THE MAXIMAL FINITE GROUPS OF 4 × 4 INTEGRAL MATRICES

BY

E. C. DADE

There are nine of them, to within equivalence. The list will be found in Theorem 4.27 below. The rest of the paper is a proof of that theorem.

This is not exactly the list of integral groups which people really need. However, the techniques used here can probably be extended to handle more interesting problems.

A person interested in space groups needs a list of *all* finite groups of integral matrices, not just the maximal ones. It might be possible to satisfy him by listing all subgroups of the nine groups below, and then checking for equivalences (which would be the hard part). But the number of groups to be handled should be in the hundreds. This seems to be a job for computers.

A person interested in quadratic forms needs a list of all possible groups of automorphs of positive definite forms. This is a more reasonable request. The methods of this paper could easily be modified to obtain such a list. It would only be necessary to reconsider the eight cases thrown out by Lemma 3.10, and to avoid condition (1.4b) by using successive minima.

Could our techniques be extended to degrees larger than 4? Possibly they can. The inequalities to be satisfied by Hermite-reduced forms have been worked out in detail for degrees 5 and 6 (see [1] and [2]). From these it should be possible to obtain axiomatic descriptions of the sets $S(\phi, L)$ similar to those in Theorem 1.14. Then these subsets might be classified. Of course, no simple description by means of graphs (as used here) would suffice. But this is merely a notational convenience. Our subsets could have been described directly in terms of basis elements, as in (2.16). The computational problems would increase greatly with the degree, but the method might be worth considering.

The purpose of Sections 1, 2 and 3 is to obtain a short list of groups which contains every maximal group at least once. Instead of trying to list groups directly, we classify those sets S of non-zero integral points which have minimum "distance" from the origin with respect to some positive definite quadratic form. In Section 1, we show that the sets S are adequate for a description of our groups (Lemma 1.2) and find an axiomatic description for almost all of them (Theorem 1.14). Almost all the sets satisfying these axioms can be described by means of certain graphs (Theorem 2.21). Section 2 explains how this is done. Finally, we list the relevant graphs in Section 3 (see Figure 3.4) and remove some which obviously do not lead to maximal groups (Lemma 3.10).

Received October 4, 1963.

The result of the first three sections is a list of eight graphs and two "exceptional" sets S. In Section 4, we examine in turn each of these ten cases, showing that nine of them lead to inequivalent maximal groups, while the tenth doesn't.

Throughout the paper V is a fixed real vector space of dimension 4 and L is a fixed lattice (of integral points) in V. All the groups mentioned in Sections 1, 2, and 3 are finite groups of linear transformations of V carrying L into itself (integral transformations). In Section 4 it is necessary to relax this definition somewhat to include finite groups of linear transformations of arbitrary real vector spaces. It should be clear from the context what vector spaces are operated on by what groups.

I wish to thank Professor H. Zassenhaus both for suggesting this problem and for many enlightening remarks in the course of the work.

1. The use of quadratic forms

The orbit of any element of L under the action of one of our groups G must be finite. By taking, e.g., the union of the orbits of some basis elements of L, we see that G must leave invariant at least one finite subset S of L which spans V. On the other hand, if S is any such subset, then the group $G(S, L)$ of all linear transformations of V which map both S and L onto themselves is finite. (The permutation representation of $G(S, L)$ on S is faithful since S spans V.) We conclude immediately that

(1.1) *the group G is maximal if and only if $G = G(S, L)$ for all finite subsets S of L which span V and are invariant under G.*

Our problem is to pick out from the infinite family of subsets of L satisfying the conditions of (1.1) some distinguished representatives which we can classify. To do so, we recall that G must leave invariant a positive definite (real) quadratic form ϕ on V. There is a certain positive minimum $r(\phi, L)$ among the (squared) "lengths" $\phi(l)$, where $l \in L$, $l \neq 0$. And only a finite set $S(\phi, L)$ of elements $l \in L$ attain this minimum. The set $S(\phi, L)$ is certainly invariant under G. Our first important observation is that ϕ can be chosen so that $S(\phi, L)$ spans V.

LEMMA 1.2. *For any group G, there is at least one positive definite quadratic form ϕ on V which is invariant under G and for which $S(\phi, L)$ spans V.*

Proof. If the lemma is false for some group G, choose a positive definite quadratic form ϕ on V such that the subspace V_1 spanned by $S(\phi, L)$ has the largest possible dimension. Then V is the direct sum $V_1 \dot{+} V_2$ of V_1 and the subspace $V_2 \neq 0$ perpendicular to V_1 under ϕ. Of course, V_2 is also invariant under G.

We denote by π_i the projection of V onto V_i, for $i = 1, 2$. Each of the quadratic forms ϕ_t, $t > 0$, defined by

$$\phi_t(v) = \phi(\pi_1(v)) + t\phi(\pi_2(v)) \quad \text{for} \quad v \in V,$$

is positive definite and invariant under G. We shall show that, for a suitable $t > 0$, $S(\phi_t, L)$ spans a subspace properly containing V_1.

Let $r = r(\phi, L)$. Then, for any $t > 0$, the hyperellipsoid $H_t : \phi_t(v) \leq r$, must contain $S(\phi, L)$. If $l \neq 0$ is any other point of $H_t \cap L$, then $l \notin V_1$, so that $r \geq \phi_t(l) > \phi(\pi_1(l))$. Conversely, if $l \in L - \{0\}$ and $\phi(\pi_1(l)) < r$, then $l \notin V_1$, and $l \in H_t$ if and only if $t \leqq [r - \phi(\pi_1(l))]/\phi(\pi_2(l))$.

If $V_2 \cap L \neq 0$, then any $l \in V_2 \cap L - \{0\}$ satisfies $\phi(\pi_1(l)) = 0 < r$. On the other hand, if $V_2 \cap L = 0$, then π_1 is an isomorphism of L into V_1. So $\pi_1(L)$ is not a discrete subgroup of V_1. Therefore some element $l \in L$ must satisfy $0 < \phi(\pi_1(l)) < r$. In either case we conclude from the paragraph above that

(1.3) *for sufficiently small* $t > 0$, H_t *contains some points of* L *which are not in* V_1.

Let $t > 0$ satisfy (1.3), and let $T \geq t$ be the maximum of the real numbers $[r - \phi(\pi_1(l))]/\phi(\pi_2(l))$, where l runs over the finite set $H_t \cap L - V_1$. Since $\phi_t(v)$ increases monotonically with t (for fixed $v \in V$), the set $H_T \cap L - \{0\}$ consists precisely of $S(\phi, L)$ and of those $l \in H_t \cap L - V_1$ for which $[r - \phi(\pi_1(l))]/\phi(\pi_2(l)) = T$. Furthermore, each of the latter elements l satisfies $\phi_T(l) = r$. It follows that $r(\phi_T, L) = r$, and that $S(\phi_T, L) = H_T \cap L - \{0\}$ spans a space properly containing V_1. This, of course, contradicts the maximality of V_1, and proves the lemma.

We now restrict our attention to those finite subsets S of L satisfying

(1.4a) $S = S(\phi, L)$, *for some positive definite quadratic form* ϕ *on* V,
(1.4b) S *spans* V.

By the preceding discussion, we know that every maximal group must be of the form $G(S, L)$ for some S satisfying (1.4). We shall classify these sets S, and, hence, the maximal groups G.

To find the combinatorial properties of the above sets which enable us to classify them, we turn to a paper by Minkowski [3]. A basis $l_1, \cdots, l_4$ of L is *reduced* (with respect to ϕ) if the vector $(\phi(l_1), \cdots, \phi(l_4))$ is minimal in the lexicographical ordering of all such vectors attached to all possible bases of L. In our case an alternative definition is given by

LEMMA 1.5. *If* $S(\phi, L)$ *satisfies* (1.4), *then a basis* $l_1, \cdots, l_4$ *of* L *is reduced if and only if each* l_i *lies in* $S(\phi, L)$.

Proof. If $l_1, \cdots, l_4 \in S(\phi, L)$, then

$$(\phi(l_1), \cdots, \phi(l_4)) = (r(\phi, L), \cdots, r(\phi, L))$$

is obviously minimal. So $l_1, \cdots, l_4$ is reduced.

Conversely, let $l_1, \cdots, l_4$ be a reduced basis of L. Let $\phi(l_j) > r(\phi, L)$ for some $j = 1, \cdots, 4$. Since $S(\phi, L)$ spans L, some element

$$l = m_1 l_1 + \cdots + m_4 l_4$$

of $S(\phi, L)$ must satisfy $m_j > 0$. By inequality (m) of [3], this implies that

$$r(\phi, L) = \phi(l) \geq \phi(l_j) > r(\phi, L),$$

a contradiction. So $l_1, \cdots, l_4 \in S(\phi, L)$.

COROLLARY 1.6. *If S satisfies* (1.4), *it must contain at least one basis of L.*

The following lemma is our main application of Minkowski's theory:

LEMMA 1.7. *Let ϕ satisfy* (1.4) *with $r(\phi, L) = 1$. Let $l_1, \cdots, l_4$ be a reduced basis for L. If any element $l = m_1 l_1 + \cdots + m_4 l_4$ of $S(\phi, L)$ satisfies $| m_i | > 1$, for some $i = 1, \cdots, 4$, then, with respect to a suitable choice of $l_1, \cdots, l_4$, the form ϕ is given by*

$$\phi(X_1 l_1 + \cdots + X_4 l_4) = X_1^2 + X_2^2 + X_3^2 + X_4^2 - (X_1 + X_2 + X_3)X_4. \tag{1.8}$$

Proof. Assume the element $l \in S(\phi, L)$ is chosen to minimize $\sum_i | m_i |$ among all those for which some $| m_j |$ is > 1. By changing the signs of the l_i and permuting them, we may assume that

$$0 \leq m_1 \leq m_2 \leq m_3 \leq m_4 \quad \textit{and} \quad m_4 \geq 2. \tag{1.9}$$

Let α_{ij} be the real numbers such that $\alpha_{ij} = \alpha_{ji}$, for $i, j = 1, \cdots, 4$, and $\phi(X_1 l_1 + \cdots + X_4 l_4) = \sum_{i,j=1}^{4} \alpha_{ij} X_i X_j$. By Lemma 1.5, $\alpha_{11} = \cdots = \alpha_{44} = 1$.

