathrm{Aut}(\Gamma)$ is an imprimitive matrix group, namely equal to the wreath product $\mathrm{Aut}(\Gamma_0) \wr S_{n/d}$ of $\mathrm{Aut}(\Gamma_0)$ with the symmetric group $S_{n/d}$.

Moreover, cf. [Hum 72, p. 66], $\mathrm{Aut}(\Gamma_0)$ is a split extension of the reflection group corresponding to Γ with a group of order 1, 2, or—in the case of $\Gamma_0 = D_4$—of order 6.

Sometimes it is possible to predict for some finite subgroup G of $GL_n(\mathbb{Q})$ not containing reflections that finite groups H are contained in some $\mathrm{Aut}(\Gamma)$ for suitable root systems Γ. For instance, such a result was proved in [Ban 73] for the group G of all degree n permutation matrices of determinant 1 thus generalizing Burnsides answer for the same question with G consisting of all permutation matrices of degree n, cf. [Bur 12]. Of course, nowadays Burnside's result can be obtained as an immediate consequence of (III.1) and the classification of root systems. Bannai's result will be sharpened in Theorem (III.3) below with a completely different proof. For this and other purposes some special lattices have to be described, which are well known for a long time already, cf., e.g., [Cox 51].

The condition $*_p$ below for a prime p and a permutation group G of degree m with natural permutation lattice $M = \bigoplus_{i=1}^m \mathbb{Z}E_i$ ($gE_i := E_{g(i)}$ for $g \in G$, $i = 1, ..., m$) will be used:

($*_p$) M/pM has 2 irreducible $\mathbb{Z}/p\mathbb{Z}G$-constituents, namely the trivial one with multiplicity $1+\varepsilon$ and a $(m-1-\varepsilon)$-dimensional one with multiplicity 1, where $\varepsilon = 0$ for $p \nmid m$ and $\varepsilon = 1$ for $p \mid m$.

Apart from S_n and A_n on n symbols, M_{11} and M_{12} on 11 (resp. 12) points, also, for instance, $PSL_2(q)$ for $q \equiv \pm 3 \bmod 8$ on $q+1$ points satisfy $*_p$ for all primes p.

(III.2) Lemma. *Let G be a transitive permutation group of degree m with natural permutation lattice $M = \bigoplus_{i=1}^m \mathbb{Z}E_i$.*

(i) [Ple 77, *Theorem* 5.1]. *Let G be 2-transitive satisfying $*_p$ for all p, define $L = M/\mathbb{Z}\sum_{i=1}^m E_i$ as G-factor lattice of M, and $e_k = E_k + \mathbb{Z}\sum_{i=1}^m E_i$ for $k = l, ..., m$. Then all $\mathbb{Z}G$-sublattices of L are given by multiples of $L_d = \{\sum_{i=1}^m d_i e_i \mid d \text{ divides } \sum_{i=1}^m d_i\}$, where $d > 0$ divides m. Moreover the dual $L_d^{\#}$ of L_d with respect to some G-invariant rational scalar product $\phi \neq 0$ is a multiple of $L_{m/d}$.*

(ii) [Ple 77, *Theorem* 5.2 *and* 5.4]. *Assume G is transitive and satisfies $*_2$. Extend the action of G on M to the wreath product $\tilde{G} = C_2 \wr G$ of order $2^n |G|$ on M such that the base group of $C_2 \wr G$ induces all possible sign changes of the vectors E_i. Then the $\mathbb{Z}\tilde{G}$ sublattices of M are multiples of $M_1 = M$, $M_2 = \{\sum_{i=1}^m \alpha_i E_i \mid 2 \text{ divides } \sum_{i=1}^m \alpha_i\}$ and $M_3 = \{\sum_{i=1}^m \alpha_i E_i \mid \alpha_i \equiv \alpha_j (\bmod 2)\}$. Moreover the dual lattices with respect to a rational $\tilde{G}$-invariant scalar product ψ satisfy $M_1^{\#} \cong M_1$, $M_2^{\#} \cong M_3$, and $M_3^{\#} \cong M_2$.*

Note, for $m = n+1$ G of (III.2)(i) and for $m = n$ $\tilde{G}$ of (III.2)(ii) give rise to subgroups $\hat{G}$ and $\hat{\tilde{G}}$ of $GL_n(\mathbb{Q})$ via the action of G on $\mathbb{Q}L$ and $\tilde{G}$ on $\mathbb{Q}M$ such that all finite groups $H \leqslant GL_n(\mathbb{Q})$ containing $\hat{G}$ or $\hat{\tilde{G}}$ are contained in $\mathrm{Aut}(\Gamma)$ for some root system of rank n. Namely each such H is contained in some $\mathrm{Aut}(L_d, \phi)$ or $\mathrm{Aut}(M_i, \psi)$, which clearly contain reflections. The following result was proved already in [Ple 80, Satz (II.12)].

(III.3) THEOREM. *Let G be a 2-transitive permutation group of degree n embedded into $GL_n(\mathbb{Q})$ as group of permutation matrices and assume G satisfies $*_p$ for $m = n$ and all primes p. Then any finite group H with $G \leqslant H \leqslant GL_n(\mathbb{Q})$ can be embedded into* $\mathrm{Aut}(\Gamma)$ *for some root system Γ of rank n containing the root system A_{n-1}.*

Note though the scalar product going with Γ in (III.3) is not necessarily unique, $\mathrm{Aut}(\Gamma)$ is well defined up to conjugacy in $GL_n(\mathbb{Q})$.

Proof. H acts on some lattice L of $\mathbb{Z}$-rank n in $\mathbb{Q}^{n \times 1}$ and fixes some positive definite scalar product ϕ of $\mathbb{Q}^{n \times 1}$. It suffices to prove that the group $G_n \supset G$ of all permutation matrices of degree n also operates on L and fixes ϕ. (Note, G_n can be viewed as reflection group corresponding to the root system A_{n-1}.) Namely then $\langle H, G_n \rangle$ is finite and contains reflections, and (III.1) can be applied either to $\langle H, G_n \rangle$ directly if $\langle H, G_n \rangle$ is irreducible, or to the $(n-1)$-dimensional constituent group of $\langle H, G_n \rangle$. By 2-transitivity G_n and G both fix a 2-dimensional space of quadratic forms, which must be the same since $G \subseteq G_n$. Hence G_n fixes ϕ. That G_n also acts on L follows from the fact that the sets of $\mathbb{Z}G$- and the $\mathbb{Z}G_n$-lattices contained in $\mathbb{Q}^{n \times 1} = \mathbb{Q}L$ are exactly the same. One has $\mathbb{Q}^{n \times 1} = V_1 \oplus V_{n-1}$ where V_1 consists of the G_n-fixed points in $\mathbb{Q}^{n \times 1}$ and V_{n-1} is the unique $\mathbb{Q}G_n$-complement. By 2-transitivity V_{n-1} and $V_1 (\cong \mathbb{Q})$ are irreducible as $\mathbb{Q}G_n$- and as $\mathbb{Q}G$-modules. From (III.2)(i) one gets that $L \cap V_{n-1}$ and (trivially) $L \cap V_1$ are $\mathbb{Z}G_n$-lattices; also $\pi_1(L)$ and $\pi_{n-1}(L)$ are $\mathbb{Z}G_n$-lattices, where $\pi_i \colon \mathbb{Q}^{n \times 1} \rightarrow V_i$ are the projections for $i = 1$, $n-1$. Moreover, G as well as G_n act trivially on $\pi_1(L)/L \cap V_1$, hence also on the isomorphic module $\pi_{n-1}(L)/L \cap V_{n-1}$, cf. [Ple 78, Chap. 2]; hence each $\mathbb{Z}$-lattice X with $(V_1 \cap L) \oplus (V_{n-1} \cap L) \leqslant X \leqslant \pi_1(L) \oplus \pi_2(L)$ is a $\mathbb{Z}G_n$—as well as a $\mathbb{Z}G$-lattice. Hence G_n also acts on L. Q.E.D.

(III.4) *Remark.* Let

$$z = \begin{pmatrix} 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \end{pmatrix} \in GL_n(\mathbb{Z})$$

be the standard n-cycle generating the ring $\mathbb{Z}[z]$ of $n \times n$-circulants.

(i) Each of the lattices L_d of rank $n = m - 1$ with $d \mid m$ described in (III.2)(i) with G-invariant scalar product ϕ has the circulant Gram matrix aF_d for some $a \in \mathbb{Q}$ with respect to a suitable $\mathbb{Z}$-basis of L_d. Namely, if $\gamma_d = 1 + z + \cdots + z^{d-1}$ then $F_d = (1/d\tilde{d})\, \gamma_d^{\mathrm{tr}}(mI_n + J_n)\, \gamma_d = (1/d\tilde{d})[m(dI_n + \sum_{i=1}^{d}(d-i)(z^i + z^{-i})) - d^2 J_n]$ with $I_n, J_n \in \mathbb{Z}^{n \times n}$ the unit matrix (resp. the matrix) with all entries equal to 1 and $\tilde{d} = gcd(d, m/d)$.

(ii) For $n = m$ odd the lattices M_2 and M_3 of (III.2)(ii) with $\tilde{G}$-invariant scalar product ψ have the circulant matrices $a\tilde{F}_2$ (resp. $a'\tilde{F}_3$) for some $a, a' \in \mathbb{Q}$ as Gram matrices with respect to suitable bases, where $\tilde{F}_2 = \gamma_2^{\mathrm{tr}}\gamma_2 = 2I_n + z^2 + z^{-2}$ and

$$\tilde{F}_3 = 4\gamma_2^{-\mathrm{tr}}\gamma_2^{-1} = nI_n - (n-2)(z + z^{-1}) + (n-4)(z^2 + z^{-2}) \\ - (n-6)(z^3 + z^{-3}) + \cdots \pm (z^{(n-1)/2} + z^{-(n-1)/2}).$$

Proof. (i) Clearly the Gram matrix of ϕ with respect to the basis $(e_1, ..., e_n)$ is a multiple of $mI_n - J_n$. It remains to show that the columns of γ_d represent coordinate columns of a $\mathbb{Z}$-basis of L_d with respect to $(e_1, ..., e_n)$. That these vectors lie in L_d is obvious and $|\det \gamma_d| = d$ $(= [L_1 : L_d])$ can be seen from the eigenvalues of γ_d which are d and units in the n-th cyclotomic field.

(ii) Clear. Q.E.D.