Define $k = 1, \cdots, 4$ by $m_1 = \cdots = m_{k-1} = 0 < m_k$. We consider separately the possible values of k.

$k = 4$. In this case $l = m_4 l_4$. So $1 = \phi(l) = m_4^2 \alpha_{44} = m_4^2$, contradicting (1.9).

In all the other cases notice that

$$1 = \phi(l) = \phi(l - m_k(l_{k+1} + \cdots + l_4)) + m_k^2 [\phi(l_k + \cdots + l_4) - 1] + 2m_k \textstyle\sum_{j=k+1}^{4} [(m_j - m_k)(\alpha_{j,k+1} + \cdots + \alpha_{j,4})].$$

As noted in [3], each term in brackets $[\cdots]$ is non-negative. Since $l - m_k(l_{k+1} + \cdots + l_4) \neq 0$, all these terms must be zero, and

$$l - m_k(l_{k+1} + \cdots + l_4) \in S(\phi, L).$$

Hence

$$\phi(l_k + \cdots + l_4) = 1, \tag{1.10a}$$

$$(m_j - m_k)(\alpha_{j,k+1} + \cdots + \alpha_{j,4}) = 0 \quad \textit{for} \quad j = k + 1, \cdots, 4, \tag{1.10b}$$

$$m_k l_k + (m_{k+1} - m_k)l_{k+1} + \cdots + (m_4 - m_k)l_4 \in S(\phi, L). \tag{1.10c}$$

Since $k < 4$, $m_k + (m_{k+1} - m_k) + \cdots + (m_4 - m_k) < m_k + \cdots + m_4$.

By the minimality of the latter sum, we conclude that $m_k = 1$ and $m_j - m_k \leq 1$, for $j = k + 1, \cdots, 4$. Hence $m_4 = 2$.

We return to the separate cases of k.

$k = 3$. By (1.10b) with $j = 4$, $\alpha_{44} = 0$, a contradiction.

$k = 2$. By (1.10b) with $j = 4$, $\alpha_{34} + \alpha_{44} = 0$. The inequality (α) of [3] implies $| \alpha_{34} | \leq \frac{1}{2}$. But $\alpha_{44} = 1$. This is a contradiction.

$k = 1$. By (1.10b) with $j = 4$, $\alpha_{24} + \alpha_{34} + \alpha_{44} = 0$. Using inequality (α) of [3], we conclude that

$$\alpha_{24} = \alpha_{34} = -\tfrac{1}{2} \tag{1.11}$$

Since $1 \leq m_3 \leq 2$, there are only two possible values for m_3 :

$m_3 = 2$. Interchange l_3 and l_4. The equalities corresponding to (1.11) are $\alpha_{23} = \alpha_{43} = -\frac{1}{2}$. But this and (1.11) imply

$$\phi(l_2 + l_3 + l_4) = 3 + 2(\alpha_{23} + \alpha_{24} + \alpha_{34}) = 0,$$

a contradiction.

$m_3 = 1$. Then, by (1.9), $m_1 = m_2 = m_3 = 1$, $m_4 = 2$. By permuting l_1, l_2, l_3, we conclude from (1.11) that $\alpha_{14} = \alpha_{24} = \alpha_{34} = -\frac{1}{2}$. Equation (1.10a) is now

$$4 + 2(\alpha_{12} + \alpha_{13} + \alpha_{14} + \alpha_{23} + \alpha_{24} + \alpha_{34}) = 1,$$

or

$$\alpha_{12} + \alpha_{13} + \alpha_{23} = 0. \tag{1.12}$$

Since $l_1 + l_2 + l_4 \neq 0$, we must have

$$1 = r(\phi, L) \leq \phi(l_1 + l_2 + l_4) = 3 + 2(\alpha_{12} + \alpha_{14} + \alpha_{24}) = 1 + 2\alpha_{12}.$$

Hence

$$\alpha_{12} \geq 0.$$

Similarly

$$\alpha_{13}, \alpha_{23} \geq 0.$$

This, and (1.12), imply that

$$\alpha_{12} = \alpha_{13} = \alpha_{23} = 0.$$

Therefore ϕ is given by (1.8).

At last we reach the desired combinatorial property of the sets in (1.4):

PROPOSITION 1.13. *If the form ϕ of (1.4) is not equivalent to a multiple of the form (1.8), then any four independent elements of $S(\phi, L)$ form a basis for L.*

Proof. Let $l_1, \cdots, l_4$ be a reduced basis of L, and let $u_1, \cdots, u_4$ be four independent elements of $S(\phi, L)$. Arrange the l's and u's so that, for each $i = 1, \cdots, 4$, the elements $l_1, \cdots, l_{i-1}, u_i, \cdots, u_4$ are independent.

If $l_1, \cdots, l_{i-1}, u_i, \cdots, u_4$ is a basis for L, it is reduced by Lemma 1.5. Furthermore $u_{i-1} = \cdots + m_{i-1} l_{i-1} + m_i u_i + \cdots$, where $| m_{i-1} | \leq 1$, by the preceding lemma. If $m_{i-1} = 0$, then $l_1, \cdots, l_{i-2}, u_{i-1}, u_i, \cdots, u_4$ are dependent, a contradiction. Hence $m_{i-1} = \pm 1$, and $l_1, \cdots, l_{i-2}, u_{i-1}, \cdots, u_4$ form a basis of L. By induction, $u_1, \cdots, u_4$ are a basis of L.

We sum up the results of this section in

Theorem 1.14. *Any maximal group is of the form* $G(S, L)$, *where* S *satisfies*

(a) $S = S(\phi, L)$, *where the form* ϕ *is given by* (1.8) *with respect to some basis of* L,

or (b)

$$(1.15) \quad \begin{cases} S = -S, \\ 0 \notin S, \\ \text{any four independent elements of } S \text{ form a basis for } L, \\ \text{and } S \text{ spans } V. \end{cases}$$

2. Graphical subsets

We wish to classify the subsets S of L satisfying (1.15). We shall do this by constructing one such subset B and proving that every S is equivalent either to a subset of B or to one "exceptional" set.

In order to define B, we start from a lattice K of rank 5 with a fixed basis k_0, k_1, k_2, k_3, k_4. For L we choose the sublattice of rank 4 consisting of all $m_0 k_0 + \cdots + m_4 k_4$ (with $m_i \in Z$) for which $m_0 + \cdots + m_4 = 0$. Then B will be the subset of L consisting of the 20 elements $k_i - k_j$, where $i, j = 0, \cdots, 4, i \neq j$.

It is clear that $-B = B$, $0 \notin B$ and B spans V. In fact, B generates L. However, it is not immediately obvious that any four independent elements of B form a basis for L. In order to prove this, and to aid in the classification of subsets of B, we introduce a 2-to-1 map β of B onto the complete graph Γ_5 on five points $P_0, \cdots, P_4$. This is defined by $\beta : k_i - k_j \to \overline{P_i P_j}$. Note that β defines a one-to-one correspondence between all subsets S of B satisfying $-S = S$ and all subgraphs of Γ_5.

The following proposition expresses the basic property of the set B:

PROPOSITION 2.1. *Let* $b_1, \cdots, b_4$ *be elements of* B. *The following statements are equivalent*:

(a) $b_1, \cdots, b_4$ *are independent.*

(b) $\Gamma = \{\beta(b_1), \cdots, \beta(b_4)\}$ *is a maximal subtree of* Γ_5.

(c) $b_1, \cdots, b_4$ *form a basis for* L.

Proof. Suppose (a) holds. Then $b_i \neq \pm b_j$, for $i \neq j$. So Γ consists of four distinct line segments. Either Γ is a maximal subtree of Γ_5 or it contains a closed loop $\overline{P_{i_1} P_{i_2}}, \overline{P_{i_2} P_{i_3}}, \cdots, \overline{P_{i_n} P_{i_1}}$, where $i_1, i_2, \cdots, i_n$ are distinct, and $n \geqq 3$. In the latter case, we may assume that

$$\beta(b_1) = \overline{P_{i_1} P_{i_2}}, \quad \beta(b_2) = \overline{P_{i_2} P_{i_3}}, \quad \cdots, \quad \beta(b_n) = \overline{P_{i_n} P_{i_1}}.$$

From the definition of β, we see that, for some choice of signs,

$$\pm b_1 = k_{i_1} - k_{i_2}, \quad \pm b_2 = k_{i_2} - k_{i_3}, \quad \cdots, \quad \pm b_n = k_{i_n} - k_{i_1}.$$

For the same choice of signs, $(\pm b_1) + (\pm b_2) + \cdots + (\pm b_n) = 0$. This contradicts the independence of $b_1, \cdots, b_4$. So (a) implies (b).

Assume that (b) holds. By choosing P_4 to be one "end" of the graph Γ and using induction, we may assume that the indices are so arranged that

$$\beta(b_1) = \overline{P_{i_1}P_1}, \quad \cdots, \quad \beta(b_4) = \overline{P_{i_4}P_4},$$

where $i_1 < 1, \cdots, i_4 < 4$. Replace b_j by $-b_j$, if necessary, to reach

$$b_1 = k_1 - k_{i_1}, \quad \cdots, \quad b_4 = k_4 - k_{i_4}.$$

This is clearly a basis of L. So (b) implies (c).

Obviously (c) implies (a).

COROLLARY 2.2. *A subset S of B satisfies* (1.15) *if and only if $S = \beta^{-1}(\Gamma)$, where Γ is a subgraph of Γ_5 containing at least one maximal subtree of Γ_5. In particular, B satisfies* (1.15).

Because of the close connection between subsets of B and subgraphs of Γ_5, we use the adjective *graphical* to denote those subsets S of L satisfying (1.15) which are equivalent to subsets of B.

For the rest of this section, S will be a fixed subset of L satisfying (1.15), and $s_1, \cdots, s_4$ will be a basis for L lying in S.

The property that any four independent elements of S form a basis of L restricts the possible forms of elements of S. For example

(2.3) *if* $s = m_1 s_1 + \cdots + m_4 s_4 \in S$ (with $m_i \in Z$) *then* $|m_i| \leq 1$, *for all* i.

Indeed, if $|m_1| > 1$, then s, s_2, s_3, s_4 would be four independent elements of S but would not form a basis of L, since the determinant of the transformation $s_1, \cdots, s_4 \to s, s_2, s_3, s_4$ is $m_1 \neq \pm 1$.

The following consequence of the same property is more difficult to state but very powerful. Divide the basis $s_1, \cdots, s_4$ into two disjoint subsets $\{s_{i_1}, \cdots, s_{i_n}\}$ and $\{s_{j_1}, \cdots, s_{j_m}\}$, where $2 \leq n \leq 4$, and $m = 4 - n$. Let $l_1, \cdots, l_n$ be any linear combinations of $s_{j_1}, \cdots, s_{j_m}$. Then we have

PROPOSITION 2.4. *If S contains*

$$s_1' = s_{i_1} - s_{i_2} + l_1, \cdots, s_{n-1}' = s_{i_{n-1}} - s_{i_n} + l_{n-1},$$

then it cannot contain $s_n' = s_{i_n} + s_{i_1} + l_n$.

Proof. Assume that $s_n' \in S$. Consider the matrix A of the linear transformation sending the basis $s_{i_1}, \cdots, s_{i_n}, s_{j_1}, \cdots, s_{j_m}$ into $s_1', \cdots, s_n', s_{j_1}, \cdots, s_{j_m}$. It has the form

$$A = \begin{bmatrix} 1 & -1 & & & & \\ & & \ddots & \ddots & & L \\ & & & 1 & -1 & \\ 1 & & & & 1 & \\ & & & & & \\ & & & & & I \end{bmatrix}$$

where L is some integral matrix, I is the $m \times m$ identity matrix and the blank spaces are filled with zeroes. The determinant of this matrix is clearly 2. So $s'_1, \cdots, s'_n, s_{j_1}, \cdots, s_{j_m}$ are four independent elements of S which do not form a basis for L. This contradicts (1.15).

To apply Proposition 2.4, it is convenient to introduce the following equivalence relation on $s_1, \cdots, s_4$:

$s_i \sim s_j$ if $i = j$ or there are distinct indices $i = h_1, h_2, \cdots, h_n = j$ such that $s_{h_1} - s_{h_2}, \cdots, s_{h_{n-1}} - s_{h_n}$ all lie in S.

Clearly $s_i \sim s_j$ implies that S contains no elements of the form $s_i + s_j + l$, where l is a linear combination of those s_k for which $k \neq h_1, \cdots, h_n$.

To make our equivalence relation as strong as possible we use

LEMMA 2.5. *After replacing s_i by $-s_i$, for various i, we may assume that S contains no elements of the form $s_j + s_h$.*

Proof. Assume that our basis $s_1, \cdots, s_4$ is already chosen from among the 2^4 bases of the form $\pm s_1, \cdots, \pm s_4$ to maximize the number N of elements in S of the form $s_i - s_j$.

Suppose that $s_j + s_h \in S$. By Proposition 2.4, $s_j \nsim s_h$. Define a new basis $s'_1, \cdots, s'_4$ by

$$s'_i = s_i \quad \text{if} \quad s_i \nsim s_h, \qquad s'_i = -s_i \quad \text{if} \quad s_i \sim s_h.$$

If $s_i - s_k \in S$, then $s_i \sim s_k$. So $s'_i - s'_k = \pm(s_i - s_k) \in S$. Furthermore S contains $s'_j - s'_h$, while $s_j - s_h \notin S$. So S has at least $N + 1$ elements of the form $s'_i - s'_k$. This contradicts the maximality of N and proves the lemma.

From now on we assume that the replacement in Lemma 2.5 has already been carried out. In view of (2.3), this means that

(2.6) *any element in S of the form $m_i s_i + m_j s_j$, where $i \neq j$ and $m_i, m \neq 0$, must be either $s_i - s_j$ or $s_j - s_i$.*

We can embed L into K by $T : s_i \rightarrow k_i - k_0$, for $i = 1, \cdots, 4$. Then $T : s_i - s_j \rightarrow k_i - k_j \in B$. Hence

(2.7) *if S consists only of elements of the forms $\pm s_i$ and $\pm s_j \pm s_k$, then it is graphical.*

Now we consider the relationship between an element

$$s = m_i s_i + m_j s_j + m_k s_k = \pm s_i \pm s_j \pm s_k \quad (i, j, k \text{ distinct}) \tag{2.8}$$

of S and the equivalence relation $\sim$. The basic fact is this immediate consequence of Proposition 2.4:

(2.9) *If S contains elements $s_{h_1} - s_{h_2}, \cdots, s_{h_{n-1}} - s_{h_n}$ ($n \geq 2$) such that $h_1 = i$, $h_n = j$ and $h_l \neq k$, for $l = 1, \cdots, n$, then $m_i = -m_j$.*

In particular

(2.10) *if* $s_i \sim s_j \nsim s_k$, *then* $m_i = -m_j$.

When $s_i \sim s_j \sim s_k$, things are more complicated. Let $s_{h_1} - s_{h_2}, \cdots, s_{h_{n-1}} - s_{h_n} \in S$ satisfy $h_1 = i$, $h_n = k$ and $h_1, \cdots, h_n$ are *all distinct.* If $j = h_r$, for some $r = 2, \cdots, n-1$, then the chain $s_{h_1} - s_{h_2}, \cdots, s_{h_{r-1}} - s_{h_r}$ satisfies (2.9). So $m_i = -m_j$. Similarly $m_j = -m_k$. In this case we say that s_j *splits* s_i and s_k.

If, on the other hand, $j \neq h_r$ for $r = 2, \cdots, n-1$, then, by (2.9), $m_i = -m_k$. Since $m_i = -m_j$, $m_j = -m_k$, $m_k = -m_i$ is impossible, one of s_i, s_j, s_k must always split the other two. Hence

(2.11) *if* $s_i \sim s_j \sim s_k$, *then precisely two of* m_i, m_j, m_k *are equal.*

This is enough to prove

LEMMA 2.12. *Suppose that* S *consists of* $\pm s$, *where* s *is given by* (2.8), *some elements of the form* $s_k - s_l$ *and, of course,* $\pm s_1, \cdots, \pm s_4$. *Then* S *is graphical.*

Proof. We consider the "worst" case first. Suppose that $s_i \sim s_j \sim s_k$, and that s_j splits s_i and s_k. Then $\pm s = \pm(s_i - s_j + s_k)$. By (2.9), S cannot contain $\pm(s_i - s_k)$, but it can contain $\pm(s_i - s_j)$ and $\pm(s_j - s_k)$.

Let s_h be the fourth basis element. By (2.9), S cannot contain both $\pm(s_i - s_h)$ and $\pm(s_h - s_k)$. Assume, by symmetry, that $\pm(s_h - s_k) \notin S$. Then S must be contained in the set

$$S_0 = \{\pm s_i, \pm s_j, \pm s_k, \pm s_h, \pm(s_i - s_j + s_k), \pm(s_i - s_j), \pm(s_j - s_k), \pm(s_i - s_h), \pm(s_j - s_h)\}$$

Embed L in K by $T: s_i \to k_i - k_0, s_j \to k_j - k_0, s_h \to k_h - k_0, s_k \to k_j - k_k$. Clearly $T(S_0) \subseteq B$, so S_0, and therefore S, is graphical.

In any other case, one of s_i, s_j, s_k, say s_i, must be $\nsim$ the other two. After a possible transformation of the form $s_l \to s_l$, if $s_l \nsim s_i$; $s_l \to -s_l$, if $s_l \sim s_i$ (which does not change (2.6)), we may assume that precisely two of m_i, m_j, m_k are equal. A repetition of the argument above shows that S is graphical.

Not many elements of the form (2.8) can lie in S:

LEMMA 2.13. *At most four elements of the form* (2.8) *can appear in* S. *If precisely four appear, then, after reindexing the* s_i, *they have the form*

(2.14) $\pm(m_1 s_1 + m_2 s_2 + m_3 s_3)$, $\pm(m_1 s_1 + m_2 s_2 + m_4 s_4)$, *where* $|m_i| = 1$ *for all* i.

Proof. If two pairs $\pm s$ of those elements appear, we may assume, after reindexing, that they are $\pm(m_1 s_1 + m_2 s_2 + m_3 s_3)$, and $\pm(n_1 s_1 + n_2 s_2 + n_k s_k)$, where $|m_i| = |n_j| = 1$, for all i, j, and $k = 3$ or 4. We may even assume that $n_1 = m_1$.

If $n_2 = -m_2$, then S contains elements of the form $s_1 + s_2 + \cdots$ and $s_1 - s_2 + \cdots$, contradicting Proposition 2.4. Hence $n_2 = m_2$.

If $k = 3$, then similarly $n_3 = m_3$, contradicting the fact that

$$n_1 s_1 + n_2 s_2 + n_k s_k \neq m_1 s_1 + m_2 s_2 + m_3 s_3 .$$

So $k = 4$. Therefore (2.14) holds, with $m_4 = n_4$.

If a fifth element of the form (2.8) appears in S, the above arguments show that, after reindexing, $m_1 s_1 + m_3 s_3 + m_4 s_4 \in S$. Then s_1, $m_1 s_1 + m_2 s_2 + m_3 s_3$, $m_1 s_1 + m_2 s_2 + m_4 s_4$, $m_1 s_1 + m_3 s_3 + m_4 s_4$ are four independent elements of S which do not form a basis for L. This contradicts (1.15) and proves the lemma.