In view of the discussion of positive definite units of $\mathbb{Z}[z + z^{-1}]$ in [New 72, Chap. X, Sect. 6 ff], (III.4)(i) yields infinitely many such units which are not of the form $g^{\mathrm{tr}}g$ for some $g \in GL_n(\mathbb{Z})$. Namely choose (n, d) such that $d^2 = n + 1$ $(= m)$, then $F_d \in \mathbb{Z}[z + z^{-1}]$ is unimodular. In particular, the root lattice of the root system E_8 admits a circulant Gram matrix, as already proved in [NeT 56]. In dimension 24 (III.4)(i) together with taking tensor products yields two inequivalent positive definite units of $\mathbb{Z}[z + z^{-1}]$ both of which are not of the form $g^{\mathrm{tr}}g$ with $g \in GL_{24}(\mathbb{Z})$. However the positive definite units of $\mathbb{Z}[z + z^{-1}] \subseteq \mathbb{Z}^{24 \times 24}$ modulo $\{g^{\mathrm{tr}}g \mid g \in GL_{24}(\mathbb{Z})\}$ form an elementary abelian group of order 8, with a subgroup of order 4 represented by odd lattices. Unfortunately, the Leech lattice does not have a circulant Gram matrix.

The rest of this section is restricted to f.i.u.g. of prime degree $p > 2$; the notation of Section II is kept.

(III.5) Lemma. *Let $G \leqslant GL_p(\mathbb{Z})$ be a* f.i.u.g. *such that $p - 1$ of the p elementary divisors of the Gram matrix F_G of ϕ_G are equal. Then there exists a nonsingular matrix $X \in \mathbb{Q}[z]$, where $z \in G$ has order p, such that $\tilde{G} = X^{-1}GX \leqslant GL_p(\mathbb{Z})$ and $F_{\tilde{G}}$ has $p - 1$ elementary divisors equal to* 1.

Proof. Let $P = \langle z \rangle$ be a Sylow p-subgroup of G. For the natural $\mathbb{Z}G$-lattice L one has $L^{\#}/L \cong \mathbb{Z}/a\mathbb{Z} \oplus (\mathbb{Z}/b\mathbb{Z})^{p-1}$ (as abelian groups) with $\gcd(a, b) = 1$. All prime divisors q of a or b divide $|G|/p$ by Theorem (II.4), and hence are smaller than p. No prime ideal $\mathfrak{q}$ of $\mathbb{Z}[\zeta_p]$ has norm q, since $p \nmid q \pm 1$ for $p > 3$ and $p = 3$ is obvious. Therefore the $\mathbb{Z}P$-ideal $\mathfrak{a}$ isomorphic to L_P (as $\mathbb{Z}P$-lattice) projects onto the same ideal of $\mathbb{Z}[\zeta_p]$ as the $\mathbb{Z}P$-ideals $\mathfrak{a}'$ with $\mathfrak{a}' \subset \mathfrak{a}$ and $\mathfrak{a}/\mathfrak{a}'$ cyclic of order b. Hence the $\mathbb{Z}G$-lattice bL_a of index a in L, where L_a is the unique sublattice of index a of $L^{\#}$ containing L, is isomorphic to L as $\mathbb{Z}P$-lattice. Moreover, the action of G on bL_a gives rise to the f.i.u.g. $\tilde{G}$ with the desired properties. Q.E.D.

The hypothesis of the next theorem was already explained in (II.6) and the comments following (II.6).

(III.6) THEOREM. *Assume that each totally positive unit of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ is a square in $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Let $G \leqslant GL_p(\mathbb{Z})$ be a* f.i.u.g. *containing the standard p-cycle z_p such that $p-1$ of the elementary divisors of the Gram matrix of (L_G, ϕ_G) are equal. Then $G \leqslant \mathrm{Aut}(\Gamma)$ for some root system Γ of rank p.*

Proof. By Lemma (III.5) it may be assumed that $p-1$ elementary divisors of F_G are equal to 1, i.e., $L^{\#}/L$ is cyclic, and (L, ϕ_G) isometric to $(\mathbb{Z}[P], f)$ for $f \in \mathbb{Z}[z_p + z_p^{-1}] \subseteq \mathbb{Z} \oplus \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ such that the $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$-component is a unit. Note, because of $z_p \in G$ we may choose $\mathfrak{a} = \mathbb{Z}[P]$. Because every totally positive unit of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ is a square, one may assume by (II.6) and (II.3) that the $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$-component of f is equal to 1. Let $v \in \mathbb{Z}[P]$ correspond to $(0, 1 - \zeta_p)$ under the embedding of $\mathbb{Z}P$ into $\mathbb{Z} \oplus \mathbb{Z}[\zeta_p]$. Then $\phi_G(v, v) = 2$ and hence $\mathrm{Aut}(L, \phi_G)$ contains reflection $x \mapsto x - \phi_G(x, v)\, v$. The result now follows from (III.1). Q.E.D.

Note, the lattices of the group turning up in (III.6) have been described in (III.2) and (III.4).

(III.7) COROLLARY. *Assume $p = 2q + 1$ with q prime and that totally positive units of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ are squares in $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. If $\sigma_0(n)$ denotes the number of divisors of $n \in \mathbb{N}$, then there are $3 + \sigma_0(p+1)$ conjugacy classes of maximal* f.i.u.g. *in $GL_p(\mathbb{Z})$ for $q > 1$, which contain one group G with $z_p \in G$. For $p = 3$ this number is $3 = \sigma_0(p+1)$. Always the groups of three classes are isomorphic to $C_2 \wr S_p$ and except for $p = 7$ the groups of the other $\sigma_0(p+1)$ classes are isomorphic to $C_2 \times S_{p+1}$. For $p = 7$ only two of the $\sigma_0(8)$ other groups are isomorphic to $C_2 \times S_p$ and two are isomorphic to $W(E_7)$.*

Proof. By (III.6) and the discussion before (II.4) one only has to show that each prime number $r \in \mathbb{N}$, $r < p$ generates a prime ideal in $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. This is trivial for $p = 3$ and for the other cases it follows since r or $-r$ is a primitive root modulo p (note, $\mathbb{Z}/p\mathbb{Z}^* \cong C_2 \times C_q$). Since the lattices have been described earlier in this chapter and since their automorphism groups can easily be determined from (III.1), the claim follows. Q.E.D.

(III.8) Corollary. *For $p=3$ there are three, and for $5 \leqslant p \leqslant 11$ there are $3+\sigma_0(p+1)$ conjugacy classes of maximal* f.i.u.g. *of degree p.*

Proof. Because of (III.8) it remains to show that each conjugacy class of maximal f.i.u.g. of degree $p \leqslant 11$ contains a representative G with $z_p \in G$. But this is clear, since the class number of $\mathbb{Q}[\zeta_p]$ is equal to 1 for $p \leqslant 19$, cf., e.g., [Was 82]. Q.E.D.

Of course (III.8) was well known for $p=3$, and also for $p \leqslant 7$, cf. [PlP 77, 80, Part 1]. For completeness sake the circulant Gram matrices F_G of suitable representatives G for the conjugacy classes of maximal f.i.u.g. of degree $p \leqslant 11$ will be given. Notation: $(a_0, ..., a_{(p-1)/2})$ corresponds to $F_G = a_0 I_p + \sum_{i=1}^{(p-1)/2} a_i(z_p^i + z_p^{-i})$ ($I_p =$ unit matrix, $z_p =$ standard p-cycle).

$p=3$: $(1,0), (3,-1), (2,1)$ $(G \cong C_2 \wr S_3 \cong C_2 \times S_4)$;

$p=5$: $(1,0,0), (2,0,1), (5,-3,1)$ $(G \cong C_2 \wr S_5)$,

$(5,-1,-1), (4,1,-2), (3,1,-1), (2,1,1)$ $(G \cong C_2 \times S_6)$;

$p=7$: $(1,0,0,0), (2,0,1,0), (7,-5,3,-1)$ $(G \cong C_2 \wr S_7)$,

$(7,-1,-1,-1), (2,1,1,1)$ $(G \cong C_2 \times S_8)$,

$(3,1,-1,-1), (2,1,0,-1)$ $(G \cong W(E_7))$;

$p=11$: $(1,0,0,0,0,0), (2,0,1,0,0,0), (11,-9,7,-5,3,-1)$

$(G \cong C_2 \wr S_{11})$,

$(11,-1,-1,-1,-1,-1), (5,2,-1,-1,-1,-1)$,

$(9,5,1,-3,-3,-3), (8,5,2,-1,-4,-4)$,

$(3,2,1,0,-1,-2), (2,1,1,1,1,1)$ $(G \cong C_2 \times S_{12})$.

IV. Some Strategies for Finding Maximal f.i.u.g. of Degree p

The notation of Section II is kept. Additionally π_1 and π_2 denote the epimorphisms of $\mathbb{Q}[z_p + z_p^{-1}]$ onto $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$, respectively, $(\zeta = \zeta_p)$. Among the possibilities for $(\mathfrak{a}, f)$ isometric to (L, ϕ_G) for some f.i.u.g. G left open in Theorem (II.4) the case $\mathfrak{a}$ principal, i.e., without loss of generality $\mathfrak{a} = \mathbb{Z}P$, and $\pi_2(f)\, \mathbb{Z}[\zeta_p + \zeta_p^{-1}] = m\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ for some $m \in \mathbb{N}$ has been settled in Theorem (III.6) for those p with $U_p^+ = U_p^2$, cf. (II.6). A way to handle the possibly large number of remaining possibilities can be based on the following theorem.

(IV.1) THEOREM. *Let $G \leqslant GL_p(\mathbb{Z})$ be a* f.i.u.g.

(i) [Fei 74] *There is a $\mathbb{Z}G$-sublattice M of $L = L_G$ with $[L : M] < \infty$ and an $\alpha \in \mathbb{Q}_{>0}$ such that the dual lattice $M^{\#}$ of M with respect to $\alpha\phi$ satisfies: $M \subseteq M^{\#}$ and for each prime q the Sylow q-subgroup of $M^{\#}/M$ is elementary abelian of rank less than $(p+1)/2$.*

(ii) *The lattice of $\mathbb{Z}G$-submodules of L is distributive; more precisely a $\mathbb{Z}P$-isomorphism $\varphi \colon L \to \mathfrak{a}$ of L onto a $\mathbb{Z}P$-ideal $\mathfrak{a}$ maps $M \leqslant_{\mathbb{Z}G} L$ with $M \nsubseteq qL$ for any prime q onto $\mathfrak{a}\mathfrak{a}'$ for some integral invertible ideal $\mathfrak{a}'$ of $\mathbb{Z}P$ with $(|G|/p)\,\mathbb{Z}P \subseteq \mathfrak{a}' \subseteq \mathbb{Z}P$.*

Proof. (i) This follows from general results of [Fei 74, Chap. 3], namely 3.4 and 3.18.