The most complicated of our lemmas is

LEMMA 2.15. *Suppose that S consists of the elements* (2.14), *some elements of the form $s_i - s_j$ and $\pm s_i, \cdots, \pm s_4$. Then either S is graphical or else, after reindexing, S is*

$$\{\pm s_1, \pm s_2, \pm s_3, \pm s_4, \pm(s_1 - s_3), \pm(s_3 - s_4), \pm(s_2 - s_4), \pm(s_1 + s_2 - s_3), \pm(s_1 + s_2 - s_4)\} \tag{2.16}$$

Proof. Assume, to begin with, that $m_1 = -m_2$. There are two possibilities:

$m_3 = m_4$. In this case, after reindexing, the elements (2.14) become

$$\pm(s_1 - s_2 + s_3), \quad \pm(s_1 - s_2 + s_4)$$

By (2.9), neither $\pm(s_1 - s_3)$ nor $\pm(s_1 - s_4)$ can lie in S. So S is contained in

$$S_1 = \{\pm s_1, \pm s_2, \pm s_3, \pm s_4, \pm(s_1 - s_2 + s_3), \pm(s_1 - s_2 + s_4), \pm(s_1 - s_2), \pm(s_2 - s_3), \pm(s_2 - s_4), \pm(s_3 - s_4)\}.$$

Embed L in K by $T: s_1 \to k_2 - k_1$, $s_2 \to k_2 - k_0$, $s_3 \to k_3 - k_0$, $s_4 \to k_4 - k_0$. Then $T(S) \subseteq T(S_1) \subseteq B$. So S is graphical.

$m_3 = -m_4$. After reindexing, the elements (2.14) become

$$\pm(s_1 - s_2 + s_3), \quad \pm(s_1 - s_2 - s_4)$$

By (2.9), neither $\pm(s_1 - s_3)$ nor $\pm(s_2 - s_4)$ can lie in S. Furthermore, if $\pm(s_3 - s_4) \in S$, then $s_2 - s_3 - s_1$, $s_3 - s_4$, $s_4 + s_2 - s_1 \in S$ contradicts Proposition 2.4. Hence S is contained in

$$S_2 = \{\pm s_1, \pm s_2, \pm s_3, \pm s_4, \pm(s_1 - s_2 + s_3), \pm(s_1 - s_2 - s_4), \pm(s_1 - s_2), \pm(s_2 - s_3), \pm(s_1 - s_4)\}.$$

Embed L in K by $T: s_1 \to k_1 - k_0$, $s_2 \to k_2 - k_0$, $s_3 \to k_2 - k_3$, $s_4 \to k_1 - k_4$. Then $T(S) \subseteq T(S_2) \subseteq B$. So S is graphical.

Now assume that $m_1 = m_2$. If $s_1 \nsim s_2$, change bases by

$$s_i \to -s_i \quad \text{if} \quad s_i \sim s_1 ; \qquad s_i \to s_i \quad \text{if} \quad s_i \nsim s_1 .$$

This reduces S to the case above. So we may suppose $s_1 \sim s_2$. By (2.10), $s_1 \sim s_2 \sim s_3 \sim s_4$. Furthermore, by (2.11), $m_3 = m_4 = -m_1$. So the elements (2.14) are

$$\pm(s_1 + s_2 - s_3), \quad \pm(s_1 + s_2 - s_4).$$

Using the first of these elements and (2.9), we see that S cannot contain both $s_1 - s_4$ and $s_2 - s_4$. Using the second, S cannot contain both $s_1 - s_3$ and $s_2 - s_3$. Furthermore, it cannot contain $s_1 - s_2$.

By symmetry, we may assume that $s_1 - s_4 \notin S$. Some $s_1 - s_j$ lies in S, since $s_1 \sim s_2$. And $s_1 - s_2$, $s_1 - s_4 \notin S$. So $s_1 - s_3 \in S$. As noted above, this forces $s_2 - s_3 \notin S$. Some $s_2 - s_j$ lies in S. It must be $s_2 - s_4$. If $s_3 - s_4 \notin S$, then $\pm(s_1 - s_3)$, $\pm(s_2 - s_4)$ are the only elements in S of the form $s_i - s_j$. This contradicts $s_1 \sim s_2$. Hence $s_3 - s_4 \in S$, and S is given by (2.16).

Rather than consider a large number of cases, we handle the elements of the form $\pm s_1 \pm s_2 \pm s_3 \pm s_4$ in S by different arguments.

LEMMA 2.17. *Suppose that, for any basis $s_1, \cdots, s_4$ of L lying in S, some element of the form $\pm s_1 \pm s_2 \pm s_3 \pm s_4$ appears in S. Then, with respect to a suitable basis, S is*

$$\{\pm s_1, \pm s_2, \pm s_3, \pm s_4, \pm(s_1 + s_2 + s_3 + s_4)\}. \tag{2.18}$$

Proof. We may change the signs of the elements of some basis $s_1, \cdots, s_4$ to reach

$$\pm(s_1 + s_2 + s_3 + s_4) \in S.$$

By (2.4), S can contain no elements of the form $s_i - s_j + \cdots$, where $i \neq j$. As in Lemma 2.13, this implies that *no other elements of the form $\pm s_1 \pm s_2 \pm s_3 \pm s_4$ appear in S.*

If some element of the form (2.8) appears in S, we may assume that it is $s_1 + s_2 + s_3$. Let s_1', s_2', s_3', s_4' be the new basis $s_1 + s_2 + s_3 + s_4$, $s_1 + s_2 + s_3$, s_1, s_2. By hypothesis,

$$m_1 s_1' + m_2 s_2' + m_3 s_3' + m_4 s_4'$$
$$= (m_1 + m_2 + m_3)s_1 + (m_1 + m_2 + m_4)s_2 + (m_1 + m_2)s_3 + m_1 s_4 \in S,$$

for some m_i with $|m_i| = 1$, for $i = 1, \cdots, 4$. Since $|m_1 + m_2| \leq 1$, by (2.3), and $m_1 + m_2$ is even, we see that $m_1 = -m_2$. So S contains elements of the form $\pm s_1 \pm s_2 \pm s_4$. These must be $\pm(s_1 + s_2 + s_4)$. Similarly $\pm(s_1 + s_3 + s_4) \in S$. But s_1, $s_1 + s_2 + s_3$, $s_1 + s_2 + s_4$, $s_1 + s_3 + s_4$ do not form a basis for L, contradicting (1.15). Therefore

(2.19) *no elements of the form* (2.8) *appear in S.*

If some element of the form $\pm s_i \pm s_j$ $(i \neq j)$ appears in S, we may assume that it is $s_1 + s_2$. Let $s_1'', s_2'', s_3'', s_4''$ be the new basis $s_1 + s_2$, s_2, s_3, s_4. By hypothesis,

$$m_1 s_1'' + m_2 s_2'' + m_3 s_3'' + m_4 s_4'' = m_1 s_1 + (m_1 + m_2) s_2 + m_3 s_3 + m_4 s_4 \in S,$$

for some m_i with $|m_i| = 1$, for $i = 1, \cdots, 4$. Clearly $m_1 = -m_2$. So S contains $m_1 s_1 + m_3 s_3 + m_4 s_4$ of the form (2.8), contradicting (2.19).

We conclude that S is given by (2.18).

COROLLARY 2.20. *S is graphical.*

Proof. Embed L in K by $T : s_1 \to k_1 - k_0$, $s_2 \to k_2 - k_1$, $s_3 \to k_3 - k_2$, $s_4 \to k_4 - k_3$. Then T sends $s_1 + s_2 + s_3 + s_4$ into $k_4 - k_0$. So $T(S) \subseteq B$.

By (2.7), Lemmas 2.12, 2.13 and 2.15, and Corollary 2.20, we conclude with

THEOREM 2.21. *Let S satisfy* (1.15). *Then either S is graphical, or else it is given by* (2.16), *with respect to a suitable basis.*

3. A list of graphs

We wish to list, to within equivalence, those graphical subsets of L which can lead to maximal groups (two subsets S, S' being *equivalent* if there is an automorphism of L carrying S onto S'). As we shall see, this by no means requires a list of all graphs on five points, or even those containing maximal trees.

A subgraph Γ (on any number of points) of Γ_5 will be called *reduced* if each vertex $P_i \in \Gamma$ lies on at least two distinct segments $\overline{P_i P_j}$, $\overline{P_i P_k} \subseteq \Gamma$, $i \neq j \neq k \neq i$.

LEMMA 3.1. *Any graphical subset of L is equivalent to a subset S of the form.*

$$S = \beta^{-1}(\Gamma) \cup \{\pm s_1, \cdots, \pm s_n\}, \qquad n \geq 0, \tag{3.2}$$

where Γ is a reduced subgraph of Γ_5 on 5 - n points, and $s_1, \cdots, s_n$ form a basis for L modulo the sublattice L_Γ generated by $\beta^{-1}(\Gamma)$.

Proof. Let $S' = \beta^{-1}(\Gamma')$, where Γ' is a connected subgraph of Γ_5. If Γ' is reduced, we are done. Otherwise some vertex of Γ', say P_4, must be on only one segment, say $\overline{P_3 P_4}$. Let $\Gamma'' = \Gamma' - \{\overline{P_3 P_4}\}$, a graph on $P_0, \cdots, P_3$. Then $S' = \beta^{-1}(\Gamma'') \cup \{\pm(k_3 - k_4)\}$. Clearly Γ'' is connected. So $k_3 - k_4$ is a basis for L modulo $L_{\Gamma''}$.

An obvious induction completes the proof.

There are, to within isomorphism, just 16 reduced subgraphs of Γ_5:

LEMMA 3.3. *Any reduced subgraph of Γ_5 is isomorphic to one of the graphs displayed in Figure* 3.4.

Note. The circles appearing on certain lines in Figure 3.4 will be explained in Lemma 3.10 below.

Proof. Let Γ be a reduced subgraph of Γ_5. We first prove that

(3.5) *Any segment of Γ must appear in some closed loop in Γ.*

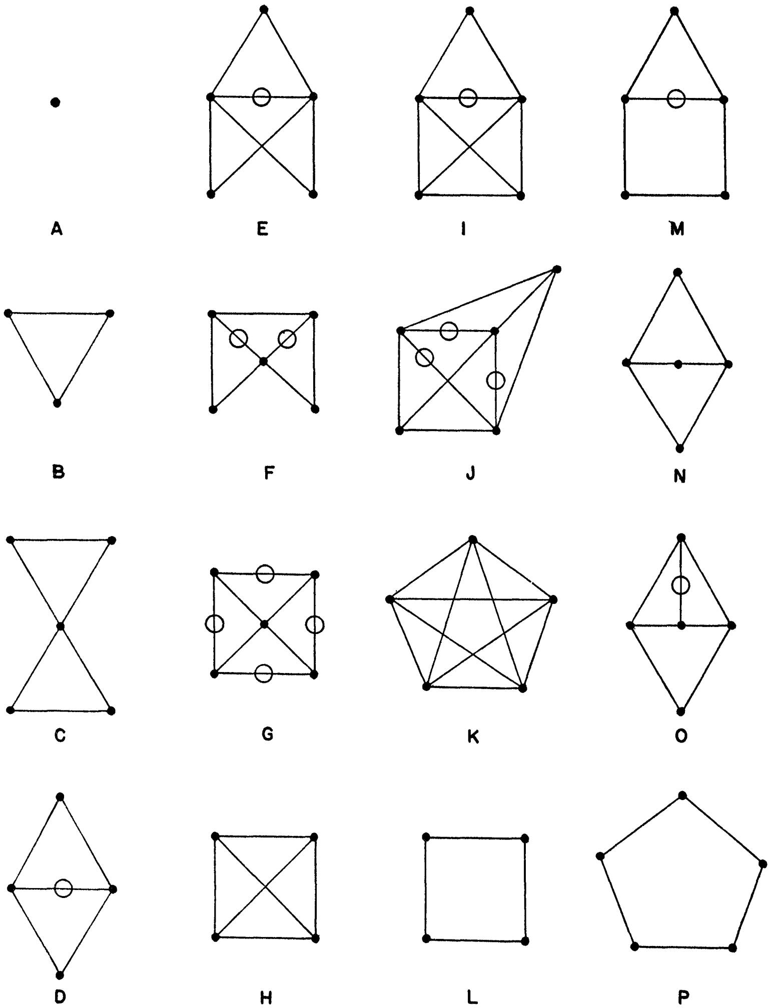

FIGURE 3.4

Suppose, e.g., $\overline{P_{i_0} P_{i_1}} \in \Gamma$ lies on no closed loop. Construct a chain

$$\cdots, \overline{P_{i_{-1}} P_{i_0}}, \overline{P_{i_0} P_{i_1}}, \overline{P_{i_1} P_{i_2}}, \cdots$$

of segments in Γ such that $i_{j-1} \neq i_{j+1}$, for all j. Let n be the first index such that $n \geq 1$, and $i_n = i_j$, for some $j < n$. Since $\overline{P_{i_0} P_{i_1}}$ appears in no closed loop, j must be ≥ 1. So $n > j + 2 \geq 3$, and $P_{i_0}, P_{i_1}, P_{i_2}, P_{i_3}$ are all distinct.

Similarly $P_{i_{-2}}, P_{i_{-1}}, P_{i_0}, P_{i_1}$ are all distinct. Since $i_{-r} = i_s$, $r \geq 0$, $s \geq 1$, would force $\overline{P_{i_0} P_{i_1}}$ to lie on a loop, the six points $P_{i_{-2}}, \cdots, P_{i_3}$ are all distinct. But Γ is a graph on ≤ 5 points. This proves (3.5).

By (3.5), Γ is a union of triangles (3.4B), quadrilaterals (3.4L) and pentagons (3.4P). We consider all cases.

If Γ has no segments, it is (3.4A).

Suppose Γ *is a union of triangles:*

If Γ contains one triangle, it is (3.4B).

If Γ contains two triangles, it is (3.4C) or (3.4D).

If Γ contains three or more triangles, then two of them must intersect in a line (count vertices!). So Γ has a subgraph isomorphic to (3.4D).

Suppose Γ has three or more triangles, and does not contain a tetrahedron (3.4H). Then it consists of (3.4D), together with two or more segments connecting this subgraph with a fifth point P_0.

If two segments contain P_0, then Γ is (3.4E) or (3.4F) or (3.4O).

If three segments contain P_0, then Γ is (3.4G) or (3.4I) (which is excluded, since it contains a tetrahedron).

If four segments contain P_0, then Γ contains a tetrahedron.

Suppose Γ contains a tetrahedron (3.4H). Any further segments must connect these vertices with the fifth vertex P_0.

If no segments contain P_0, Γ is (3.4H).

If two segments contain P_0, Γ is (3.4I).

If three segments contain P_0, Γ is (3.4J).

If four segments contain P_0, Γ is (3.4K).

Suppose Γ *is not a union of triangles:*

If Γ is not a union of triangles and quadrilaterals, it must be a pentagon (3.4P).

Otherwise, Γ must contain a quadrilateral (3.4L) but no further segments on these four vertices. Let the fifth vertex be P_0.

If no segments contain P_0, Γ is (3.4L).

If two segments contain P_0, Γ is (3.4M) or (3.4N).

If three segments contain P_0, Γ is (3.4O).

If four segments contain P_0, Γ is (3.4G) (which is excluded as a union of triangles).

We have considered all cases.

Half the graphs in Figure 3.4 are removed from consideration by the following argument:

We say that a subgraph Γ' of graph Γ is a *closed loop of length* $n \geq 3$ if it has the form

$$\Gamma' = \{\overline{P_{i_1} P_{i_2}}, \overline{P_{i_2} P_{i_3}}, \cdots, \overline{P_{i_{n-1}} P_{i_n}}, \overline{P_{i_n} P_{i_1}}\},$$

where $P_{i_1}, \cdots, P_{i_n}$ are *distinct* vertices. If $\overline{P_i P_j} \in \Gamma$, and $n \geq 3$, let $N_n(\overline{P_i P_j}, \Gamma)$ denote the number of closed loops of length n in Γ which contain $\overline{P_i P_j}$.

LEMMA 3.6. *Let* Γ *be a subgraph of* Γ_5, *and* $S = \beta^{-1}(\Gamma)$. *If* $s \in S$ *and* $n \geq 3$, *then* $N_n(\beta(s), \Gamma)$ *equals the number of subsets* S_1 *of* S *satisfying*

(a) S_1 *has* $n - 1$ *elements,*

(3.7) (b) $\sum_{s_1 \in S_1} s_1 = s$,

(c) *if* S_2 *is a proper subset of* S_1, *then* $\sum_{s_2 \in S_2} s_2 \neq s$.

Proof. Let $\beta(s) = \overline{P_{i_1} P_{i_2}}$, and $s = k_{i_1} - k_{i_2}$.

Suppose $S_1 \subseteq S$ satisfies (3.7). By (3.7b), some element of S_1 must have the form $k_{i_3} - k_{i_2}$. Suppose, by induction, that S_1 contains elements $k_{i_3} - k_{i_2}, k_{i_4} - k_{i_3}, \cdots, k_{i_r} - k_{i_{r-1}}$, where $r \geq 3$, and $i_1, i_2, \cdots, i_{r-1}$ are all distinct. If $i_r = i_1$, then the sum of these elements is s. So, by (3.7c), they are all the elements of S_1. If $i_r = i_j$, for some j with $2 \leq j \leq r - 1$, then the sum of the elements $k_{i_{j+1}} - k_{i_j}, \cdots, k_{i_r} - k_{i_{r-1}}$ is zero. The sum of the rest of the elements of S_1 must be s, contradicting (3.7c). If $i_1, \cdots i_r$ are distinct, the sum of the above elements is $k_{i_r} - k_{i_2}$. So S_1 must contain an element of the form $k_{i_{r+1}} - k_{i_r}$, and the induction is complete.

We conclude that S_1 has the form

$$S_1 = \{k_{i_3} - k_{i_2}, k_{i_4} - k_{i_3}, \cdots, k_{i_n} - k_{i_{n-1}}, k_{i_1} - k_{i_n}\}$$

where $i_1, \cdots, i_n$ are distinct. Obviously $\beta(S_1) \cup \{\beta(s)\}$ is a closed loop of length n containing $\beta(s)$.

Suppose $\Gamma' = \{\overline{P_{i_1} P_{i_2}}, \overline{P_{i_2} P_{i_3}}, \cdots, \overline{P_{i_n} P_{i_1}}\}$ is a closed loop of length n in Γ containing $\overline{P_{i_1} P_{i_2}}$. Then $S_1 = \{k_{i_3} - k_{i_2}, \cdots, k_{i_n} - k_{i_{n-1}}, k_{i_1} - k_{i_n}\}$ satisfies (3.7) and $\beta(S_1) \cup \{\beta(s)\} = \Gamma'$. Any other subset S_1' of $\beta^{-1}(\Gamma')$ satisfying (3.7) must be of the form $\{\varepsilon_2(k_{i_3} - k_{i_2}), \cdots, \varepsilon_n(k_{i_1} - k_{i_n})\}$, where $\varepsilon_2, \cdots, \varepsilon_n$ are all ± 1. Then (3.7b) becomes

$$k_{i_1} - k_{i_2} = \varepsilon_n k_{i_1} - \varepsilon_2 k_{i_2} + (\varepsilon_2 - \varepsilon_3) k_{i_3} + \cdots + (\varepsilon_{n-1} - \varepsilon_n) k_{i_n}.$$

Since $i_1, \cdots, i_n$ are all distinct, this implies $\varepsilon_2 = \cdots = \varepsilon_n = 1$, and $S_1 = S_1'$.