(ii) The distributivity follows from [Ple 77, Theorem 3.19] and the fact that L/qL has no repeated $\mathbb{Z}/q\mathbb{Z}G$-composition factors for all primes q. The latter is clear for $q = p$, since L lies in a p-block of defect zero, and it follows for all other q by restricting the operation to P and observing that $x^p - 1$ has no repeated factors as polynomial over $\mathbb{Z}/q\mathbb{Z}$. The rest follows from Theorem (II.4) and [Ple 77, Theorem 2.8]. Q.E.D.

Theorem (IV.1) allows to improve the strategy for searching the maximal f.i.u.g. of degree p sketched at the end of Section II as follows:

(A) Perform steps 2, 3, and 4 only for those totally positive $f \in \mathbb{Q}[z_p + z_p^{-1}]$ satisfying

(**) $s_p\mathbb{Z}P \subseteq \mathfrak{a}\bar{\mathfrak{a}}f \subseteq \mathbb{Z}P$ and $\operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}P/\mathfrak{a}\bar{\mathfrak{a}}f) \leqslant (p-1)/2$ where s_p is the product of all prime numbers $q < p$.

(B) Find the minimal irreducible subgroups G of the irreducible $\operatorname{Aut}(\mathfrak{a}, f)$ found under (A) (up to conjugacy). For each such G find $\operatorname{Aut}(M, \phi_G)$ where M is a $\mathbb{Z}G$-sublattice of $L = L_G$ with $M \nsubseteq qL$ for all primes q (cf. (IV.1)(ii)).

Some comments are necessary. Finding $\operatorname{Aut}(\mathfrak{a}, f)$ might sometimes be complicated. In the context of (A) the implemented algorithm for finding automorphism groups of lattices of [PlP 83] was successfully applied in dimensions 13, 17, and 19, where no applications of Section III were possible. In dimension 23 most discussions could be reduced to well-known lattices. The restriction in (**) leaves only very few possibilities for f; sometimes, cf., e.g., dimension 19, even more f's can be excluded by theoretical arguments. As for (B) there are two strategies both based on Theorem (IV.1)(ii) possible:

(B1) Check G-invariance of candidates M as given in (IV.1)(ii).

(B2) Compute $\mathrm{Aut}(M, \phi_G)$ for candidates M as given in (IV.1)(ii).

In both cases one certainly will minimize the computations by checking the candidates M in a suitable order, e.g., one will first try to find $\mathbb{Z}G$-lattices defining composition series for L/qL for prime divisors q of $|G|$ and use this to find all relevant $\mathbb{Z}G$-sublattices of L layer by layer: first the maximal, then the second maximal sublattices etc. In the case of (B1) this is a simplified version of the centering algorithm applied in [PlP 77, 80], which only involves finding lattice bases, inverting and multiplying matrices in this case. It should be noted that the idea of starting out with minimal irreducible groups was also already used in [PlP 77, 80]. In the situation of (B1) the full automorphism groups are usually not difficult to find since they are up to $GL_p(\mathbb{Q})$-conjugacy subgroups of the automorphism groups found under (A) already by (IV.1)(i). For both, finding the G's in (B) and the automorphism groups in (B2) (II.2) and (II.5) might be a help. In case $E_p^2 = E_p^+$, cf. (II.6), Lemma (II.7) can be used in the context of (B1) or (B2) as a sufficient criterion for those candidates M which must be dropped because not even $N_G(P)$ operates on them. Also in the case $E_p^2 = E_p^+$ in the terminology of (II.6), it is easy to distinguish the conjugacy classes of maximal f.i.u.g. of degree p, since the totally positive $f \in \mathbb{Z}[z_p + z_p^{-1}]$ is uniquely determined up to squares of units by the ideal $f\mathbb{Z}[z_p + z_p^{-1}]$. For instance, in dimensions $p \leqslant 19$ the elementary divisors of F_G will be sufficient to distinguish the conjugacy classes of maximal f.i.u.g. in $GL_p(\mathbb{Z})$, and for $p = 23$ in addition to this $\mathfrak{a} \cong L_P$ principal or not principal has to be taken into account. At the end of these general remarks another a priori restriction for the possibilities for f will be indicated. Note, it is convenient to consider all those candidates $f \in \mathbb{Q}[z_p + z_p^{-1}]$ simultaneously for which $\pi_2(f)$ generates the same $\mathbb{Z}[\zeta + \zeta^{-1}]$-ideal. It is convenient and without loss of generality to assume $\mathfrak{a} \leqslant \mathbb{Z}[z_p]$ and $\mathfrak{a}$ is mapped onto $\mathbb{Z}$ under the epimorphism of $\mathbb{Q}[z_p]$ onto $\mathbb{Q}$ or equivalently $J_p \mathfrak{a} = \mathbb{Z} J_p$ for $J_p = \sum_{i=0}^{p-1} z_P^i$.

(IV.2) *Remark.* Assume $E_p^+ = E_p^2$ (cf. (II.6)). Let $\mathfrak{a} \trianglelefteq \mathbb{Z}[z_p]$ be an invertible ideal with $J_p \mathfrak{a} = p\mathbb{Z}$, and assume that $f \in \mathbb{Q}[z_p + z_p^{-1}]$ is totally positive and satisfies (**) of (A). Up to multiplication by elements of E_p^2 (cf. (II.3)) all totally positive $f' \in \mathbb{Q}[z_p + z_p^{-1}]$ satisfying (**) and for which $\pi_2(f)$ and $\pi_2(f')$ generate the same $\mathbb{Z}[\zeta + \zeta^{-1}]$-ideal are given by $\Xi_i^2 f + \alpha J_p$ with $i^2 \pi_1(f) + p\alpha > 0$, $\alpha \in \mathbb{Z}$, and $1 \leqslant i \leqslant (p-1)/2$, where $\Xi_i^2 = iI_p + \sum_{j=1}^{i} (i-j)(z_p^i + z_p^{-i})$ is the $p \times p$-circulant with first row $(i, i-1, \ldots, 1, 0, \ldots, 0, 1, \ldots, i-1)$.

Proof. By (II.6) and the proof of (II.6) the elements $\pi_2(f)\,\xi_i^2$ for $1 \leqslant i \leqslant (p-1)/2$ form a set of representatives of the U_p^2-orbits on the totally positive generators of $\pi_2(f)\,\mathbb{Z}[\zeta+\zeta^{-1}]$. But $\pi_2(\Xi_i^2)=\xi_i^2$. Hence any f' with the conditions in (IV.2) can be multiplied by an element of E_p^2 such that it differs from $\Xi_i^2 f$ for some i, $1 \leqslant i \leqslant (p-1)/2$ only by a rational multiple $\alpha \cdot J_p$ of J_p for some $\alpha \in \mathbb{Q}$. Since $\pi_1(\Xi_i^2)=i^2$, total positivity yields $i^2\pi_1(f)+p\alpha>0$. Finally $\mathfrak{a}\bar{\mathfrak{a}}f' \leqslant \mathbb{Z}P$ and $J_p\mathfrak{a}=\mathbb{Z}J_P$ yield $\alpha \in \mathbb{Z}$. Q.E.D.

(IV.3) Lemma. *Let $\mathfrak{a} \trianglelefteq \mathbb{Z}[z_p]$ be an invertible ideal, $f \in \mathbb{Q}[z_p+z_p^{-1}]$ totally positive with $T_f(\mathfrak{a},\mathfrak{a}) \subseteq \mathbb{Z}$. Define $m(f,\mathfrak{a})=\min\{T_f(x,x) \mid x \in (1-z_p)\,\mathfrak{a}, x \neq 0\}$ and $M(f,\mathfrak{a})=\min\{T_f(x,x) \mid x \in \mathfrak{a}\backslash(1-z_p)\,\mathfrak{a}\}$. The following holds.*

(i) *$m(f+J_p,\mathfrak{a})=m(f,\mathfrak{a})$. Moreover, if $E_p^+=E_p^2$ (cf. (II.6)), then $m(f',\mathfrak{a})=m(f,\mathfrak{a})$ for any totally positive $f' \in \mathbb{Q}[z_p+z_p^{-1}]$ with $\pi_2(f')$ generating the same $\mathbb{Z}[\zeta+\zeta^{-1}]$-ideal as $\pi_2(f)$.*

(ii) *If* Aut$(\mathfrak{a}, f+\alpha J_p)$ *is irreducible for an $\alpha \in \mathbb{Z}_{\geqslant 0}$, then $\alpha \leqslant m(f,\mathfrak{a})-M(f,\mathfrak{a})$. (Note, this is applied in the case $f-J_p$ not totally positive.)*

Proof. (i) The first statement is clear from $J_p(1-z_p)=0$. The second follows from the first, (II.3) and (II.6).

(ii) Let $x \in (1-z_p)\,\mathfrak{a}$ with $T_f(x,x)=m(f,\mathfrak{a})$. Since Aut$(\mathfrak{a}, f+\alpha J_p)$ is irreducible, there is some $y \in \mathfrak{a}\backslash(1-z_p)\,\mathfrak{a}$ lying in the Aut$(\mathfrak{a}, f+\alpha J_p)$-orbit of x. Hence $m(f,\mathfrak{a})=T_{f+\alpha J_p}(y,y)=T_f(y,y)+\alpha T_{J_p}(y,y)$ and therefore $\alpha \leqslant \alpha T_{J_P}(y,y)=m(f,\mathfrak{a})-T_f(y,y) \leqslant m(f,\mathfrak{a})-M(f,\mathfrak{a})$. Q.E.D.

The last result is sometimes useful to see quickly that an integral form has a reducible automorphism group; it supplements (II.4) but can also be applied in dimensions which are not prime numbers.