We have constructed a one to one correspondence between subsets S_1 satisfying (3.7) and loops of length n containing $\beta(s)$. So the lemma is true.

COROLLARY 3.8. *If* $g \in G(S, L)$, *then, for any* $n \geq 3$,

$$N_n(\beta(s), \Gamma) = N_n(\beta(gs), \Gamma).$$

Proof. Obviously the number of subsets S_1 satisfying (3.7) is invariant under $G(S, L)$.

If S is any finite subset spanning V and S' is a proper subset of S satisfying

(3.9) S' *spans* V *and* $G(S, L)$ *sends* S' *into itself,*

then $G(S, L) \subseteq G(S', L)$. Since we are only interested in maximal finite groups, we need only consider the *reduced* subsets S of L, i.e., those for which no proper subset S' of S satisfies (3.9).

LEMMA 3.10. *If S has the form* (3.2), *where* Γ *is* D, E, F, G, I, J, M *or* O *of Figure* (3.4), *then S is not reduced.*

Proof. Let $S = \beta^{-1}(\Gamma')$, for some $\Gamma' \subseteq \Gamma_5$. It is clear from Lemma 3.1 that $N_n(\beta(s), \Gamma') = 0$, for all $n \geq 3$, if $\beta(s) \notin \Gamma$, while $N_n(\beta(s), \Gamma') = N_n(\beta(s), \Gamma)$, if $\beta(s) \in \Gamma$. Furthermore, in the latter case $N_n(\beta(s), \Gamma) \neq 0$, for some $n \geq 3$. We conclude from Corollary 3.8 that subset $S_0 = \beta^{-1}(\Gamma_0)$ is invariant under $G(S, L)$ provided Γ_0 is the subgraph of all $\overline{P_i P_j}$ in Γ satisfying equations of the form $N_n(\overline{P_i P_j}, \Gamma) = a_n$, for some $n \geq 3$ and some a_n. If $S - S_0 = S'$ spans V, or, what is the same thing, if $\Gamma' = \Gamma - \Gamma_0$ contains a maximal subtree, then (3.9) is satisfied and S is not reduced.

In each case below the subgraph Γ_0 consists of those segments $\overline{P_i P_j} \in \Gamma$ for which $N_n = N_n(\overline{P_i P_j}, \Gamma)$ has the indicated value. In Figure 3.4, Γ_0 is the subgraph consisting of all segments with circles on them. By inspection it satisfies the conditions above. So S is not reduced.

D: $N_3 = 2$
E: $N_3 = 3$
F: $N_3 = 2$
G: $N_3 = 1$
I: $N_3 = 3$
J: $N_3 = 3$
M: $N_3 = 1$ *and* $N_4 = 1$
O: $N_3 = 2$

We conclude from Lemma 3.10, and the arguments above:

THEOREM 3.11. *If S is a graphical subset of L, and $G(S, L)$ is maximal, then S has the form* (3.2), *where* Γ *is one of the graphs* A, B, C, H, K, L, N *or* P *in Figure* 3.4.

4. The maximal groups

After Theorems 1.14, 2.21 and 3.11, there are $1 + 1 + 8 = 10$ cases to be considered. In each case we must decide whether the group in question is maximal, and whether it is equivalent to any of the other groups.

We say that a group H is *uniform* if there is, up to constant multiples, precisely one positive definite quadratic form ϕ invariant under H for which $S(\phi, L)$ spans V. We call ϕ an *associated form* of H and the set $S(\phi, L)$, which is uniquely determined by H, *the associated subset.* It turns out that all our maximal groups are uniform. So both of our questions above are simplified by the following observations:

Observation 4.1. *If a group H is uniform, with associated subset S, then $G(S, L)$ is maximal* (*and uniform with the same subset*).

For any group K containing $G(S, L)$ must leave invariant some form ϕ. Since $G(S, L)$ contains H, the form ϕ must be associated to H. Therefore K

leaves $S = S(\phi, L)$ invariant, i.e., $K \subseteq G(S, L)$. The uniformity of $G(S, L)$ is obvious.

Observation 4.2. *Let G_1, G_2 be maximal and uniform groups, with associated sets S_1, S_2, resp. Then G_1, G_2 are equivalent if and only if S_1, S_2 are equivalent.*

For any equivalence between G_1 and G_2 must be an equivalence between their associated forms ϕ_1, ϕ_2 and hence, between S_1 and S_2. Since, by (1.1), $G_i = G(S_i, L)$, the converse is also obvious.

We begin with the exceptional form in Theorem 1.14:

Case I. $S = S(\phi, L)$, *where ϕ is given by* (1.8).

The ring I of integral quaterions (see [4]) has a lattice basis

$$b_1 = 1, \quad b_2 = i, \quad b_3 = j, \quad b_4 = -\tfrac{1}{2}(1 + i + j + k).$$

The norm of a general element of I is given by

$$N(X_1 b_1 + \cdots + X_4 b_4) = X_1^2 + X_2^2 + X_3^2 + X_4^2 - (X_1 + X_2 + X_3)X_4 .$$

So we may identify L with I by $l_i \leftrightarrow b_i$, $i = 1, \cdots, 4$, sending ϕ into N.

The unit group U of I consists of the 24 elements of norm 1,

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad \tfrac{1}{2}(\pm 1 \pm i \pm j \pm k).$$

Since the norm of any element of I is an integer, $U = S(N, I)$.

Let H be the group of all maps $r \rightarrow u \cdot r$ of I into I, where $u \in U$. Clearly H is transitive on U. So any form ϕ invariant under H must have a constant value $c = \phi(u)$, for all $u \in U$. This easily implies that $\phi = c \cdot N$. So H is uniform. From Observation 4.1, we conclude that

(4.3) *the group $Qn = G(U, I)$ is maximal and uniform, with associated subset U.*

Incidently, Qn has $1152 = 3^2 \cdot 2^7$ elements. To see this, note that it is transitive on U, since H is. The subgroup leaving 1 fixed must permute the elements $\pm i$, $\pm j$, $\pm k$, which are perpendicular to 1, among themselves. It does this in $6 \cdot 4 \cdot 2 = 3 \cdot 2^4$ ways. Since the images of 1, i, j, k determine a transformation of I, this gives $24 \cdot 3 \cdot 2^4 = 3^2 \cdot 2^7$ elements.

Suppose that S is given by (3.2). Let L' be the sublattice of L having $s_1, \cdots, s_n$ as basis. Then L is the direct sum $L_\Gamma \dotplus L'$. As in the proof of Lemma 3.10, the subsets $\beta^{-1}(\Gamma)$ and $\{\pm s_1, \cdots, \pm s_n\}$ are invariant under $G(S, L)$. So the sublattices L_Γ, L' which they generate are also invariant. We conclude that

$$(4.4) \qquad G(S, L) = G(\beta^{-1}(\Gamma), L_\Gamma) \otimes G(\{\pm s_1, \cdots, \pm s_n\}, L').$$

Consider the second factor in (4.4). Evidently

$$G(\{\pm s_1, \cdots, \pm s_n\}, L') = Cu_n$$

is the "generalized permutation group" of order $n! \cdot 2^n$, consisting of all linear transformations of the form $s_i \to \varepsilon_i s_{\pi(i)}$, $i = 1, \cdots, n$, where π is some permutation of $1, \cdots, n$, and $\varepsilon_1, \cdots, \varepsilon_n$ are arbitrarily chosen ± 1's. The only form left invariant by Cu_n is the identity form $\phi(X_1 s_1 + \cdots + X_n s_n) = X_1^2 + \cdots + X_n^2$ (or a multiple thereof). Clearly $\{\pm s_1, \cdots, \pm s_n\} = S(\phi, L')$. So, from Observation 4.1,

(4.5) *for any integer* $n \geq 1$, *the group* Cu_n *is uniform and maximal, with associated subset* $\{\pm s_1, \cdots, \pm s_n\}$.

Case II. *S comes from the graph* Λ *of Figure* 3.4 *via* (3.2).

In this case Γ is empty. So, by (4.4) and (4.5), $G(S, L) = Cu_4$ is uniform and maximal. Its associated subset contains 8 points. By (4.3), the associated subset of Qn contains 24 points. So, by Observation 4.2, Cu_4 and Qn are inequivalent. Hence

(4.6) *the group* Cu_4 *is uniform, maximal, and inequivalent to* Qn. *Its associated subset is the S of this case.*

In applying (4.4), the following lemma is useful:

Lemma 4.7. *Let* H_1, H_2 *be uniform groups on lattices* L_1, L_2 *respectively. Suppose that each* H_i *contains the transformation* -1 *on* L_i. *Then* $H_1 \otimes H_2$ *is uniform on the lattice* $L_1 \oplus L_2$. *If* S_1, S_2 *are the associated subsets of* H_1, H_2, *resp., then* $(S_1 \oplus 0) \cup (0 \oplus S_2) = S$ *is the associated subset of* $H_1 \otimes H_2$.

Proof. Since $H_1 \otimes H_2$ contains a transformation which is -1 on L_1 and $+1$ on L_2, any form invariant under it must be a perpendicular direct sum $\phi_1 \oplus \phi_2$ of forms ϕ_i on L_i invariant under H_i, $i = 1, 2$. Clearly $S(\phi_1 \oplus \phi_2, L_1 \oplus L_2)$ is given by

$$S(\phi_1, L_1) \oplus 0, \qquad \text{if } \min \phi_1 < \min \phi_2,$$

$$0 \oplus S(\phi_2, L_2), \qquad \text{if } \min \phi_1 > \min \phi_2,$$

$$(S(\phi_1, L_1) \oplus 0) \cup (0 \oplus S(\phi_2, L_2)), \qquad \text{if } \min \phi_1 = \min \phi_2. \tag{4.8}$$

So $S(\phi_1 \oplus \phi_2, L_1 \oplus L_2)$ spans the vector space if and only if both $S(\phi_1, L_1)$ and $S(\phi_2, L_2)$ span their respective spaces, and $\min \phi_1 = \min \phi_2$. Since H_1, H_2 are both uniform, only one ray of forms can satisfy this condition. Therefore $H_1 \otimes H_2$ is uniform. The rest of the lemma follows from (4.8).

When the reduced graph Γ is the 1-skeleton of a simplex, its group is maximal by the following argument:

For any integer $n \geq 1$, let K be a lattice of dimension $n + 1$ with a fixed basis $k_0, k_1, \cdots, k_n$. The symmetric group S_{n+1} on $0, \cdots n$ operates on K by $\pi : k_i \to k_{\pi(i)}$, $i = 0, \cdots, n$. The vector space V_K spanned by K is the direct sum $V_K = V_1 \dotplus V_2$ of two absolutely irreducible subspaces under S_{n+1}. The subspace V_1 consists of all multiples of $k_0 + \cdots + k_n$, while V_2 consists of all $r_0 k_0 + \cdots + r_n k_n$ for which $r_0 + \cdots + r_n = 0$.

Let $L' = K \cap V_2$. It is a lattice of rank n invariant under the group H of transformations of V_2 induced by S_{n+1}. Since H is absolutely irreducible on V_2, there is only one invariant form ϕ (up to multiples). It must be the restriction to V_2 of the form $\phi'(X_0 k_0 + \cdots + X_n k_n) = X_0^2 + \cdots + X_n^2$ on V_K which is invariant under S_{n+1}. Since any element $r_0 k_0 + \cdots + r_n k_n \neq 0$ of L' must have at least two non-zero integral coefficients r_i, it is clear that

$$S(\phi, L') = \{k_i - k_j \mid i \neq j;\ i, j = 0, \cdots, n\}. \tag{4.9}$$

The uniformity of H and Observation 4.1 imply that the group $Sx_n = G(S(\phi, L'), L')$ satisfies

(4.10) *Sx_n is uniform and maximal. Its associated subset is given by* (4.9).

Incidently, it can be shown easily that Sx_n consists of all $\pm h$, where $h \in H$. So it has $2 \cdot n!$ elements, if $n \geq 2$, and 2 elements if $n = 1$.

Case III. *S comes from the graph* B *of Figure* 3.4 *via* (3.2).

By (4.9), it is clear that $G(\beta^{-1}(\Gamma), L_\Gamma) = Sx_2$. Hence, by (4.4) and (4.5), $G(S, L) = Sx_2 \otimes Cu_2$. This group is uniform with associated subset S (by Lemma 4.7). So it is maximal (by Observation 4.1). Since S has 10 elements, while the associated subsets of Qn and Cu_4 have 24 and 8 elements respectively, we conclude from Observation 4.2 that

(4.11) *The group $Sx_2 \otimes Cu_2$ is uniform, maximal, and inequivalent to Qn or Cu_4. Its associated subset is the S of this case.*

Case IV. *S comes from the graph* H *of Figure* 3.4 *via* (3.2).

By an argument similar to that of Case III, $G(S, L) = Sx_3 \otimes Cu_1$ is uniform and maximal, with associated subset S. Since S has 14 elements we conclude that

(4.12) *the group $Sx_3 \otimes Cu_1$ is uniform, maximal, and inequivalent to Qn, Cu_4 or $Sx_2 \otimes Cu_2$. Its associated subset is the S of this case.*

Case V. *S comes from the graph* K *of Figure* 3.4 *via* (3.2).

By (4.10), $G(S, L) = Sx_4$ is uniform and maximal, with S as its associated subset. Since S has 20 points, it is inequivalent to the preceding groups. Thus

(4.13) *the group Sx_4 is uniform, maximal and inequivalent to any of the groups in Cases* I–IV. *Its associated subset is the S of this case.*

Case VI. *S comes from the graph* C *of Figure* 3.4 *via* (3.2).

It is clear that L is the direct sum of two sublattices L_1, L_2 of rank 2, each of which is generated by β^{-1} of one of the triangles of Γ. So $S = S_1 \cup S_2$, where $S_i = S \cap L_i$ is equivalent to the set in (4.9) with $n = 2$. Hence $Sx_2 \otimes Sx_2$ is contained in $G(S, L)$. By (4.10) and Lemma 4.7, the group $Sx_2 \otimes Sx_2$ is uniform, with associated subset S. Therefore, by Observation 4.1, the group $G(S, L)$, which we denote by $Sx_2^{(2)}$, is uniform and maximal.

Since S has 12 elements, while the five preceding S's have, in order, 24, 8, 10, 14 and 20 elements, $Sx_2^{(2)}$ is inequivalent to any of the above groups. Hence

(4.14) *the group* $Sx_2^{(2)}$ *is uniform, maximal and inequivalent to any of the groups in Cases* I–V. *Its associated subset is the* S *of this case.*

Incidentally, it is clear that $Sx_2^{(2)}$ is the wreath product of the symmetric group S_2 with Sx_2 (See [5]). So its order is $(3!\,2)^2 \cdot 2 = 3^2 \cdot 2^5 = 288$.

We return to the lattice K with basis $k_0, \cdots, k_n$, and the subspaces V_1, V_2 of V_K invariant under S_{n+1}. Now let L'' be the image of K under the projection of $V_1 \dotplus V_2$ onto V_2. This is the dual lattice to L' (with respect to ϕ) and is also invariant under H. The image of k_i under this projection is

$$l_i = k_i - \frac{k_0 + \cdots + k_n}{n+1}.$$

So L'' consists of all elements of the form

(4.15) $l'' = \dfrac{r_0 k_0 + \cdots + r_n k_n}{n+1}$, *where* $r_0, \cdots, r_n$ *are integers satisfying* $r_0 + \cdots + r_n = 0$ *and* $r_0 \equiv \cdots \equiv r_n \pmod{n+1}$.

The set $S(\phi, L'')$ is more difficult to compute than some of the other such sets. Suppose l'', given by (4.15), lies in $S(\phi, L'')$. Let $r_i = (n+1)t_i + r$, where $t_i \in Z$, $i = 0, \cdots, n$, and $0 \le r < n+1$. Since $\sum r_i = 0$, we have $r = -(t_0 + \cdots + t_n)$. Thus

$$\phi(l'') = \frac{1}{(n+1)^2} \sum r_i^2 = t_0^2 + \cdots + t_n^2 - \frac{r^2}{n+1}.$$

If some integer t_i, say t_0, is different from 0 or ± 1, then the two elements corresponding to $t_0 \pm 1, t_1, \cdots, t_n, r \mp 1$ will be non-zero. So the value of ϕ at these elements must be $\ge \phi(l'')$. This tells us that

$$\phi\left(l'' \pm \left(k_0 - \frac{k_0 + \cdots + k_n}{n+1}\right)\right) = \phi(l'') \pm 2t_0 + 1 \pm \frac{2r}{n+1} - \frac{1}{n+1} \ge \phi(l'')$$

or

$$\left| t_0 + \frac{r}{n+1} \right| \le \tfrac{1}{2}\left(1 - \frac{1}{n+1}\right) < \tfrac{1}{2}.$$

But $|r/(n+1)| < 1$, and $|t_0| \ge 2$. Hence $|t_0 + r/(n+1)| \ge 1$, a contradiction. So

Each t_i *is either* 0 *or* $\pm$ 1.

Let T be the number of non-zero t_i, and T' the number of t_i equal to $+1$. Then $\phi(l'') = T - (2T' - T)^2/(n+1)$. For $0 \le T' \le T$, and fixed T, the minima of this function clearly are taken on for $T' = 0$ and $T' = T$, i.e.

All the non-zero t_i are equal.

Finally $\phi(l'') = T - T^2/(n+1) = T(n+1-T)/(n+1)$. Since $0 < T < n+1$, the minima are given by $T = 1$ and $T = n$. Therefore

(4.16) *$S(\phi, L'')$ consists of all*

$$\pm\left(k_i - \frac{k_0 + \cdots + k_n}{n+1}\right),$$

where $i = 0, \cdots, n$.

In particular, for $n \geq 2$, $S(\phi, L'')$ has $2(n+1)$ elements.

The map

$$k_i - \frac{k_0 + \cdots + k_n}{n+1} \to k_i - k_{i-1},$$

for $i = 1, \cdots, n$ sends L'' onto L and $s(\phi, L'')$ onto

$$\{\pm(k_1 - k_0), \pm(k_2 - k_1), \cdots, \pm(k_n - k_{n-1}), \pm(k_0 - k_n)\}.$$

So

(4.17) *$S(\phi, L'')$ is graphical. Its graph is a regular $(n+1)$-gon.*

As in the case of (4.10), the group $Py_n = G(S(\phi, L''), L'')$ satisfies

(4.18) *Py_n is uniform and maximal. Its associated subset is $S(\phi, L'')$.*

Case VII. *S comes from the graph* L *of Figure* 3.4 *via* (3.2).

By (4.17), it is clear that $G(\beta^{-1}(\Gamma), L_\Gamma) = Py_3$. So $G(S, L) = Py_3 \otimes Cu_1$. This is uniform and maximal with associated subset S. Since S has 10 elements, this group can be equivalent only to $Sx_2 \otimes Cu_2$ among our previous groups. But the two sets S cannot be equivalent since $N_3(\beta(s), \Gamma) = 1$ for some elements s of the earlier set, while $N_3(\beta(s), \Gamma) = 0$ for all elements s of the present set (consult Lemma 3.6). Hence

(4.19) *the group $Py_3 \otimes Cu_1$ is uniform, maximal, and inequivalent to any of the groups in cases* I–VI. *Its associated subset is the S of this case.*

Case VIII. *S comes from the graph* P *of Figure* 3.4 *via* (3.2).