(IV.4) Proposition. *Let (L,ϕ) be an integral lattice of dimension n with $\phi\colon L \times L \to \mathbb{Z}$ positive definite. Let q be a prime number dividing the discriminant of (L,ϕ) only to the first power such that $q \neq n+1$ and $n<2(q-1)$. Then* Aut(L,ϕ) *is not absolutely irreducible.*

Proof. Assume $G=\text{Aut}(L,\phi)$ is absolutely irreducible. By Minkowski's bound (cf. (II.1)(iii) for $n=p$) and Theorem 2.8 of [Ple 77] (cf. also proof of (II.4)) q divides $|G|$ exactly to the first power. Let R denote the q-adic integers. Since 1-dimensional RG/qRG-modules can be lifted to RG-lattices, i.e., are of the form X/qX for some RG-lattice X of R-rank 1, it is an elementary property to the Brauer tree that the projective cover of the RG-lattice $R \otimes_{\mathbb{Z}} L^{\#}$ is of R-rank $n+1$. This is a contradiction, since q does not divide $n+1$. Q.E.D.

A short word on the computer calculation of $\mathrm{Aut}(L, \phi)$ might be appropriate; a detailed account of the methods is given in [PlP 84]. Let $(b_1, ..., b_n)$ be a $\mathbb{Z}$-basis of L. Then the elements of $\mathrm{Aut}(L, \phi)$ can be identified with the n-tuples $(b'_1, ..., b'_n)$ of vectors in L satisfying $\phi(b'_i, b'_j) = \phi(b_i, b_j)$ for $1 \leqslant i, j \leqslant n$. The algorithm in [PlP 85] is essentially a backtrack search of such tuples $(b'_1, ..., b'_n)$, possibly under the assumption that some of the b'_i are already preassigned. For identifying the isomorphism type of $\mathrm{Aut}(L, \phi)$ the permutation representation on a certain set of vectors in L, e.g., the vectors of minimum length is used. The resulting permutation groups can easily be investigated by means of CAYLEY, cf., e.g., [Can 74].

V. Dimensions 13, 17, and 19

The class number of $\mathbb{Q}(\zeta_p)$ is 1 for $p \leqslant 19$, cf., e.g., [Was 82]. Hence one may assume $z_p \in G$, and—in the terminology of (II.4)—$\mathfrak{a} = \mathbb{Z}P = \mathbb{Z}[z_p]$ and $f = F_G$ in step 1 of the discussion at the end of Section II. The modifications of Section IV will be taken into account; the notation of the previous sections is kept and $f(a_0, ..., a_{(p-1)/2})$ is used as shorthand notation for $a_0 I_p + \sum_{i=1}^{(p-1)/2} a_i(z_p^i + z_p^{-i})$.

(a) $p = 13$.

Let $f = f(a_0, ..., a_6) \in \mathbb{Q}[z_{13} + z_{13}^{-1}]$ be totally positive satisfying (**) of Section IV. Since $\mathfrak{a} = \mathbb{Z}[z_{13}]$ one has $f \in \mathbb{Z}[z_{13} + z_{13}^{-1}]$ and there are four possibilities for the ideal of $\mathbb{Z}[\zeta + \zeta^{-1}]$ generated by $\pi_2(f)$, namely $\mathbb{Z}[\zeta + \zeta^{-1}]$, $\mathfrak{q}_3$, $\mathfrak{q}_5$, $\mathfrak{q}_3 \cdot \mathfrak{q}_5$, where $\mathfrak{q}_3$ (resp. $\mathfrak{q}_5$) is a fixed prime ideal of $\mathbb{Z}[\zeta + \zeta^{-1}]$ containing 3 (resp. 5). (Note, 2, 7, and 11 are primitive roots mod 13, and 3, -1 (resp. 5, -1) generate subgroups of order 6 (resp. 4) of $(\mathbb{Z}/13\mathbb{Z})^*$. Note also the transitivity of $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q})$ on the prime ideals above 3 (resp. 5) and on the products of a prime ideal containing 3 with one containing 5.)

If $\pi_2(f)$ is a unit in $\mathbb{Z}[\zeta + \zeta^{-1}]$, the result of Section III imply that only $f = I_{13}$ and $f = I_{13} + J_{13}$ (with $J_{13} = \sum_{i=0}^{12} z_{13}^i$) have to be investigated.

The case $\pi_2(f)\,\mathbb{Z}[\zeta + \zeta^{-1}] = \mathfrak{q}_3$ will be discussed in some more detail; the argument for the other cases are simular and will be omitted. According to (IV.2) the relevant elements f with $\pi_2(f)\,\mathbb{Z}[\zeta + \zeta^{-1}] = \mathfrak{q}_3$ come into 6 series distinguished by $\pi_1(f) \bmod 13$, namely $f \in \{f_{3,i} + \alpha J_{13} \mid i = 1, 4, 3, 12, 9, 10, \alpha \in \mathbb{Z}_{\geqslant 0}\}$, where the $f_{3,i}$ can be chosen, e.g., as $f_{3,1} = f(3, 1, -1, -1, 0, 0, 0)$, $f_{3,4} = f(4, 2, 1, -1, -1, -1, 0)$, $f_{3,3} = f(5, 3, 2, 1, -1, -3, -3)$, $f_{3,12} = f(4, 2, 2, 1, 0, 0, -1)$, $f_{3,9} = f(3, 0, 1, 0, 0, 1, 1)$, and $f_{3,10} = f(4, 2, 0, -1, -1, 1, 2)$ (note $\pi_1(f_{3,i}) = i$). One easily checks $m(f, \mathbb{Z}[z_{13}]) = 4$ for all these elements f, cf. (IV.3)). By applying condition (**) of Section IV, (IV.3)(ii) and (IV.4), one concludes that $f_{3,1}$,

$f_{3,14} = f_{3,1} + J_{13}$, and $f_{3,10}$ are the only forms whose automorphism groups have to be checked for irreducibility.

An analogous discussion for $\pi_2(f)\,\mathbb{Z}[\zeta + \zeta^{-1}] = \mathfrak{q}_5$ yields $f_{5,2} = f(4, -2, 0, 1, 0, -1, 1)$, $f_{5,6} = f(4, 0, 0, 1, -1, 0, 1)$, $f_{5,5} = f(3, 0, 1, -1, 0, 0, 1)$, and $f_{5,7} = f(3, 0, 1, 1, 0, 0, 0)$ as only forms to be investigated. Finally, if $\pi_2(f)\,\mathbb{Z}[\zeta + \zeta^{-1}] = \mathfrak{q}_3\mathfrak{q}_5$, then $m(f, \mathbb{Z}[z_{13}]) = 6$ and 5 possibilities for f have to be taken into account, namely $\pi_1(f) \in \{6, 5, 7, 2, 11\}$.

The automorphism program of [PlP 85] shows that 2 of these 11 forms have an irreducible automorphism group, namely $f_{3,1}$ and $f_{5,2}$. For instance, the lattices for the last 5 forms contain up to sign only 13 vectors of minimum length. Since they are not pairwise orthogonal, the automorphism group must act reducibly. In some other cases more detailed information has to be used from the machine calculation. Usually one can see that the group order is less than 13^2. As the final result of this discussion and machine computation one has the following.

(V.1) LEMMA. *Up to isometry, there are four lattices* $(\mathbb{Z}[z_{13}], f)$ *with* $f \in \mathbb{Q}[z_{13} + z_{13}^{-1}]$ *totally positive and satisfying* (**) *of Section* IV *such that* $\mathrm{Aut}_{\mathbb{Z}}(f) = \mathrm{Aut}(\mathbb{Z}[z_{13}], f)$ *is irreducible*:

(i) $f = f_{1,1} = I_{13}$ *with automorphism group isomorphic to* $C_2 \wr S_{14}$;

(ii) $f = f_{1,14} = f(2, 1, \ldots, 1)$ *with automorphism group isomorphic to* $C_2 \times S_{14}$;

(iii) $f = f_{3,1} = f(3, 1, -1, -1, 0, 0, 0)$ *with automorphism group isomorphic to* $C_2 \times \widetilde{SL_3(3)}$, *where* $\widetilde{SL_3(3)}$ *is* $SL_3(3)$ *extended by the automorphism* $g \to g^{-\mathrm{tr}}$ *of order* 2;

(iv) $f = f_{5,2} = f(4, -2, 0, 1, 0, -1, 1)$ *with automorphism group isomorphic to* $C_2 \times \widetilde{PSL_2(25)}$, *where* $\widetilde{PSL_2(25)}$ *is the extension of* $PSL_2(25)$ *by the Frobenius automorphism of order* 2.

Proceeding to (B) of Section IV the minimal irreducible subgroups of the four groups listed above have to be identified, which is easily done by means of (II.2). $\mathrm{Aut}_{\mathbb{Z}}(I_{13})$ has up to conjugacy two such subgroups, one isomorphic to $SL_3(3)$ and the other to a subgroup of index 2 of $C_2 \wr C_{13}$; cf. [Sim 70] for the transitive permutation groups of degree 13. $\mathrm{Aut}_{\mathbb{Z}}(f_{1,14})$ has one such subgroup up to conjugacy, namely f of isomorphism type $PSL_2(13)$; cf. also [Sim 70] for the 2-transitive permutation groups of degree 14. Finally $\mathrm{Aut}_{\mathbb{Z}}(f_{3,1})$ and $\mathrm{Aut}_{\mathbb{Z}}(f_{5,2})$ have their commutator subgroups (isomorphic to $SL_3(3)$ and $PSL_2(25)$ resp.) as unique minimal irreducible subgroups.

According to (B), Section IV, the sublattices of the natural $\mathbb{Z}G$-lattice L

have to be found for each of the four minimal f.i.u.g. just discussed. In case G is isomorphic to a subgroup of index 2 of $C_2 \wr C_{13}$, the group $\bar{G} = \langle G, -I_{13} \rangle$ is isomorphic to $C_2 \wr C_{13}$ and leaves the same sublattices of L invariant as G. But by (II.2)(ii) the $\mathbb{Z}\bar{G}$-sublattices of L coincide with the ones invariant under the full monomial group $\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})$ ($\cong C_2 \wr S_{13}$). For $G \cong PSL_2(13)$ the sublattices are described in (III.2)(i) and coincide with those of $\mathrm{Aut}_{\mathbb{Z}}(f_{1,13})$. However the remaining two cases yield new lattices; either of the strategies (B1) of (B2) or some theoretical arguments can be applied.

Let $G \leqslant \mathrm{Aut}_{\mathbb{Z}}(f_{3,1})$, $G \cong SL_3(3)$. The $\mathrm{Aut}_{\mathbb{Z}}(f_{3,1})$-sublattices of 3-power index in L are given by 3^iL and $3^jL^{\#}$ for $i \in \mathbb{Z}_{\geqslant 0}$ and $j \in \mathbb{Z}_{\geqslant 1}$. As $\mathbb{Z}/3\mathbb{Z}G$-module $L^{\#}/L$ becomes reducible: $L^{\#}/L = L_1/L \oplus L_2/L$ where L_1 and L_2 are $\mathbb{Z}G$-lattices on which G acts monomially. This explains why $SL_3(3)$ also turns up as a subgroup of $\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})$. All $\mathbb{Z}G$-sublattices with 3-power index in L are given by 3^iL, $3^jL^{\#}$, 3^jL_1, 3^jL_2 with $i \in \mathbb{Z} \geqslant 0$ and $j \in \mathbb{Z} \geqslant 1$. The $\mathbb{Z}G$-sublattices of L_1 with 2-power index in L_1 are the same as under the full monomial group, cf. (III.2)(ii). All other $\mathbb{Z}G$-lattices in $\mathbb{Q}L$ are obtained by taking sums and intersections of multiples of the lattices described so far; they fall into $3 \cdot 4 = 12$ isomorphism classes.

Finally let $G \leqslant \mathrm{Aut}_{\mathbb{Z}}(f_{5,2})$, $G \cong PSL_2(25)$. The Brauer characters of G are well known; in particular L/qL becomes irreducible only for $q = 2$ and $q = 5$, where one has two irreducible constituents in each case. Let L_1 and L_2 be the $\mathbb{Z}G$-sublattices of $L^{\#}$ such that L_1/L and L_2/L are the Sylow 2- resp. 5-subgroup of $L^{\#}/L$. One easily checks that the multiples of L, L_1, L_2, and $L^{\#}$ are the only $\mathbb{Z}G$-sublattices in $\mathbb{Q}L$: That 2^iL and 2^jL_1 for $i \in \mathbb{Z}_{\geqslant 0}$ and $j \in \mathbb{Z}_{\geqslant 1}$ are all $\mathbb{Z}G$-sublattices of 2-power index in L follows by comparing the central characters belonging to the trivial $\mathbb{Q}G$-module and to $\mathbb{Q}L$: they are not congruent mod 8, cf. [Ple 83] (IV.13), or Chapter VII of [Ple 83]. That $5L_2$ is the only proper $\mathbb{Z}G$-sublattice of L not contained in $5L$ follows from (II.4)(ii).

This finishes essentially the proof of the classification of the maximal f.i.u.g. of degree 13. For some of the more interesting lattices also the minimum (square) length ($\neq 0$) denoted by m and the number of vectors of (square) length m are given. For all forms the determinant of the form F_G is given as the product of the elementary divisors of F_G.

(V.2) THEOREM. *There are* 17 *conjugacy classes of maximal* f.i.u.g. *of degree* 13 *falling into* 4 *conjugacy classes under* $GL_{13}(\mathbb{Q})$. *Representatives for the* 17 *classes are given by the* $\mathrm{Aut}_{\mathbb{Z}}(F)$ *with* F *as follows.*

(i) $F = I_{13} = f(1, 0, \ldots, 0)$ ($\det F = 1$), $F = f(2, 0, 1, 0, 0, 0, 0)$ ($\det F = 4$), $F = f(13, -11, 9, -7, 5, -3, 1)$ ($\det F = 4^{12}$) *with* $\mathrm{Aut}_{\mathbb{Z}}(F) \cong C_2 \wr S_{13}$;

(ii) $F=f(13, -1,\ldots, -1)$ ($\det F=14^{12}$), $F=f(2, 1,\ldots, 1)$ ($\det F=14$), $F=f(12, 5, -2, -2, -2, -2, -2)$ ($\det F=7^{11}\cdot 14$), $F=f(7, 5, 3, 1, -1, -3, -5)$ ($\det F=2^{11}\cdot 14$) *with* $\mathrm{Aut}_{\mathbb{Z}}(F)\cong C_2\times S_{14}$;

(iii) $F=f(3, 1, -1, -1, 0, 0, 0)$ ($\det F=3^6$, $m=3$, $a=104$), $F=f(5, 3, 2, 1, -1, -3, -3)$ ($\det F=3^7$, $m=3$, $a=52$), $F=f(4, 2, 1, -1, -1, -1, 0)$ ($\det F=3^5\cdot 12$, $m=4$, $a=468$), $F=f(4, 2, 2, 1, 0, 0, -1)$ ($\det F=3^6\cdot 12$, $m=4$, $a=234$), $F=f(15, -5, -5, 3, -1, 7, -5)$ ($\det F=4^5\cdot 12^7$, $m=12$, $a=52$), $F=f(13, -3, -7, 5, 1, -7, 5)$ ($\det F=4^6\cdot 12^6$, $m=12$, $a=52$) *with* $\mathrm{Aut}_{\mathbb{Z}}(F)\cong C_2\times \widetilde{SL_3(3)}$, *where* $\widetilde{SL_3(3)}$ *denotes* $SL_3(3)$ *extended by its outer automorphism* $(g\mapsto g^{-\mathrm{tr}})$ *of order* 2;

(iv) $F=f(4, -2, 0, 1, 0, -1, 1)$ ($\det F=5^3\cdot 10$, $m=4$, $a=780$), $F=f(13, -7, 1, 1, -1, 3, -1)$ ($\det F=2^3\cdot 10^9$, $m=12$, $a=130$), $F=f(6, 1, 2, 2, -2, 1, -2)$ ($\det F=5^8\cdot 10^8$, $m=6$, $a=130$), $F=f(5, -1, -1, -1, 1, -1, 1)$ ($\det F=2^8\cdot 10^4$, $m=5$, $a=52$) *with* $\mathrm{Aut}_{\mathbb{Z}}(F)\cong C_2\times \widetilde{PSL_2(25)}$, *where* $\widetilde{PSL_2(25)}$ *is* $PSL_2(25)$ *extended by the outer automorphism of order* 2 *induced by the field automorphism.*

Moreover, if $\tilde{F}=f(a_0,\ldots, a_6)\in\mathbb{Z}[z_{13}+z_{13}^{-1}]$ *is positive definite and has the same elementary divisors as a form* F *listed above, then* $\mathrm{Aut}_{\mathbb{Z}}(\tilde{F})$ *is conjugate under* $GL_{13}(\mathbb{Z})$ *to* $\mathrm{Aut}_{\mathbb{Z}}(F)$.

(b) $p=17$.

In this case one can restrict oneself to two possibilities for $\pi_2(f)\,\mathbb{Z}[\zeta+\zeta]$ for the totally positive $f=f(a_0,\ldots, a_8)\in\mathbb{Z}[z_{17}+z_{17}^{-1}]$ satisfying (**) of Section IV with $\mathfrak{a}=\mathbb{Z}[z_{17}]$, namely to $\mathbb{Z}[\zeta+\zeta^{-1}]$ itself, or one fixed prime ideal $\mathfrak{q}_2$ containing 2. By the results of Section III the first possibility leads to $f=I_{18}$ and $f_{1,18}=I_{17}+J_{17}=f(2, 1,\ldots, 1)$ as only forms whose automorphism groups have to be considered. In the case $\pi_2(f)\,\mathbb{Z}[\zeta+\zeta^{-1}]=\mathfrak{q}_2$ a similar discussion as for $p=13$ shows that it suffices to consider $f_{2,3}=f(3, 0, 0, 0, -1, 0, -1, 1, 1)$, $f_{2,5}=f(3, 1, 1, 1, 0, 0, -1, 0, -1)$, and $f_{2,7}=f(3, 0, 1, 0, 0, 0, 0, 0, 1)$. The computer computation with the automorphism program of [PlP 85] shows that only $f_{2,3}$ has an irreducible automorphism group; $\mathrm{Aut}_{\mathbb{Z}}(f_{2,3})$ is isomorphic to $C_2\times\widetilde{SL_2(16)}$, where $\widetilde{SL_2(16)}$ is the extension of $SL_2(16)$ by the field automorphism of order 4.

Proceeding to (B), Section IV, the minimal irreducible subgroups of the automorphism groups of $f_{1,1}$, $f_{1,18}$, and $f_{2,3}$ have to be found. Similarly as in the case $p=13$ one finds a subgroup of order $2^8\cdot 17$ of $\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})$, a subgroup isomorphic to $PSL_2(17)$ of $\mathrm{Aut}_{\mathbb{Z}}(f_{1,18})$, and the commutator subgroup of $\mathrm{Aut}_{\mathbb{Z}}(f_{2,3})$, which is isomorphic to $SL_2(16)$.

Let $G\leqslant\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})$ be the extension of one of the two $\langle z_{17}\rangle$-invariant subgroups of diagonal matrices in $\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})$ of order 2^8 by $\langle z_{17}\rangle$. Then the $\mathbb{Z}G$-sublattices of $L=L_G$ are quickly found by method (B1) of Section IV. Identify L with $\mathbb{Z}[z_{17}]$ and let $\mathfrak{p}$, $\tilde{\mathfrak{p}}$, and $\mathfrak{q}$ be the three ideals of $\mathbb{Z}[z_{17}]$ containing $2\cdot I_{17}$ such that $\mathfrak{q}$ has index 2 and $\mathfrak{p}$ and $\tilde{\mathfrak{p}}$ have index 2^8 in $\mathbb{Z}[z_{17}]$. Then the $\mathbb{Z}G$-sublattices of L correspond to multiples of $\mathbb{Z}[z_{17}]$, $\mathfrak{p}$, $\tilde{\mathfrak{p}}$, $\mathfrak{q}$, $\tilde{\mathfrak{p}}\mathfrak{p}$, $\mathfrak{p}\mathfrak{q}$, $\tilde{\mathfrak{p}}\mathfrak{q}$, and—depending on the choice of G—of $\mathfrak{p}\mathfrak{q}^2$ and $\tilde{\mathfrak{p}}^2$ (resp. of $\tilde{\mathfrak{p}}\mathfrak{q}^2$ and $\tilde{\mathfrak{p}}\mathfrak{p}^2$). The $\mathrm{Aut}_{\mathbb{Z}}(\mathfrak{a}, f_{1,1})$ for these various ideals $\mathfrak{a}$ are all induced by subgroups of $\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})\cong C_2 \wr S_{17}$. To see this, let M be a $\mathbb{Z}G$-sublattice of L. Then one will always find an $\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})$-invariant lattice (cf. (II.2)(ii)) among the sums and intersections of multiples of M and $M^{\#}$. With this in mind one finds that $\mathrm{Aut}(\mathfrak{a}, f_{1,1})$ corresponds to the extension of the group of all diagonal matrices in $\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})$ by a Frobenius group of permutation matrices of order $17\cdot 8$, for $\mathfrak{a}\in\{\mathfrak{p}, \tilde{\mathfrak{p}}, \mathfrak{p}\mathfrak{q}, \tilde{\mathfrak{p}}\mathfrak{q}\}$. Since $(\mathfrak{p}, f_{1,1})$ and $(\tilde{\mathfrak{p}}, f_{1,1})$ as well as $(\mathfrak{p}\mathfrak{q}, f_{1,1})$ and $(\tilde{\mathfrak{p}}\mathfrak{q}, f_{1,1})$ are isometric, cf. (II.3)(ii). Hence one ends up with 2 conjugacy classes of subgroups in this case, and similary in the case $\mathfrak{a}\in\{\mathfrak{p}\mathfrak{q}^2, \mathfrak{p}\tilde{\mathfrak{p}}^2, \tilde{\mathfrak{p}}\mathfrak{q}^2, \tilde{\mathfrak{p}}\mathfrak{p}^2\}$ where the automorphism group corresponds to an extension of group of order 2^9 of diagonal matrices in $\mathrm{Aut}_{\mathbb{Z}}(f_{1,1})$ extended by a Frobenius group of order $17\cdot 8$.

Next let $G\leqslant \mathrm{Aut}_{\mathbb{Z}}(f_{1,18})$ be isomorphic to $PSL_2(17)$. It follows from [Ple 83, Chaps. VII and VIII], that there $4\cdot 3=12$ isomorphism types of sublattices of $L=L_G$. By (III.1) and (III.2)(i) for $2\cdot 3=6$ of these the full automorphism group is isomorphic to $C_2\times S_{18}$. The remaining 6 lattices come in isometric pairs and have an automorphism group isomorphic to $C_2\times PSL_2(17)$ by similar arguments as in the previous case.

Finally let $G\cong SL_2(16)$ be the commutator subgroup of $\mathrm{Aut}_{\mathbb{Z}}(f_{2,3})$. Applying strategy (B1) or (B2) of Section IV, one checks that all $\mathbb{Z}G$-sublattices of $L=L_G$ can be obtained from L, its even sublattice $L'=\{x\in L \mid T_{f_{2,3}}(x, x) \text{ even}\}$, $L^{\#}$, and $L'^{\#}$ by taking sums and intersection of multiples. There are $4\cdot 2=8$ isomorphism types of lattices, no two of which are isometric, and the full automorphism groups of which are all isomorphic to $\mathrm{Aut}(f_{2,3})$. This finishes the proof of the following theorem for which the same notation is used as in (V.3).

(V.4) THEOREM. *There are* 24 *conjugacy classes of maximal* f.i.u.g. *of degree* 17 *falling into* 6 *conjugacy classes under* $GL_{17}(\mathbb{Q})$ (*only four of which consists of maximal finite subgroup of* $GL_{17}(\mathbb{Q})$). *Representatives are given by the* $\mathrm{Aut}_{\mathbb{Z}}(F)$ *with* F *as follows.*

(i) $F=I_{17}=f(1, 0,\ldots, 0)$ $(\det F=1)$, $F=f(2, 0, 1, 0, 0,\ldots, 0)$ $(\det F=4)$, $F=f(17, -15, 13, -11, 9, -7, 5, -3, 1)$ $(\det F=4^{16})$ *with* $\mathrm{Aut}_{\mathbb{Z}}(F)\cong C_2\wr S_{17}$;

(ii) $F=f(17, -1,\ldots, -1)$ $(\det F=18^{16})$, $F=f(2, 1,\ldots, 1)$ $(\det F=18)$, $F=f(16, 7, -2,\ldots, -2)$ $(\det F=9^{15}\cdot 18)$, $F=f(9, 7, 5, 3, 1, -1, -3,$

$-5, -7)$ ($\det F = 2^{15}\cdot 18$), $F = f(4, 3, 2, 1, 0, -1, -2, -2, -2)$ ($\det F = 2$), $F = f(5, 3, 1, -1, -1, \dots, -1)$ ($\det F = 2^{16}$) *with* $\mathrm{Aut}_{\mathbb{Z}}(f) \cong C_2 \times S_{18}$;

(iii) $F = f(5, 1, 2, 0, 1, 0, -2, -2, -2)$ ($\det F = 4^8$, $m = 4$, $a = 34$), $F = f(6, 0, 3, -2, 2, -1, 1, -2, -2)$ ($\det F = 4^9$, $m = 4$, $a = 34$) *where* $\mathrm{Aut}_{\mathbb{Z}}(F)$ *is a split extension of* C_2^{17} *by a Frobenius group of order* $17\cdot 8$.

(iv) $F = f(8, -4, 5, -4, 5, -2, 3, -1, 2)$ ($\det F = 4^8\cdot 16$, $m = 6$, $a = 2176$), $F = f(17, -3, 1, 5, -3, 1, -7, 5, -7)$ ($\det F = 4^8\cdot 16^8$, $m = 16$, $a = 34$), *where* $\mathrm{Aut}_{\mathbb{Z}}(F)$ *is a split extension of* C_2^9 *by a Frobenius group of order* $17\cdot 8$;

(v) $F = f(4, 0, 0, 1, -2, 0, 0, -1, 1)$ ($\det F = 2\cdot 4^8$, $m = 4$, $a = 204$), $F = f(6, 2, -1, 1, 2, 1, -1, -1, 3)$ ($\det F = 2\cdot 4^7\cdot 36$, $m = 6$, $a = 2040$), $F = f(52, 25, 16, 7, -20, -20, -11, -20, -2)$ ($\det F = 9^7\cdot 18\cdot 36^8$, $m = 34$, $a = 36$) *with* $\mathrm{Aut}_{\mathbb{Z}}(F) \cong C_2 \times PSL_2(17)$;

(vi) $F = f(3, 0, 0, 0, -1, 0, -1, 1, 1)$ ($\det F = 2^7\cdot 6$, $m = 3$, $a = 136$), $F = f(4, 0, -1, 1, 2, 1, -1, 1, 1)$ ($\det F = 2^8\cdot 12$, $m = 4$, $a = 1326$), $F = f(4, 1, 1, -1, -1, -2, 0, 1, 2)$ ($\det F = 2^8\cdot 6$, $m = 4$, $a = 2040$), $F = f(7, 1, -3, -1, -1, 1, 3, 1, -3)$ ($\det F = 2^8\cdot 4^7\cdot 12$, $m = 7$, $a = 816$), $F = f(10, -2, -5, 1, 4, 1, -5, 1, 1)$ ($\det F = 3^7\cdot 6^9$, $m = 10$, $a = 1020$), $F = f(17, -1, -1, -1, -7, -1, -7, 5, 5)$ ($\det F = 6^8\cdot 12^8$, $m = 17$, $a = 240$), $F = f(11, 2, 2, -4, -4, -7, -1, 2, 5)$ ($\det F = 3^8\cdot 6^8$, $m = 8$, $a = 102$), $F = f(8, -1, 2, -1, -1, -1, -1, -1, 2)$ ($\det F = 3^7\cdot 6^8\cdot 12$, $m = 8$, $a = 102$) *with* $\mathrm{Aut}_{\mathbb{Z}}(F) \cong C_2 \times \widetilde{SL_2(16)}$, *where* $\widetilde{SL_2(16)}$ *denotes the extension of* $SL_2(16)$ *by the field automorphism group of order* 4.

Moreover, if $F = f(a_0, \dots, a_8) \in \mathbb{Z}[z_{17} + z_{17}^{-1}]$ *is positive definite with elementary divisors equal to those of a form F listed above, then* $\mathrm{Aut}_{\mathbb{Z}}(F)$ *and* $\mathrm{Aut}_{\mathbb{Z}}(F)$ *are conjugate under* $GL_{17}(\mathbb{Z})$.

(c) $p = 19$.

In this case $\pi_2(f)\,\mathbb{Z}[\zeta + \zeta^{-1}]$ for the totally positive $f \in \mathbb{Z}[z_{19} + z_{19}^{-1}]$ satisfying (**) of Section IV can be assumed to be $\mathbb{Z}[\zeta + \zeta^{-1}]$, $\mathfrak{q}_7$ or an integral $\mathbb{Z}[\zeta + \zeta^{-1}]$-ideal divisible by $\mathfrak{q}_{11}$, where $\mathfrak{q}_7$ and $\mathfrak{q}_{11}$ are fixed prime ideals of $\mathbb{Z}[\zeta + \zeta^{-1}]$ containing 7 (resp. 11). Those elements f with $\pi_2(f) \in \mathfrak{q}_{11}$ cannot have an irreducible automorphism group by [Fei 74, Theorem C], or more directly by Feit's theorem (3.1) p. 347, of [Fei 82] as follows: $L_G^{\#}/L_G$ has a $\mathbb{Z}G$-submodule elementary abelian of order 11^6 or 11^7. Hence by (II.1)(iii) and (II.4) a Sylow 11-subgroup $S = \langle y \rangle$ of G has order 11 and y has minimum polynomial of degree $< \frac{1}{3}(2\cdot 11 - 2)$ on a factor, or submodule of $L/11L$, thus contradicting (II.2) and Feit's result just quoted. (Not applying Feit's result leaves 4 more ideal $\pi_2(f)\,\mathbb{Z}[\zeta + \zeta^{-1}]$ to be checked.) The usual arguments show that there are only 4 elements $f \in \mathbb{Z}[z_{19} + z_{19}^{-1}]$, which have to be checked, namely $f = I_{19}$ and $f = I_{19} + J_{19}$

in case $\pi_2(f)$ is a unit in $\mathbb{Z}[\zeta+\zeta^{-1}]$, and $f=f_{7,1}=f(7, 0, -3, 0, 2, -2, -5, 3, 3, -1)$ and $f=F_{7,7}=f(5, 1, 0, -3, -1, 1, 3, 2, 0, -2)$ in case $\pi_2(f)$ generates $\mathfrak{q}_7$. The automorphism program [PlP 85] shows easily that $f_{7,1}$ and $f_{7,7}$ have a reducible automorphism group and the even sublattice of the lattice for $f_{7,7}$ the automorphism groups have an orbit of 19 vectors (and their negatives) of minimum length which are not pairwise orthogonal).

Proceeding to (B) of Section IV, $\mathrm{Aut}_{\mathbb{Z}}(I_{19})$ has only one minimal irreducible subgroup up to conjugacy, namely, the subgroup of index 2 of the extension of the group of all diagonal matrices in $\mathrm{Aut}_{\mathbb{Z}}(I_{19})$ by $\langle z_{19}\rangle$. As in the case $p=13$ one sees by means of (III.2)(ii) that this group does not have more invariant sublattices of $L=\mathbb{Z}^{19\times 1}$ than $\mathrm{Aut}_{\mathbb{Z}}(I_{19})$ itself. Finally $\mathrm{Aut}_{\mathbb{Z}}(I_{19}+J_{19})$ has only a group isomorphic to $PSL_2(19)$ as minimal irreducible subgroup. By (III.2)(i) one concludes that this group does not have any other invariant lattices in $L=\mathbb{Z}^{19\times 1}$ than $\mathrm{Aut}_{\mathbb{Z}}(I_{19}+J_{19})$ itself. This proves that one has a situation in dimension 19 as in prime dimensions less equal to 11, namely that all maximal f.i.u.g. are essentially reflection groups. The Gram matrices can be taken from (III.4).

(V.5) THEOREM. *There are* $3+\sigma_0(20)=9$ *conjugacy classes of maximal* f.i.u.g. *of degree* 19 *falling into two conjugacy classes under* $GL_{19}(\mathbb{Q})$. *The groups in the first three classes are isomorphic to* $C_2 \wr S_{19}$ *and the others are isomorphic to* $C_2\times S_{20}$.

VI. DIMENSION $p=23$

In [Fei 74, Theorem E], Feit proved that a f.i.u.g. of degree 23 has a subgroup of index 23 or 24 or is embedable in $C_2\times Co.2$ or $C_2\times Co.3$, where $Co.2$ and $Co.3$ are the Conway groups turning up as stabilizers in the automorphism group of the Leech lattice of a vector of norm 4 resp. 6, cf. [Con 69]. This result will not be applied, but follows from the subsequent discussion along the lines of Section IV. Similarly as in [Fei 74] no automorphism computations are necessary since sufficiently many lattices of dimension 23 are known.

The class number of $\mathbb{Q}(\zeta)$ is three; the nonprincipal ideal classes are represented by the two prime ideals of $\mathbb{Z}[\zeta+\zeta^{-1}]$ which contain 2. Hence by (II.3) one may assume $\mathfrak{a}=\mathbb{Z}[z_{23}]$ or $\mathfrak{a}=\mathfrak{a}_2$, where $\mathfrak{a}_2$ is one fixed ideal of $\mathbb{Z}[z_{23}]$ of index 2^{11} in $\mathbb{Z}[z_{23}]$.

In the case $\mathfrak{a}=\mathbb{Z}[z_{23}]$ the totally positive $f\in\mathbb{Q}[z_{23}+z_{23}^{-1}]$ satisfying (**) of Section IV can be chosen to be $f=I_{23}$ or $f=I_{23}+J_{23}$ by the results of Section III. Since the transitive permutation groups of degree 23 are well known, cf., e.g., [Neu 77], and the 2-transitive permutation groups of degree 24 are easily derived from those, one only finds an extension of a group of order 2^{11} of diagonal matrices in $\mathrm{Aut}_{\mathbb{Z}}(I_{23})$ extended by $\langle z_{23} \rangle$ as minimal irreducible subgroup of $\mathrm{Aut}_{\mathbb{Z}}(I_{23})$ and a group isomorphic to $PSL_2(23)$ as minimal irreducible subgroup of $\mathrm{Aut}_{\mathbb{Z}}(I_{23}+J_{23})$, cf. also (II.2).

Next let $\mathfrak{a}=\mathfrak{a}_2$. Then $f \in \mathbb{Q}[z_{23}+z_{23}^{-1}]$ satisfying (**) of Section IV has the property $\pi_2(f)\,\mathbb{Z}[\zeta+\zeta^{-1}]=\frac{1}{2}\mathbb{Z}[\zeta+\zeta^{-1}]$, because each prime number q, $2 \leqslant q < 23$, generates a prime ideal in $\mathbb{Z}[\zeta+\zeta^{-1}]$. One finds the relevant elements $f \in \mathbb{Q}[z_{23}+z_{23}^{-1}]$ by applying (IV.2), (IV.3) (note $m(f, \mathfrak{a})=4$), and (IV.4), namely (in the terminology of (IV.2)): $f_2=\frac{1}{2}\Xi_2^2$, $f_1=\frac{1}{2}(\Xi_5^2-J_{23})$, $f_6=\frac{1}{2}(\Xi_9^2-3J_{23})$, and $f_3=\frac{1}{2}(\Xi_{11}^2-5J_{23})$, as well as a few other elements f, which can be ruled out by applying (IV.3)(ii) to the even sublattice of $(\mathfrak{a}, f)$. The automorphism group of $(\mathfrak{a}_2, f_2)$ is isomorphic to $C_2 \wr M_{23}$. This can be seen from the fact that the Mathieu group M_{23} is the automorphism group of the Golay code of length 23, cf. [MaS 77], that $(\mathfrak{a}_2, f_2)$ is isometric to $(\mathfrak{a}'_2, \frac{1}{2}I_{23})$, where $\mathfrak{a}'_2$ is the $\mathbb{Z}C_{23}$-ideal of index 2 in $\mathfrak{a}_2$, cf. also (III.1). $\mathrm{Aut}(\mathfrak{a}_2, f_1)$ is isomorphic to $C_2 \times Co.2$, because the even sublattice of $(\mathfrak{a}_2, f_1)$ is isometric to the lattice of all vectors in the Leech lattice which are orthogonal to a fixed vector of norm 4 cf. [Con 69]. Similarly $\mathrm{Aut}(\mathfrak{a}_2, f_6)$ is isomorphic to $C_2 \times Co.3$, since $(\mathfrak{a}_2, f_6)$ is isometric to the lattice of all vectors orthogonal to a fixed vector of norm 6 in the Leech lattice. Finally a similar argument or a direct reference to the Golay Code of length 24 proves that $\mathrm{Aut}(\mathfrak{a}_2, f_3)$ is isomorphic to $C_2 \times M_{24}$. (Note, at this stage Feit's result quoted at the beginning of this section follows already.) The minimal irreducible subgroups of the $\mathrm{Aut}(\mathfrak{a}_2, f_i)$ are isomorphic to an extension of C_2^{11} by C_{23} for $i=2$, to $Co.2$ (resp. $Co.3$) for $i=1$ (resp. $i=6$), and to $PSL_2(23)$ for $i=3$.

The first of the four minimal irreducible groups the lattices of which have to be discussed according to B of Section IV is $G \cong C_2^{11} \cdot C_{23}$ acting monomially of $L=\mathbb{Z}^{23\times 1}$. Identify L with $\mathbb{Z}[z_{23}]$, and let $\mathfrak{p}$, $\tilde{\mathfrak{p}}$, and $\mathfrak{q}$ be the three prime ideals of $\mathbb{Z}[z_{23}]$ containing $2 \cdot I_{23}$ which are of index 2^{11}, 2^{11} (resp. 2) in $\mathbb{Z}[z_{23}]$. The $\mathbb{Z}G$-sublattices of L correspond to multiples of $\mathbb{Z}[z_{23}]$, $\mathfrak{p}$, $\tilde{\mathfrak{p}}$, $\mathfrak{q}$, $\mathfrak{p}\mathfrak{q}$, $\tilde{\mathfrak{p}}\mathfrak{q}$, $\mathfrak{p}\tilde{\mathfrak{p}}$, and—depending on the choice of G—of $\mathfrak{p}\mathfrak{q}^2$, $\mathfrak{p}^2\tilde{\mathfrak{p}}$ or $\tilde{\mathfrak{p}}\mathfrak{q}^2$, $\mathfrak{p}\tilde{\mathfrak{p}}^2$. Using the automorphism of $\mathbb{Z}[z_{23}]$ which interchanges $\mathfrak{p}$ and $\tilde{\mathfrak{p}}$, cf. (II.3), and omitting the principal $\mathbb{Z}[z_{23}]$-ideals, because of (III.8), one has to find the automorphism groups of $(\mathfrak{p}, I_{23})$, $(\mathfrak{p}\mathfrak{q}, \frac{1}{2}I_{23})$, $(\mathfrak{p}\mathfrak{q}^2, \frac{1}{2}I_{23})$, $(\mathfrak{p}^2\tilde{\mathfrak{p}}, I_{23})$. As noted earlier, $\mathrm{Aut}(\mathfrak{p}\mathfrak{q}, \frac{1}{2}I_{23}) \cong C_2 \wr M_{23}$. Since $(\mathfrak{p}, I_{23})$ is dual to a scaled version of $(\mathfrak{p}\mathfrak{q}, \frac{1}{2}I_{23})$ one also gets $\mathrm{Aut}(\mathfrak{p}, I_{23}) \cong C_2 \wr M_{23}$. The other two lattices are also dual to multiples of each other and hence have $GL_{23}(\mathbb{Q})$-conjugate automorphism groups. One easily checks that $\mathrm{Aut}(\mathfrak{p}\mathfrak{q}^2, \frac{1}{2}I_{23})$ is isomorphic to a subgroup of $C_2 \wr M_{23}$, namely to a split extension of C_2^{12} with M_{23}.

Next let $G \leqslant \mathrm{Aut}_{\mathbb{Z}}(I_{23}+J_{23})$ be isomorphic to $PSL_2(23)$. The sublattices of $L=L_G$ are determined in [Ple 83, Chaps. VII and VIII]. They fall into

$10 \cdot 2 = 20$ isomorphism classes $4 \cdot 2 = 8$ of which also admit the operation of $\mathrm{Aut}_{\mathbb{Z}}(I_{23} + J_{23})$ by (III.2)(i). The remaining 12 types come in 6 isometric pairs. The remaining 6 lattices have automorphism groups conjugate under $GL_{23}(\mathbb{Q})$, since each of the lattices can be obtained from the others by taking intersections and sums of multiples of one arbitrarily given lattice, its even sublattice, their dual lattices etc. Since one of the lattices (with discriminant 3) was seen to have $C_2 \times M_{24}$ as isomorphism type of its automorphism group, the same holds for all six of them.

For the discussion of the *Co*.2- and *Co*.3-lattices the following notion is helpful.

(VI.1) DEFINITION. Let G be a finite group. The $\mathbb{Z}G$-lattice L is called monomially generated, if there is an $x \in L$ with $L = \mathbb{Z}Gx$ such that the induced lattice $\mathbb{Z}G \otimes_{\mathbb{Z}H} \mathbb{Z}x$ has no epimorphic image of $\mathbb{Z}$-rank 1, where $H = \{g \in G \mid gx = \pm x\}$.

(VI.2) PROPOSITION. *Assume* $[G : G'] \leqslant 2$. *A monomially generated* $\mathbb{Z}G$-*lattice L has at most one* $\mathbb{Z}G$-*sublattice* $L' \neq L$ *with* L/L' *cyclic (as abelian group). If* L' *exists, one has* $[L : L'] = 2$.

Proof. In the terminology of (IV.1) one has a $\mathbb{Z}G$-epimorphism φ of $M := \mathbb{Z}G \otimes_{\mathbb{Z}H} \mathbb{Z}x$ onto L which maps $1 \otimes x$ onto x. Let $L' \leqslant_{\mathbb{Z}G} L$ with L/L' cyclic of order bigger than 2. Then there is a unique 1-dimensional $\mathbb{Z}G$-lattice X having L/L' as epimorphic image. The composition of φ with the natural epimorphism $L \to L/L'$ factors over X, since G acts monomially on M. But M does not have a 1-dimensional lattice as epimorphic image, hence $[L : L'] \leqslant 2$. If $L' \leqslant_{\mathbb{Z}G} L$ with $[L : L'] = 2$, then clearly L' is the only sublattice with this property, since L is generated (as $\mathbb{Z}G$-lattice) by a single element. Q.E.D.

Let $G \leqslant \mathrm{Aut}(\mathfrak{a}_2, f_1)$ be isomorphic to *Co*.2. Then $L = \mathfrak{a}_2$ contains $2 \cdot 2300$ vectors of minimum norm 3, cf. [PlP 85]. This together with the character table of *Co*.2 shows that L is monomially generated, namely 2300 is the minimal degree of a nontrivial permutation representation of G and the irreducible character of degree 23 is not contained in the permutation character. Proposition (VI.2) implies that the even sublattice L' of L is the only sublattice of L with cyclic factor group ($\neq 1$). By restricting the operation of G to a Sylow 5-subgroup and to a Sylow 23-subgroup one sees that L/qL is either irreducible as $\mathbb{Z}/q\mathbb{Z}G$-module or has a 1- and a 22-dimensional constituent for any prime number q dividing $|G|$. Using the selfduality of L, one obtains now that the multiples of L, L', and $L'^{\#}$ are the only $\mathbb{Z}G$-sublattices of L.

Let $G \leqslant \mathrm{Aut}(\mathfrak{a}_2, f_6)$ be isomorphic to *Co*.3. Then $L = \mathfrak{a}_2$ is contained in a $\mathbb{Z}G$-lattice L' with index 2, since $L^{\#}/L \cong C_6$. Computing the vectors of minimum length of L' yield $2 \cdot 276$ vectors of norm $\frac{5}{2}$. The same argument as in the $Co.2$-case yields that L' is monomially generated and that the $\mathbb{Z}G$-sublattices of L are all multiples of L, L', $L^{\#}$, and L'. This finishes the proof of the final result.

(VI.3) THEOREM. *There are* 28 *conjugacy classes of* f.i.u.g. *of degree* 23 *falling into* 7 *conjugacy classes under* $GL_{23}(\mathbb{Q})$ (*only* 4 *of which consist of maximal finite subgroups of* $GL_{23}(\mathbb{Q})$). *The* 28 *classes can be characterized by two invariants: the elementary divisors of the Gram matrix* F_G *of some group* G *in the class and the minimum number of generators of the* $\mathbb{Z}P$-*lattice* L_P, *where* L *is the natural* $\mathbb{Z}G$-*lattice and* P *a Sylow* 23-*subgroup of* G. *In case* L_P *is generated by one element, the possible elementary divisors are*

(i) $1^{22} \cdot 24$, $1 \cdot 24^{22}$, $1^{22} \cdot 6$, $1 \cdot 6^{22}$, $1 \cdot 2^{21} \cdot 6$, $1 \cdot 3^{21} \cdot 6$, $1 \cdot 8^{21} \cdot 24$, $1 \cdot 3^{21} \cdot 24$ *with* $G \cong C_2 \times S_{24}$,

(ii) 1^{23}, $1^{22} \cdot 4$, $1 \cdot 4^{22}$ *with* $G \cong C_2 \wr S_{23}$,

and in case L_P *is not generated by one element, the elementary divisors are*

(iii) $1^{22} \cdot 2$, $1 \cdot 2^{22}$ *with* $G \cong C_2 \wr M_{23}$,

(iv) $1^{22} \cdot 8$, $1 \cdot 8^{22}$ *where* G *is a split extension of* C_2^{12} *by* M_{23},

(v) $1^{22} \cdot 3$, $1 \cdot 3^{22}$, $1^{22} \cdot 12$, $1 \cdot 12^{22}$, $1 \cdot 4^{21} \cdot 12$, $1 \cdot 3^{21} \cdot 12$ *with* $G \cong C_2 \times M_{24}$,

(vi) 1^{23}, $1^{22} \cdot 4$, $1 \cdot 4^{22}$ *with* $G \cong C_2 \times Co.2$,

(vii) $1^{22} \cdot 6$, $1 \cdot 6^{22}$, $1 \cdot 2^{21} \cdot 6$, $1 \cdot 3^{21} \cdot 6$ *with* $G \cong C_2 \times Co.3$.

Conversely, if F *is the Gram matrix of a positive definite integral bilinear form of degree* 23 *with elementary divisors as above*, $23 \mid \mathrm{Aut}(F)$ *and* L_P *indecomposable as* $\mathbb{Z}P$-*lattice, where* $P \leqslant \mathrm{Aut}_{\mathbb{Z}}(F)$, $|P| = 23$ *and* L *the natural* $\mathrm{Aut}_{\mathbb{Z}}(F)$-*lattice, then* $\mathrm{Aut}_{\mathbb{Z}}(F)$ *is a* f.i.u.g. *of degree* 23.

REFERENCES

[Ban 73] EI. BANNAI AND ET. BANNAI, On some finite subgroups of $GL(n, \mathbb{Q})$, *J. Fac. Sci. Univ. Tokyo, Sect. IA* **20**, (3) (1973), 319–340.

[Bur 12] W. BURNSIDE, The determination of all groups of rational linear substitutions of finite order which contain the symmetric group in the variables, *Proc. London Math. Soc. (2)* **10** (1912), 284–308.

[Can 74] J. CANNON, A general purpose group theory program, *in* "Proc. Sec. Internat. Conf. Theory of Groups," Canberra 1973, pp. 204–217, Lecture Notes in Math., Vol. 372, Springer-Verlag, Berlin/New York, 1974.

[Con 69] J. H. CONWAY, A Group of Order 8, 315, 553, 086, 720, 000, Bull. London Math. Soc. **1** (1969), 79–88.

[Cox 51] H. S. M. COXETER, Extreme forms, *Canad. J. Math.* **3** (1951), 391–441.

[CuR 62] C. W. CURTIS AND I. REINER, "Representation Theory of Finite Groups and Associate Algebras," Interscience, New York, 1962.

[Dav 78] D. Davis, Computing the number of totally positive circular units which are squares, *J. Number Theory* **10** (1978), 1-9.

[Fei 74] W. Feit, On integral representations of finite groups, *Proc. London Math. Soc. (3)* **29** (1974), 633-683.

[Fei 82] W. Feit, "The Representation Theory of Finite Groups," North-Holland, Amsterdam/New York, 1982.

[Hum 72] J. E. Humphreys, "Introduction to Lie Algebras and Representation Theory," Springer-Verlag, New York/Heidelberg/Berlin, 1972.

[Kne 54] M. Kneser, Zur Theorie der Kristallgitter, *Math. Ann.* **127** (1954), 105-106.

[MaS 77] MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.

[Min 11] H. Minkowski, "Gesammelte Abhandlungen," Teubner, Leipzig, 1911.

[New 72] M. Newman, "Integral Matrices," Academic Press, New York,/London, 1972.

[NeT 56] M. Newman and O. Taussky, Classes of positive definite unimodular circulants, *Canad. J. Math.* **9** (1956), 71-73.

[Neu 77] P. M. Neumann, "Permutationsgruppen von Primzahlgrad und verwandte Themen," Vorlesungen aus d. Math. Instit. Giessen, Heft 5, 1977.

[Ple 77] W. Plesken, On absolutely irreducible representations of orders, *in* "Number Theory and Algebra" pp. 241-262 (H. Zassenhaus, Ed.), Academic Press, New York/London, 1977.

[Ple 78] W. Plesken, On reducible and decomposable representations of orders, *J. Reine Angew. Math.* **297** (1978), 188-210.

[Ple 80] W. Plesken, "Gruppenringe über lokalen Dedekindbereichen," Habilitationsschrift, Aachen, 1980.

[Ple 83] W. Plesken, "Group Rings of Finite Groups over p-adic Integers," Springer Lecture Notes in Math., Vol. 1026, Berlin/Heidelberg/New York, 1983.

[PlP 77, 80] W. Plesken and M. Pohst, On maximal finite irreducible subgroups of $GL(n, \mathbb{Z})$. I. The five- and seven-dimensional case. II. The six-dimensional case, *Math. Comp.* **31** (138) (1977), 536-577; III. The nine-dimensional case. IV. Remarks on even dimensions with applications to $n=8$. V. The eight-dimensional case and a complete description of dimensions less than ten, *Math. Comp.* **34** (149) (1980), 245-301.

[PlP 85] W. Plesken and M. Pohst, Constructing integral lattices with prescribed minimum I, *Math. Comp.*, in press.

[Reu 75] C. G. Reuschle, "Tafeln complexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind," Berlin, 1875.

[Sim 70] C. Sims, Computational methods in the study of permutation groups, *in* "Computational Problems in Abstract Algebra," pp. 169-187 (J. Leech, Ed.), Pergamon, Oxford/New York, 1980.

[Was 80] L. C. Washington, "Introduction to Cyclotomic Fields," Springer-Verlag, New York/Heidelberg/Berlin, 1980.

[Wit 41] E. Witt, Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe, *Math. Sem. Univ. Hamburg* **14** (1941), 289-322.

Printed in Belgium