Clearly $G(S, L) = Py_4$. Since S has 10 elements, this group can be equivalent only to $Sx_2 \otimes Cu_2$ or $Py_3 \otimes Cu_1$ among our previous groups. But $N_5(\beta(s), \Gamma) = 1$ for all elements s of the present S, while $N_5(\beta(s), \Gamma) = 0$ for all elements s of the two earlier S's. Hence

(4.20) *the group Py_4 is uniform, maximal and inequivalent to any of the groups in cases* I–VII. *Its associated subset is the S of this case.*

Case IX. *S is given by* (2.16).

This, of course, is the exceptional case in Theorem 2.21.

Let K be a rank three lattice with basis k_0, k_1, k_2. Let the symmetric group S_3 act on K as in the study of Cu_2. Then the direct product $S_3 \otimes S_3$ acts naturally on the tensor product (over Z) $K \otimes K$. The sublattice L' consisting of all $r_0 k_0 + r_1 k_1 + r_2 k_2 \in K$ with $r_0 + r_1 + r_2 = 0$ is invariant under S_3. The subspace V_2 spanned by L' is absolutely irreducible under S_3. So the subspace W spanned by $L' \otimes L' \subseteq K \otimes K$ is absolutely irreducible under $S_3 \otimes S_3$. In particular, the group H' of automorphisms of $L' \otimes L'$ induced by $S_3 \otimes S_3$ is uniform.

The form $\phi(\sum_{ij} X_{ij} k_i \otimes k_j) = \sum_{ij} X_{ij}^2$ on $K \otimes K$ is clearly invariant under $S_3 \otimes S_3$. So its restriction to $L' \otimes L'$ is an associated form of H'. The sublattice $L' \otimes L'$ consists of all $\sum_{i,j} r_{ij} k_i \otimes k_j$ such that all r_{ij} lie in Z, and, for each i, $\sum_j r_{ij} = 0$, while, for each j, $\sum_i r_{ij} = 0$. Therefore, if some coefficient r_{ij} is not zero, then at least one other coefficient r_{ik} is not zero, and at least one other coefficient r_{lj} is not zero. Clearly this forces at least four r_{ij} to be non-zero. Hence $l \in L' \otimes L'$, $l \neq 0$ imply $\phi(l) \geq 4$. Equality occurs if and only if

$$\begin{aligned} l &= k_i \otimes k_j - k_i \otimes k_l - k_h \otimes k_j + k_h \otimes k_l \\ &= (k_i - k_h) \otimes (k_j - k_l), \qquad i \neq h, j \neq l. \end{aligned} \tag{4.21}$$

So the associated subset S' of H' consists of the 18 elements (4.21).

Map L onto L' by

$$\begin{aligned} s_1 &\to (k_0 - k_1) \otimes (k_0 - k_1) \\ s_2 &\to (k_0 - k_2) \otimes (k_1 - k_2) \\ s_3 &\to (k_0 - k_1) \otimes (k_0 - k_2) \\ s_4 &\to (k_0 - k_2) \otimes (k_0 - k_2). \end{aligned}$$

Then the other elements of S are mapped as follows:

$$\begin{aligned} s_1 - s_3 &\to (k_0 - k_1) \otimes (k_2 - k_1) \\ s_3 - s_4 &\to (k_2 - k_1) \otimes (k_0 - k_2) \\ s_2 - s_4 &\to (k_0 - k_2) \otimes (k_1 - k_0) \\ s_1 + s_2 - s_3 &\to (k_2 - k_1) \otimes (k_2 - k_1) \\ s_1 + s_2 - s_4 &\to (k_1 - k_2) \otimes (k_1 - k_0); \end{aligned}$$

i.e., S is mapped onto S'. So $G(S, L)$ is equivalent to the group $Sx_2^{\otimes 2} = G(S', L' \otimes L')$. Since H' is uniform, $Sx_2^{\otimes 2}$ is uniform and maximal, by Observation 4.1. Since S' has 18 elements, while the associated subsets of our eight previous groups have, in order, 24, 8, 10, 14, 20, 12, 10 and 10 elements, Observation 4.2 implies that

(4.22) *The group $Sx_2^{\otimes 2}$ is uniform, maximal, and inequivalent to any of the groups in Cases* I–VIII. *Its associated subset is the S of this case.*

Case X. *S comes from the graph* N *of Figure* 3.4 *via* (3.2).

This is the only subset which does not lead to a maximal group.

S consists of the six elements

$$s_1, \quad s_2, \quad s_3, \quad -(s_1 + s_2 + s_3), \quad s_4, \quad -(s_1 + s_2 + s_4)$$

and their negatives, where $s_1, \cdots, s_4$ are the basis for L. Rename these elements, in order,

$$u_{11}, \quad u_{12}, \quad u_{21}, \quad u_{22}, \quad u_{31}, \quad u_{32}. \tag{4.23}$$

Then the only relations of the form $X_1 + X_2 + X_3 + X_4 = 0$, where $\pm X_1, \cdots, \pm X_4$ are *eight distinct* elements of S are the six relations

$$u_{i1} + u_{i2} - u_{j1} - u_{j2} = 0, \qquad i \neq j, i, j = 1, 2, 3. \tag{4.24}$$

Consider $G(S, L)$ as a permutation group on S. It must permute the six expressions on the left of (4.24) among themselves. This implies directly that any element of $G(S, L)$ either permutes the elements (4.23) among themselves, or carries this entire set into its negative. So $G(S, L) = G \otimes (\pm 1)$ where G is the subgroup sending (4.23) into itself.

It is also clear from (4.24) that the subsets $\{u_{11}, u_{12}\}$, $\{u_{21}, u_{22}\}$, $\{u_{31}, u_{32}\}$ form a system of imprimitivity for G. So G permutes among themselves the 12 elements

$$\begin{aligned} u_{i1} - u_{j1} = u_{j2} - u_{i2}, \qquad u_{i1} - u_{j2} = u_{j1} - u_{j2}, \\ u_{i2} - u_{j1} = u_{j2} - u_{i1}, \qquad i \neq j, i, j = 1, 2, 3. \end{aligned} \tag{4.25}$$

Let S' be the union of S and the elements (4.25). Since $S' = -S'$, we know that $G(S, L) = G \otimes \{\pm 1\} \subseteq G(S', L)$.

Map L onto the ring I of integral quaternions by

$$\begin{aligned} u_{11} &\rightarrow (1 + i + j + k)/2 \\ u_{21} &\rightarrow (1 - i + j + k)/2 \\ u_{31} &\rightarrow 1 \\ u_{32} &\rightarrow k. \end{aligned}$$

The other elements of S are mapped into

$$\begin{aligned} u_{12} &\rightarrow (1 - i - j + k)/2 \\ u_{22} &\rightarrow (1 + i - j + k)/2 \end{aligned}$$

The elements (4.25) are mapped as follows:

$$\begin{aligned} u_{11} - u_{21} &\rightarrow i \\ u_{11} - u_{31} &\rightarrow (-1 + i + j + k)/2 \\ u_{21} - u_{31} &\rightarrow (-1 - i + j + k)/2 \\ u_{11} - u_{22} &\rightarrow j \\ u_{11} - u_{32} &\rightarrow (1 + i + j - k)/2 \\ u_{21} - u_{32} &\rightarrow (1 - i + j - k)/2. \end{aligned}$$

Hence S' maps onto U. So $G(S', L)$ is equivalent to $G(U, I) = Qn$. Since Qn is transitive on U, the group $G(S', L)$ is transitive on S'. But $G(S, L)$ isn't. So $G(S, L) \subset G(S', L)$; i.e.

(4.26) *in this case, $G(S, L)$ is not maximal.*

Having considered all ten cases, we conclude from (4.3), (4.6), (4.11), (4.12), (4.13), (4.14), (4.19), (4.20), (4.22) and (4.26) the following result:

THEOREM 4.27. *There are precisely nine inequivalent maximal finite groups of* 4×4 *integral matrices. They are all uniform. In the notation of this section they are, with their invariant forms:*

Qn	$X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_1X_4 + X_2X_4 + X_3X_4$
Cu_4	$X_1^2 + X_2^2 + X_3^2 + X_4^2$
$Sx_2 \otimes Cu_2$	$X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_1X_2$
$Sx_3 \otimes Cu_1$	$X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_1X_2 + X_1X_3 + X_2X_3$
Sx_4	$X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4$
$Sx_2^{(2)}$	$X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_1X_2 + X_3X_4$
$Py_3 \otimes Cu_1$	$3X_1^2 + 3X_2^2 + 3X_3^2 + X_4^2 - 2X_1X_2 - 2X_1X_3 - 2X_2X_3$
Py_4	$2X_1^2 + 2X_2^2 + 2X_3^2 + 2X_4^2 - X_1X_2 - X_1X_3 - X_1X_4 - X_2X_3 - X_2X_4 - X_3X_4$
$Sx_2^{\otimes 2}$	$2X_1^2 + 2X_2^2 + 2X_3^2 + 2X_4^2 + 2X_1X_2 + 2X_1X_3 + X_1X_4 + X_2X_3 + 2X_2X_4 + 2X_3X_4$.

REFERENCES

1. H. MINKOWSKI, *Über positive quadratische Formen, Collected Works*, B. G. Teubner, 1911, vol. I, pp. 149–156. (Originally J. Reine Angew. Math., vol. 99 (1886), pp. 1–9.)
2. ———, *Zur Theorie der positiven quadratischen Formen, Collected Works*, B. G. Teubner, 1911, vol. I, pp. 212–218. (Originally J. Reine Angew. Math., vol. 101 (1887), pp. 196–202.)
3. ———, *Sur la reduction des formes quadratiques positives quaternaires, Collected Works*, B. G. Teubner, 1911, vol. I, p. 195. (Originally, with misprints, Comptes Rendus, vol. 96 (1883), p. 1205.)
4. G. H. HARDY AND E. M. WRIGHT, *The theory of numbers*, 3rd edition, Oxford, 1954, p. 305.
5. E. DADE, *Integral systems of imprimitivity*, Math. Ann., vol. 154 (1964), pp. 383–386.

CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA