ON THE CLIFFORD COLLINEATION, TRANSFORM AND SIMILARITY GROUPS (IV)

AN APPLICATION TO QUADRATIC FORMS

G. E. WALL

To RICHARD BRAUER on his 60th birthday

1. Introduction

E. S. Barnes and I recently[1] constructed a series of positive quadratic forms f_N in $N=2^n$ variables $(n=1, 2, \dots)$ with relative minima of order $N^{\frac{1}{2}}$ for large N. I continue this investigation by determining the minimal vectors of f_N and showing that, for $N \neq 8$, its group of automorphs is the Clifford group[2] $\mathscr{C}\mathscr{T}_1^+(2^n)$ (§3). This suggests a generalization. Replacing $\mathscr{C}\mathscr{T}_1^+(2^n)$ by $\mathscr{C}\mathscr{T}(p^n)$, where p is an odd prime, I derive a new series of positive forms in $N=(p-1)p^n$ variables (§4). The relative minima are again of order $N^{\frac{1}{2}}$ (p fixed, $N\to\infty$), the "best" forms being those for $p=3,5$. All forms are eutactic though only those for $p=3,5$ are extreme.

The methods used here raise several questions. Firstly, the forms constructed have fairly big relative minima while the representations of the symplectic group $Sp(2n, p)$ associated with $\mathscr{C}\mathscr{T}(p^n)$ are of smallest possible degree (CGI, theorem 10). Are these two facts directly related? Secondly, it is natural to regard the lattice introduced in §4.2 as a commutative algebra. Is there a simple direct relation between this algebra and the automorph group $\mathscr{C}\mathscr{T}(p^n)$?

2. Preliminaries

The notation used in this paper is a compromise between that of EF and that of CGI, CGII. See in particular §2.1–2.3 below.

2.1. Vector spaces and groups over $GF(p)$.

Throughout this paper, p stands for a fixed prime and n for a fixed natural

Received Nov. 22, 1961.

1) Cf. [1]. This paper is referred to as EF.

2) Cf. [2], [3]. These papers are referred to as CGI, CGII.

number. $V=V_n(p)$ denotes the vector space of all row vectors $\alpha=(\alpha_1, \ldots, \alpha_n)$ over the Galois field $GF(p)$. V_r stands generically for an r-dimensional subspace of V, C_r for a coset $\alpha+V_r$.

It is easily proved that each function $f(\alpha)$ defined on V and with values in $GF(p)$ coincides in value with a unique polynomial $P(\alpha_1, \ldots, \alpha_n)$ of degree $<p$ in each α_i. Such polynomials will be called *standard*. The *degree* of f is defined as the total degree of P.

Let $p=2$. Consider the $2n$-dimensional quadratic form $\phi(\lambda)=\sum_1^n \lambda_i\lambda_{n+i}$ over $GF(2)$, where λ is the row vector (λ_i) $(i=1, \ldots, 2n)$. The ($2n$-rowed) matrices[3] T which leave $\phi(\lambda)$ invariant, i.e., $\phi(\lambda)=\phi(\lambda T')$, form the *orthogonal group* $O_1(2n, 2)$. Let

$$T=\begin{pmatrix} P & Q \\ R & S \end{pmatrix} \qquad (P, Q, R, S \ n\times n \text{ matrices}) \tag{2.1.1}$$

$$d_T = \text{rank } R.$$

The T such that d_T is even form the *rotation subgroup* $O_1^+(2n, 2)$.

Let $p>2$. Consider the $2n$-dimensional alternate bilinear form

$$f(\lambda, \mu)=\sum_1^n(\lambda_i\mu_{n+i}-\mu_i\lambda_{n+i})$$

over $GF(p)$. The matrices T which leave $f(\lambda, \mu)$ invariant, i.e., $f(\lambda, \mu)=f(\lambda T', \mu T')$ form the *symplectic group* $Sp(2n, p)$. The notation (2.1.1) will also be used for the elements of Sp.

2.2. Vector spaces and groups over the cyclotomic field P.

Let R_0 denote the rational field, P the p-th cyclotomic field: $P=R_0(\omega)$, where $\omega=\exp(2\pi i/p)$. Then $E=E_{p^n}$ denotes a p^n-dimensional vector space over P. We choose a fixed basis of E, indexing its p^n members $\mathbf{e}_\alpha$ with the p^n elements α of V. We use the notations

$$\mathbf{x}=(x_\alpha)=\sum x_\alpha \mathbf{e}_\alpha$$

for the elements of E.

The *scalar product* on E is defined by

3) The transpose of a matrix T in denoted by T'.

$$(x_\alpha)\cdot(y_\alpha)=\sum_{\alpha\in V}\bar{x}_\alpha y_\alpha.$$

The terms *unitary* ($p>2$), *orthogonal* ($p=2$) are interpreted accordingly.

Let $p=2$. The Clifford transform group $\mathscr{C}\mathscr{T}_1^+(2^n)$[4] is a group of orthogonal transformations on E. There exists a homomorphism of $\mathscr{C}\mathscr{T}_1^+(2^n)$ onto $O_1^+(2n, 2)$ such that each original of $T\in O_1^+$ has the form[5]

$$Xe_\alpha=2^{-\frac{1}{2}d_T}\sum_{\beta\in C}(-1)^{f(\beta)}e_\beta, \tag{2.2.1}$$

where C is a coset of dimension d_T, f a function of degree ≤ 2. For each function $g(\alpha)$ of degree ≤ 2, non-singular $n\times n$ matrix D over $GF(2)$ and vector $\mathbf{t}\in V$, the linear transformation[6]

$$Ye_\alpha=(-1)^{g(\alpha)}e_{\alpha D+\mathbf{t}} \tag{2.2.2}$$

belongs to $\mathscr{C}\mathscr{T}_1^+$.

Let $p>2$. The Clifford transform group $CT(p^n)$ was defined in CGI §3.1. We define $\mathscr{C}\mathscr{T}(p^n)$ as the commutator group of $CT(p^n)$ when $p^n>3$, as the group $\{Y, Z\}\mathscr{C}\mathscr{G}$ in CGI Appendix, section (4), when $p^n=3$. $\mathscr{C}\mathscr{T}(p^n)$ is a group of unitary transformations on E. There exists a homomorphism of $\mathscr{C}\mathscr{T}(p^n)$ onto $Sp(2n, p)$ such that each original of $T\in Sp$ has the form[7]

$$Xe_\alpha=\pm\theta^{-d_T}\sum_{\beta\in C}\omega^{f(\beta)}e_\beta, \tag{2.2.3}$$

where C is a coset of dimension d_T, f a function of degree ≤ 2 and

$$\theta=\sum_{i=0}^{p-1}\omega^{i^2}. \tag{2.2.4}$$

For each function $g(\alpha)$ of degree ≤ 2, non-singular $n\times n$ matrix D over $GF(p)$ and vector $\mathbf{t}\in V$, the linear transformation[8]

$$Ye_\alpha=\omega^{g(\alpha)}e_{\alpha D+\mathbf{t}} \tag{2.2.5}$$

belongs to $\mathscr{C}\mathscr{T}$.

---

4) Defined in CGII §3.3., *for* $n\geq 3$ *only*, as the commutator group of $CT(2^n)$. A universal definition is that $\mathscr{C}\mathscr{T}_1^+(2^n)$ consists of the elements in CGII (5.10) corresponding to the elements T of $O_1^+(2n, 2)$.

5) See CGII (5 10) and (5.5).

6) These are the elements in CGII (5.10) corresponding to $d_T=0$.

7) See CGI (3.1.1) and (4.1.6).

8) These are the elements of $\mathscr{C}\mathscr{T}$ corresponding to the T with $d_T=0$.

2.3. Lattices. Let Ω denote the ring of all integers in P. We define an Ω-*lattice* as the set of all integral linear combinations

$$\sum \xi_\alpha \mathbf{u}_\alpha \qquad (\xi_\alpha \in \Omega)$$

of p^n linearly independent vectors $\mathbf{u}_\alpha$. In particular, $\Gamma = \Gamma_{p^n}$ denotes the Ω-lattice of all integral vectors

$$\sum x_\alpha \mathbf{e}_\alpha \qquad (x_\alpha \in \Omega).$$

If Λ_1, Λ_2 are Ω-lattices and $\Lambda_1 \subset \Lambda_2$, the grouptheoretical index $|\Lambda_2 : \Lambda_1|$ is finite. In particular, if $\lambda(\neq 0) \in \Omega$, we have

$$|\Gamma : \lambda\Gamma| = |N(\lambda)|^{p^n},$$

where $N(\lambda)$ is the norm of λ in P relative to R_0. For, if $\mathbf{x}$, $\mathbf{y} \in \Gamma$ then $\mathbf{x} \equiv \mathbf{y} \pmod{\lambda\Gamma}$ if, and only if, $x_\alpha \equiv y_\alpha \pmod{\lambda}$ for each $\alpha \in V$.

Let Λ be an Ω-lattice such that $\lambda\Gamma \subset \Lambda \subset \Gamma$, where $\lambda(\neq 0) \in \Omega$. We define the *dual* Λ' *of* Λ *modulo* λ as follows: Λ' is the set of $\mathbf{x} \in E$ such that $\mathbf{x} \cdot \mathbf{y} \in \lambda\Omega$ for all $\mathbf{y} \in \Lambda$. Since $\lambda\Gamma \subset \Lambda \subset \Gamma$, we have $\bar{\lambda}\Gamma \subset \Lambda' \subset \Gamma$. The argument of EF § 2 shows that Λ' is an Ω-lattice, that Λ is the dual of Λ' modulo $\bar{\lambda}$ and that

$$(2.3.1) \qquad |\Gamma : \Lambda| \, |\Gamma : \Lambda'| = |\Gamma : \lambda\Gamma| = N(\lambda)|^{p^n}.$$

It is a well known theorem that every finitely generated module over a principal ideal ring has a basis. The following variant is proved in exactly the same way.

LEMMA 2.3.1. *Let $\lambda(\neq 0) \in \Omega$ and suppose that every divisor of the principal ideal with generator λ is principal. Then every Ω-module M such that $\lambda\Gamma \subset M \subset \Gamma$ is an Ω-lattice.*

2.4. Criteria for quadratic functions on $V_n(2)$.

In the present section, $p = 2$ and $f(\alpha)$ is a function defined on V with values in $GF(2)$. If $W \subset V$, we write

$$(2.4.1) \qquad \langle W; f \rangle = \sum_{\alpha \in W} (-1)^{f(\alpha)}.$$

As stated in § 2.1., f has a unique expression in the form

$$(2.4.2) \qquad f(\alpha) = \sum_S a_S \alpha_S \qquad (a_S \in GF(2),\ \alpha_S = \prod_{i \in S} \alpha_i),$$

where summation is over the subsets (including the empty set) of $1, 2, \ldots, n$.

We note that, since $\alpha^2=\alpha$ on $GF(2)$, the degree of $f(\boldsymbol{\alpha})$ is ≤ 2 if, and only if, the function $g(\boldsymbol{\alpha})=f(\boldsymbol{\alpha})+f(\mathbf{0})$ is a quadratic form.

LEMMA 2.4.1. *The degree of $f(\boldsymbol{\alpha})$ is ≤ 2 if, and only if, $f(\boldsymbol{\alpha})$ has an even number of zeros in every $V_3 \subset V$.*

Proof. The following conditions for a scalar-valued function $h(\mathbf{u})$ on a vector space to be a quadratic form are well known:

(i) the function $k(\mathbf{u}, \mathbf{v})=h(\mathbf{u}+\mathbf{v})-h(\mathbf{u})-h(\mathbf{v})$ is bilinear, and

(ii) $h(\lambda\mathbf{u})=\lambda^2 h(\mathbf{u})$.

It follows that h is a quadratic form if, and only if, its restriction to every subspace of dimension ≤ 3 is a quadratic form. It is therefore sufficient to prove our lemma for $n \leq 3$. For $n \leq 2$, the lemma is obvious from (2.4.2). For $n=3$, it follows from the formula $\sum_{\boldsymbol{\alpha}\in V} f(\boldsymbol{\alpha})=a_{(1,2,3)}$.

COROLLARY. *The degree of $f(\boldsymbol{\alpha})$ is ≤ 2 if, and only if,*

$$\langle V_3 ;\, f\rangle \equiv 0 \pmod 4 \text{ for every } V_3 \subset V. \tag{2.4.3}$$

We suppose from now on that the degree of $f(\boldsymbol{\alpha})$ is ≤ 2. Let $q(\boldsymbol{\alpha})=f(\boldsymbol{\alpha})+f(\mathbf{0})$ be the corresponding quadratic form. The *polar form* of q is the bilinear form

$$Q(\boldsymbol{\alpha}, \boldsymbol{\beta})=q(\boldsymbol{\alpha}+\boldsymbol{\beta})+q(\boldsymbol{\alpha})+q(\boldsymbol{\beta}).$$

Since Q is alternate ($Q(\boldsymbol{\alpha}, \boldsymbol{\alpha}) \equiv 0$) its rank is even, say $2d$. We call d the *reduced rank* of f.

LEMMA 2.4.2. *Suppose that $f(\boldsymbol{\alpha})$ has degree ≤ 2, reduced rank $\leq D$. Then, for each $V_k \subset V$ $(0 \leq k \leq n)$,*

$$\langle V_k ;\, f\rangle \equiv 0 \pmod{2^t}, \tag{2.4.4}$$

where[9] $t=\max\left(\left[\frac{1}{2}(k+1)\right], k-D\right)$.

Proof. Let d be the reduced rank of f. Then $q(\boldsymbol{\alpha})=f(\boldsymbol{\alpha})+f(\mathbf{0})$ is equivalent[10] to one of

$$q_1(\boldsymbol{\alpha})=\sum_1^d \alpha_i \alpha_{d+i}, \quad q_2(\boldsymbol{\alpha})=q_1(\boldsymbol{\alpha})+\alpha_1+\alpha_{d+1}, \quad q_3(\boldsymbol{\alpha})=q_1(\boldsymbol{\alpha})+\alpha_{2d+1}.$$

---

9) $[r]$ = integral part of r.

10) See e.g., Dieudonné [6].

The number of zeros of $q(\alpha)$ is accordingly

$$2^{n-1}+\varepsilon 2^{n-d-1} \qquad (\varepsilon=1,\ -1 \text{ or } 0)$$

and so $\langle V;\, f\rangle=\varepsilon 2^{n-d}$. Therefore

$$\langle V;\, f\rangle\equiv 0 \pmod{2^{n-d}}$$

and, since $d\leq\frac{1}{2}n$,

$$\langle V;\, f\rangle\equiv 0 \pmod{2^{[\frac{1}{2}(n+1)]}}.$$

Applying the last two congruences to the restriction $\bar{f}$ of f to V_k and noting that the reduced rank of $\bar{f}$ cannot exceed that of f we get the lemma.

LEMMA 2.4.3. *Suppose that $f(\alpha)$ has degree ≤ 2, reduced rank d. Let D be an integer such that $0\leq D\leq\frac{1}{2}n$. If*

(2 4.5) $\qquad \langle V_{2D+2};\, f\rangle\equiv 0 \pmod{2^{D+2}}$ *for every* $V_{2D+2}\subset V$,

then $d\leq D$.

In fact, if d were $>D$, the restriction of $q(\alpha)$ to a suitable V_{2D+2} would be equivalent to $\sum_1^{D+1}\alpha_i\alpha_{D+1+i}$; but then $\langle V_{2D+2};\, f\rangle=\pm 2^{D+1}$, contrary to (2.4.5).

We shall later have to consider functions $h(\alpha)$ defined on a coset $\mathbf{a}+V_k$ rather than the whole of V. The degree and reduced rank of h are defined to be those of the function $l(\beta)=h(\mathbf{a}+\beta)$, whose domain of definition is the subspace V_k.

3. Lattices of dimension 2^n

We suppose throughout this section that $p=2$. The minimal vectors of the lattices $\Lambda(\lambda)$ are determined in §3.1, the automorphs of the "principal" lattices $\Lambda^{(1)}$, $\Lambda^{(2)}$ in §3.2.

We recall the definition of $\Lambda(\lambda)$ (EF §3). $(\lambda)=(\lambda_0,\ldots,\lambda_n)$ is a set of integral indices satisfying

(3.0.1) $\qquad \lambda_0=0,\ \lambda_r-1\leq\lambda_{r-1}\leq\lambda_r \quad \text{for} \quad 1\leq r\leq n,$

and $\Lambda(\lambda)$ is the lattice formed by all integral linear combinations of the vectors

$$2^{\lambda_{n-r}}[C_r]=2^{\lambda_{n-r}}\sum_{\alpha\in C_r}\mathbf{e}_\alpha,$$

where C_r runs over all cosets in V.

If $W \subset V$ and $f(\alpha)$ is a function defined on W with values in $GF(2)$, we write

(3.0.2) $$[W;\, f] = \sum_{\alpha \in W} (-1)^{f(\alpha)} \mathbf{e}_\alpha .$$

3.1. Minimal vectors of $\Lambda(\lambda)$. Let x be a minimal vector of $\Lambda = \Lambda(\lambda)$. By theorem 3.2. of EF,

(3.1.1) $$\mathbf{x}^2 \approx 2^m, \text{ where } m = \min\,(n - r + 2\lambda_r),$$

and x *has the form*

(3.1.2) $$\mathbf{x} = 2^{\lambda_R}[W;\, f],$$

where R satisfies

(3.1.3) $$n - R + 2\lambda_R = m, \qquad 0 \leq R \leq n,$$

and W is a subset of V with 2^{n-R} elements.

We now complete this partial characterization by giving the conditions that a vector of the form (3.1.2) belong to Λ.

THEOREM 3.1. *Let R be an integer satisfying* (3.1.3), *W a subset of V with 2^{n-R} etements, $f(\alpha)$ a function defined on W with values in $GF(2)$. Let d be the largest integer such that*

(3.1.4) $$\lambda_{R+k} = \lambda_R + \left[\frac{1}{2}(k+1)\right] \quad \textit{for} \quad 0 \leq k \leq 2d.$$

Then the vector $2^{\lambda_R}[W;\, f] \in \Lambda(\lambda)$ if, and only if,

(i) *W is a coset C_{n-R}, and*

(ii) *$f(\alpha)$ has degree ≤ 2, reduced rank $\leq d$.*

Proof. Lemma 3.3 of EF can be sharpened by adding the following conditions for equality:

If precisely 2^{n-s} coordinates x_α are odd, the corresponding α form a coset C_{n-s}.

The proof is straightforward and is omitted. This sharper form of the lemma shows that (i) is a necessary condition.

We may now suppose that W is a coset, or even a *subspace* V_{n-R}, because the results for cosets can easily be deduced by translation of coordinates. Now, each $V_k \subset V_{n-R}$ is the meet of V_{n-R} with some $V_{k+R} \subset V$ but not the meet of V_{n-R} with any V_{k+R+u}, $u>0$. Therefore, by theorem 3.1 of EF, the vector $\mathbf{x}=2^{\lambda_R}[W; f] \in \Lambda$ if, and only if,

$$(3.1.5) \qquad \langle V_k;\, f\rangle \equiv 0 \pmod{2^{\mu_k}} \text{ for every } V_k \subset V_{n-R},$$

where $\mu_k = \lambda_{R+k} - \lambda_R$. We remark that, by (3.1.4),

$$(3.1.6) \qquad \mu_k = \left[\frac{1}{2}(k+1)\right] \quad \text{for} \quad 0 \leq k \leq 2d,$$

and that, by (3.0.1) and (3.1.1),

$$(3.1.7) \qquad \mu_{2d+2} = d+2 \textit{ if } 2d+2 \leq n-R,$$

$$(3.1.8) \qquad \left[\frac{1}{2}(k+1)\right] \leq \mu_k \leq k-d \qquad \text{for} \qquad 2d \leq k \leq n-R.$$

Suppose now that $\mathbf{x} \in \Lambda$. By (3.1.5), (3.1.6) and (3.1.8),

$$\langle V_3;\, f\rangle \equiv 0 \pmod 4 \text{ for every } V_3 \subset V_{n-R},$$

so that, by the corollary to lemma 2.4.1, the degree of $f \leq 2$. Again, by (3.1.5) and (3.1.7),

$$\langle V_{2d+2};\, f\rangle \equiv 0 \pmod{2^{d+2}} \text{ for every } V_{2d+2} \subset V_{n-R},$$

so that, by lemma 2.4.3, the reduced rank of $f \leq d$.

Conversely, suppose that f has degree ≤ 2, reduced rank $\leq d$. If $k \leq 2d$, (3.1.5) holds by lemma 2.4.2 and (3.1.6). If $k>2d$, (3.1.5) holds by lemma 2.4.2 and (3.1.8). Hence $\mathbf{x} \in \Lambda$. This proves our theorem.

A straightforward enumeration of the quadratic functions of given reduced rank yields the total number of minimal vectors of rank R stated in (5.10) of EF.

3.2. Automorphs of the principal lattices. The first and second *principal lattices* $\Lambda^{(1)}$, $\Lambda^{(2)}$ of dimension $N=2^n$ are the $\Lambda(\lambda)$ given by

$$(3.2.1) \qquad \lambda_r = \left[\frac{1}{2}r\right] \quad \text{and} \quad \left[\frac{1}{2}(r+1)\right] \quad (0 \leq r \leq n)$$

respectively. They occupy a special position in that their (common) relative minimum $\left(\frac{1}{2}N\right)^{\frac{1}{2}}$ exceeds that of any other $\Lambda(\lambda)$ of dimension N.

The fact that $\Lambda^{(1)}$, $\Lambda^{(2)}$ are dual modulo 2^n implies that *they have the same group of automorphs*. Suppose e.g. that X is an automorph of $\Lambda^{(1)}$. If $\mathbf{x}\in\Lambda^{(1)}$, $\mathbf{y}\in\Lambda^{(2)}$, then

$$\mathbf{x}\cdot X\mathbf{y}=X^{-1}\mathbf{x}\cdot\mathbf{y}\equiv 0 \pmod{2^n}.$$

Since this holds for all $\mathbf{x}\in\Lambda^{(1)}$, $X\mathbf{y}\in\Lambda^{(2)}$. Since $X\mathbf{y}\in\Lambda^{(2)}$ whenever $\mathbf{y}\in\Lambda^{(2)}$, X is an automorph of $\Lambda^{(2)}$. The common group of automorphs is denoted by $\mathfrak{A}$.

By § 3.1, the minimal vectors of $\Lambda^{(1)}$ (n odd), $\Lambda^{(2)}$ (n even) are

$$2^{[\frac{1}{2}n]-s}[C_{2s};\,f], \tag{3.2.2}$$

where C_{2s} runs over all even-dimensional cosets in V, f over all functions of degree ≤ 2 on C_{2s}; and those of $\Lambda^{(1)}$ (n even), $\Lambda^{(2)}$ (n odd) are

$$2^{[\frac{1}{2}(n+1)]-s}[C_{2s+1};\,f], \tag{3.2.3}$$

where C_{2s+1} runs over all odd-dimensional cosets in V, f over all functions of degree ≤ 2 on C_{2s+1}.

THEOREM 3.2. *If* $n\neq 3$, $\mathfrak{A}=\mathscr{C}\mathscr{T}_1^+(2^n)$. *If* $n=3$, $\mathfrak{A}\cong[3^{4,2,1}]$ (in the notation of Coxeter and Moser [5]) *and* $\mathscr{C}\mathscr{T}_1^+(2^3)$ *is a subgroup of* $\mathfrak{A}$ *of index* 270.

Proof. Let M_s denote the set of vectors (3.2.2) of fixed dimension $2s$, M the union of all the M_s. Write $\mathbf{u}_0=2^{[\frac{1}{2}n]}\mathbf{e}_0$. We first prove that

(3.2.4) *M is the set of all vectors* $X\mathbf{u}_0$ ($X\in\mathscr{C}\mathscr{T}_1^+$).

By (2.2.1), $X\mathbf{u}_0\in M$ if $X\in\mathscr{C}\mathscr{T}_1^+$. By (2.2.2) $\mathscr{C}\mathscr{T}_1^+$ permutes the vectors in each M_s transitively. It remains to prove that for each s there is an $X\in\mathscr{C}\mathscr{T}_1^+$ such that $X\mathbf{u}_0\in M_s$, i.e., by (2.2.1), that there is a $T\in O_1^+$ such that $d_T=2s$. The matrix T defined as follows satisfies the requirement:

$$\left.\begin{array}{l}\boldsymbol{\lambda}\mathbf{T}'=\boldsymbol{\mu},\ \text{where}\\ \lambda_i=\mu_{n+i},\ \mu_i=\lambda_{n+i}\quad(1\leq i\leq 2s)\\ \lambda_i=\mu_i,\ \lambda_{n+i}=\mu_{n+i}\quad(2s<i\leq n).\end{array}\right\}$$

This proves (3.2.4).

Let $\mathfrak{A}_0$ be the group formed by the automorphs which leave $\mathbf{u}_0$ fixed. By (3.2.4),

$$\mathfrak{A} = (\mathscr{C}\mathscr{T}_1^+)\mathfrak{A}_0.$$

Assuming that $n \neq 3$, we now prove that $\mathfrak{A} = \mathscr{C}\mathscr{T}_1^+$ by showing that

(3.2.5) $$\mathfrak{A}_0 \subset \mathscr{C}\mathscr{T}_1^+.$$

We consider three cases.

(a) $n=1$. $M = [\pm \mathbf{e}_0, \pm \mathbf{e}_1]$, so that $\mathfrak{A}$ consists of the 8 symmetries of the square. O_1^+ is the identity group, so that $\mathscr{C}\mathscr{T}_1^+$ consists of the 8 linear transformations (2.2.2). Hence $\mathfrak{A} = \mathscr{C}\mathscr{T}_1^+$.

(b) $n=2$. The elements of $\mathfrak{A}_0 \cap \mathscr{C}\mathscr{T}_1^+$ are the 48 linear transformations (2.2.2) such that $\mathbf{t}=\mathbf{0}$, $g(\mathbf{0})=0$. On the other hand, $\mathfrak{A}_0$ permutes the elements of M orthogonal to $\mathbf{u}_0$, viz.,

$\pm 2\,\mathbf{e_a}$, $\pm 2\,\mathbf{e_b}$, $\pm 2\mathbf{e_c}$ ($\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ the non-zero elements of V),

so that the order of $\mathfrak{A}_0$ is at most 48. Hence $\mathfrak{A}_0 = \mathfrak{A}_0 \cap \mathscr{C}\mathscr{T}_1^+ \subset \mathscr{C}\mathscr{T}_1^+$.

(c) $n \geq 4$. We call C_{2s} the *carrier* of the vector (3.2.2). Let N_s denote the set of vectors in M_s whose carriers are subspaces, N the union of all the N_s. If $\mathbf{v} \in M$, we have

$$\mathbf{u}_0 \cdot \mathbf{v} = \left.\begin{matrix} 0 & (\mathbf{v} \notin N) \\ 2^{2[\frac{1}{2}n]-s} & (\mathbf{v} \in N_s) \end{matrix}\right\}$$

so that $\mathfrak{A}_0$ permutes the elements of each N_s.

Suppose now that

$$X \in \mathfrak{A}_0,\ \mathbf{v}_i \in N_1,\ X\mathbf{v}_i = \mathbf{w}_i \qquad (i = 1, 2, \ldots),$$

and let V_2^i, W_2^i be the (2-dimensional) carriers of $\mathbf{v}_i$, $\mathbf{w}_i$ respectively. Since

$2^{2-2[\frac{n}{2}]}\mathbf{v}_i \circ \mathbf{v}_j \equiv 0$ or $1 \pmod 2$ according as $V_2^i \cap V_2^j \neq (\mathbf{0})$ or $= (\mathbf{0})$,

it follows that

(3.2.6) $$V_2^i \cap V_2^j = (\mathbf{0}) \textit{ if, and only if, } W_2^i \cap W_2^j = (\mathbf{0}).$$

Now, since $n > 3$, a 2-dimensional subspace is uniquely determined by the set of 2-dimensional subspaces which meet it in the zero subspace $(\mathbf{0})$. Therefore, by (3.2.6),

(3.2.7) $$V_2^i = V_2^j \textit{ if, and only if, } W_2^i = W_2^j.$$

Thus, X maps the set of elements of N with fixed carrier V_2 onto the set of elements of N with a fixed carrier W_2 which depends only on V_2.

It now follows from case (b) that X has the form

$$X\mathbf{e}_\alpha = (-1)^{g(\alpha)}\mathbf{e}_{\pi(\alpha)},$$

where π is a mapping of V onto itself whose restriction to each V_2 is a non-degenerate linear mapping into V. It follows that π is a non-singular linear transformation on V. Also, since $[V]$ is a vector (3.2.2) or (3.2.3), $X[V]$ has the form $[V;\ f]$ for some function f of degree ≤ 2. Hence g has degree ≤ 2 and so, by (2.2.2), $X \in \mathscr{C}\mathscr{T}_1^+$. This proves (3.2.5).

We mention briefly the case $n=3$. $\mathfrak{A}$ has a subgroup isomorphic to $[3^{4,2,1}]$ (Coxeter and Moser [5], § 9.4). On the other hand, an argument on the lines of (c) above shows that $\mathfrak{A}$ and $[3^{4,2,1}]$ have the same order. Hence $\mathfrak{A} \cong [3^{4,2,1}]$.

4. Lattices of dimension $(p-1)p^n$

We pass now to the case $p>2$. Given the relation of $\mathscr{C}\mathscr{T}_1^+$ to $\Lambda^{(1)}$, and the similarity in form between the elements of $\mathscr{C}\mathscr{T}_1^+$ and $\mathscr{C}\mathscr{T}$, it becomes clear how to generalize $\Lambda^{(1)}$ and $\Lambda^{(2)}$. The definitions, and several alternative characterizations, are given in § 4. 1. The "Π-adic" characterization is of central importance and greatly simplifies the determination of the relative minima and minimal vectors. A real metric, which turns $\Lambda^{(1)}$, $\Lambda^{(2)}$ into $(p-1)p^n$-dimensional real lattices in the usual sense, is introduced in § 4. 2. With these preparations the main lattice properties follow fairly easily, though the anomalous cases $p=3,5$ need some further detailed consideration.

Notation. We write

$$C_r| = \theta^{n-r}[C_r] = \theta^{n-r}\sum_{\alpha\in C_r}\mathbf{e}_\alpha,$$

$$C_r;\ f| = \theta^{n-r}[C_r;\ f] = \theta^{n-r}\sum_{\alpha\in C_r}\omega^{f(\alpha)}\mathbf{e}_\alpha,$$

$$\mathbf{u}_\alpha = \theta^n\mathbf{e}_\alpha,$$

where θ is the Gauss sum (2.2.4).

We write $\Pi=\omega-1$. The principal ideal $\Pi\Omega$ is prime and $\Pi^{\frac{1}{2}(p-1)}\Omega=\theta\Omega = \bar{\theta}\Omega$, $\Pi^{p-1}\Omega=p\Omega$. The p elements of the residue class ring $\Omega/\Pi\Omega$ are represented by the rational integers $0, 1, \ldots, p-1$.

If $\lambda \in P$, the norm and trace of λ relative to R_0 are denoted by $N(\lambda)$, tr λ.

4.1. The principal lattices. We define $\Lambda^{(2)}$ as the set of $\mathbf{x}\in\Gamma$ such that $X\mathbf{x}\in\Gamma$

for all $X \in \mathscr{C}\mathscr{T}$; in other words, it is the largest set of integral vectors invariant (as a whole) under $\mathscr{C}\mathscr{T}$. By (2.2.3), $\theta^n \Gamma \subset \Lambda^{(2)}$. Therefore, by lemma 2.3.1, $\Lambda^{(2)}$ is an Ω-lattice.

We define $\Lambda^{(1)}$ as the dual of $\Lambda^{(2)}$ modulo θ^n. It is an Ω-lattice such that $\theta^n \Gamma \subset \Lambda^{(1)} \subset \Gamma$. By the argument of § 3.2, every unitary transformation which leaves $\Lambda^{(2)}$ invariant also leaves $\Lambda^{(1)}$ invariant. In particular, $\Lambda^{(1)}$ is invariant under $\mathscr{C}\mathscr{T}$. Hence, by the definition of $\Lambda^{(2)}$, $\Lambda^{(1)} \subset \Lambda^{(2)}$.

The following is an alternative characterization of $\Lambda^{(1)}$. Consider the Ω-lattice, say Λ, formed by the integral linear combinations of the vectors

$$|C_r; f|, \tag{4.1.1}$$

where C_r runs over all cosets in V, f over all functions on C_r of degree ≤ 2. The vectors (4.1.1) are, apart from sign, the vectors $X\mathbf{u}_\alpha$, where α runs over V, X over $\mathscr{C}\mathscr{T}$ (see (2.2.3) and (2.2.5)). Since

$$(X^{-1}\mathbf{u}_\alpha)\cdot \mathbf{x} = \pm \theta^n \mathbf{y}_\alpha,$$

where $\mathbf{y} = X\mathbf{x}$, it follows that Λ is dual to $\Lambda^{(2)}$ modulo θ^n. Therefore $\Lambda = \Lambda^{(1)}$.

For the remaining characterizations of $\Lambda^{(1)}$, $\Lambda^{(2)}$, some preparations are necessary. We define the *product* of two vectors by

$$(x_\alpha)(y_\alpha) = (x_\alpha y_\alpha).$$

Under this product, Γ becomes a commutative algebra over the ring Ω, with unit element $\mathbf{1} = [V]$. A *polynomial* in the elements $\mathbf{X}, \mathbf{Y}, \ldots$ of Γ means a sum

$$\sum_{\lambda, \mu, \ldots, \geq 0} a_{\lambda\mu\ldots} \mathbf{X}^\lambda \mathbf{Y}^\mu \cdots$$

of monomials with coefficients in Ω. The *subalgebra of Γ generated by* $\mathbf{X}, \mathbf{Y}, \ldots$ means the smallest subalgebra of Γ which contains these elements; it consists of the polynomials in $\mathbf{X}, \mathbf{Y}, \ldots$ *with zero constant term* $a_{00\ldots 1}$.

If $\alpha \in GF(p)$, let α' denote that rational integer in the interval $[0, p-1]$ which represents α. Write

$$\mathbf{A}_i = \sum_{(\alpha_1, \ldots, \alpha_n) \in V} \alpha_i' \mathbf{e}_{(\alpha_1, \ldots, \alpha_n)} \qquad (i = 1, \ldots, n).$$

Then each $\mathbf{x} \in \Gamma$ has a unique *Π-adic expansion*

$$\mathbf{x} \sim \sum_{i=0}^{\infty} Q_i(\mathbf{A}_1, \ldots, \mathbf{A}_n) \Pi^i, \tag{4.1.2}$$

where the Q_i are standard[11] polynomials with coefficients in $[0, p-1]$. (4.1.2) means that $\mathrm{x} \equiv \sum_0^{k-1} Q_i \Pi^i \pmod{\Pi^k \Gamma}$ for all k.

To prove our assertion, we consider the congruences

$$\sum_{\lambda_1, \ldots, \lambda_n = 0}^{p-1} q_{\lambda_1 \ldots \lambda_n} \alpha_1'^{\lambda_1} \cdots \alpha_n'^{\lambda_n} \equiv x_\alpha \pmod{\Pi^k},$$

where α runs over V. This is a system of p^n linear equations for the p^n variables $q_{\lambda_1 \ldots \lambda_n}$ in the residue class ring $\Omega/\Pi^k\Omega$. Since the determinant of the system is a power of $\prod_{i<j}(\alpha_i' - \alpha_j')$ and so a unit of $\Omega/\Pi^k\Omega$, the solution is unique. Thus, $\mathrm{x} \equiv Q(\mathrm{A}_1, \ldots, \mathrm{A}_n) \pmod{\Pi^k \Gamma}$, where Q is a standard polynomial over Ω, whose coefficients are unique modulo Π^k. Replacing the coefficients of Q by their Π-adic representations, we get the required unique representation $\mathrm{x} \equiv \sum_0^{k-1} Q_i \Pi^i \pmod{\Pi^k \Gamma}$.

If x_α is a function of $\alpha_{i_1}, \ldots, \alpha_{i_t}$ only, each Q_i is a polynomial in $\mathrm{A}_{i_1}, \ldots, \mathrm{A}_{i_t}$ only. This follows from the Π-adic expansion of the p^t-dimensional vector $y_{(\alpha_{i_1}, \ldots, \alpha_{i_t})} = x_\alpha$.

We return now to $\Lambda^{(1)}, \Lambda^{(2)}$. We first prove that $\Lambda^{(1)}$ *is the subalgebra of Γ generated by the vectors*

(4.1.3) $$|V;\, f|,\ |C_{n-1}|,$$

where f runs over all functions of degree ≤ 2, C_{n-1} over all $(n-1)$-dimensional cosets.

Consider the product $S = |C_r;\, f|\,|C_s;\, g|$, where f, g have degree ≤ 2. If $C_r \cap C_s$ is empty, $S = 0$. If not, $C_r \cap C_s = C_t$, where $n \geq \dim(C_r + C_s) = r + s - t$. Hence $S = \theta^{n+t-r-s}|C_t;\, f+g| \in \Lambda^{(1)}$. This proves that $\Lambda^{(1)}$ is a subalgebra. The elements (4.1.3) are generators because $|C_r;\, f| = |V;\, f| \prod_{i=1}^{r} |C_{n-1}^{(i)}|$ for any $(n-r)$ $C_{n-1}^{(i)}$'s with meet C_r.

Let $L^{(1)}$ denote the set of $\mathrm{x} \in \Gamma$ such that, in the Π-adic expansion (3.1.2),

(4.1.4) $$\text{degree } Q_i \leq 2i \qquad (i = 0, 1, \ldots).$$

Since (4.1.4) places no restriction on Q_i when $i \geq \frac{1}{2}n(p-1)$, we have $\Pi^{\frac{1}{2}n(p-1)}\Gamma = \theta^n \Gamma \subset L^{(1)}$. Using the Π-adic expansion

---

[11] i.e., the degree of Q_i in each variable is $< p$; cf § 2.1.

$$\mathbf{A}_i^p = \mathbf{A}_i + \Pi^{p-1}Q_{p-1}(\mathbf{A}_i) + \cdots$$

of $\mathbf{A}_i^p$, it can be verified that products and Ω-linear combinations of elements of $L^{(1)}$ are again in $L^{(1)}$; therefore $L^{(1)}$ *is a subalgebra of* Γ. We prove now that

(4.1.5) $$L^{(1)} = \Lambda^{(1)}.$$

Notation. If S is a subset or element of Γ, S^* denotes the corresponding subset or element in the factor algebra $\Gamma^* = \Gamma/\theta^n\Gamma$. The elements of Γ^* are regarded as vectors over the residue class ring $\Omega^* = \Omega/\theta^n\Omega$. $\mathscr{P}(\mathbf{X}^*, \ldots)$ denotes the subalgebra of Γ^* generated by $\mathbf{X}^*, \ldots$.

Proof of (*4.1.5*) Considering the monomials in the Π-adic expansion, we see that $L^{(1)*}$ is generated by the n^2+n+1 elements

(4.1.6) $$\mathbf{1}^*,\ \Pi\mathbf{A}_i^*,\ \Pi\mathbf{A}_i^*\mathbf{A}_j^*.$$

Since every $|V;f|$ in (4.1.3) is a polynomial in the n^2+n+1 vectors

$$\mathbf{1},\ \mathbf{a}_i = |V;\ \alpha_i| - \mathbf{1},\ \mathbf{a}_{ij} = |V;\ \alpha_i\alpha_j| - \mathbf{1},$$

$\Lambda^{(1)*}$ is generated by the corresponding elements

(4.1.7) $$\mathbf{1}^*,\ \mathbf{a}_i^*,\ \mathbf{a}_{ij}^*$$

and the vectors

(4.1.8) $$|C_{n-1}|^*.$$

We prove (4.1.5) by showing that

(A) the elements (4.1.6) and (4.1.7) can be expressed in terms of one another;

(B) the elements (4.1.8) can be expressed in terms of the elements (4.1.6).

The proof of (A) is simplified by the following lemma, whose easy proof is omitted.

LEMMA. *Let S be a subalgebra of Γ^* and $\mathbf{X}^*, \ldots$ elements of S. Then $S = \mathscr{P}(\mathbf{X}^*, \ldots)$ if, and only if, $S/\Pi S = \mathscr{P}(\mathbf{X}^* + \Pi S, \ldots)$.*

Consider now the elements $\mathbf{a}_i^*$. The α-th coordinate of $\mathbf{a}_i$ is

$$\omega^{\alpha_i} - 1 = (1+\Pi)^{\alpha_i'} - 1 = \sum_{j=1}^{\alpha_i'} \binom{\alpha_i'}{j}\Pi^j.$$

It follows that

$$\mathbf{a}_i^* = \sum_{j=1}^{p-1} (j!)^{-1} \prod_{k=0}^{j-1} (\Pi \mathbf{A}_i^* - k\Pi) + \Pi^p \mathbf{b}_i^*,$$

where $(\ )^{-1}$ denotes the inverse in Ω^* and $\mathbf{b}_i$ is a vector in Γ whose $\boldsymbol{\alpha}$-th coordinate depends only on α_i. From the Π-adic expansion of $\mathbf{b}_i$, we deduce that $\Pi^p \mathbf{b}_i^* \in \Pi \mathscr{P}(\Pi \mathbf{A}_i^*)$. It follows that $\mathbf{a}_i^* \in \mathscr{P}(\Pi \mathbf{A}_i^*)$. Further, since

$$\mathbf{a}_i^* \equiv \sum_{j=1}^{p-1} (j!)^{-1} (\Pi \mathbf{A}_i^*)^j \qquad (\operatorname{mod} \Pi \mathscr{P}(\Pi \mathbf{A}_i^*)),$$

we have

$$\Pi \mathbf{A}_i^* \equiv \sum_{j=1}^{p-1} (-1)^{j-1} j^{-1} (\mathbf{a}_i^*)^j \ (\operatorname{mod} \Pi \mathscr{P}(\Pi \mathbf{A}_i^*)),$$

whence, by the lemma, $\mathscr{P}(\Pi \mathbf{A}_i^*) = \mathscr{P}(\mathbf{a}_i^*)$.

By similar arguments, we get

$$\mathscr{P}(\Pi \mathbf{A}_i^*, \Pi \mathbf{A}_i^{*2}) = \mathscr{P}(\mathbf{a}_i^*, \mathbf{a}_{ii}^*),$$

$$\mathscr{P}(\Pi \mathbf{A}_i^*, \Pi \mathbf{A}_j^*, \Pi \mathbf{A}_i^{*2}, \Pi \mathbf{A}_j^{*2}, \Pi \mathbf{A}_i^* \mathbf{A}_j^*) = \mathscr{P}(\mathbf{a}_i^*, \mathbf{a}_j^*, \mathbf{a}_{ii}^*, \mathbf{a}_{jj}^*, \mathbf{a}_{ij}^*),$$

whence (A) follows.

By (A), and because of the symmetry of the set of vectors $|V; f|$ with respect to index transformations $\boldsymbol{\alpha} \to \boldsymbol{\alpha} D + \mathbf{t}$, it is sufficient to prove (B) when C_{n-1} is the particular coset defined by the equation $\alpha_1 = 0$. Now the Π-adic expansion shows that $[C_{n-1}]^*$ is a polynomial of degree $< p$ in $\mathbf{A}_1^*$. It follows that $\Pi^{\frac{1}{2}(p-1)}[C_{n-1}]^* \in \mathscr{P}(\Pi \mathbf{A}_1^*, \Pi \mathbf{A}_1^{*2})$ and therefore, since $\Pi^{\frac{1}{2}(p-1)}\Omega = \theta\Omega$, that $|C_{n-1}|^* \in \mathscr{P}(\Pi \mathbf{A}_1^*, \Pi \mathbf{A}_1^{*2})$. This proves (B) and (4.1.5).

There is a similar Π-adic characterization of $\Lambda^{(2)}$. Let $L^{(2)}$ denote the set of $\mathbf{x} \in \Gamma$ such that

(4.1.9) $$\text{degree } Q_i \leq 2i + 1 \qquad (i = 0, 1, \ldots);$$

then

(4.1.10) $$L^{(2)} = \Lambda^{(2)}.$$

This is proved by showing that

(C) $|\Gamma : L^{(1)}| |\Gamma : L^{(2)}| = |\Gamma : \theta^n \Gamma|$,

(D) $\mathbf{x} \cdot \mathbf{y} \equiv 0 \ (\operatorname{mod} \theta^n)$ whenver $\mathbf{x} \in L^{(1)}$, $\mathbf{y} \in L^{(2)}$.

(C), (D) imply that $L^{(1)}$, $L^{(2)}$ are dual modulo θ^n and thus that $L^{(2)} = \Lambda^{(2)}$, as required.

It is an easy combinatorial problem to show that

$$|L^{(1)}:\ \theta^n\Gamma| = p^{k_2},\ |L^{(2)}:\ \theta^n\Gamma| = p^{k_1},$$

where

(4.1.11) $$k_1 = \frac{1}{4}[n(p-1)+(p^n-1)],\ k_2 = \frac{1}{4}[n(p-1)-(p^n-1)].$$

Since $|\Gamma:\ \theta^n\Gamma| = p^{\frac{1}{2}n(p-1)p^n}$ and $k_1+k_2 = \frac{1}{2}n(p-1)p^n$, we get (C) and

(4.1.12) $$|\Gamma:\ L^{(i)}| = p^{k_i} \qquad (i=1,\ 2).$$

It is sufficient to prove (D) when

$$\mathbf{x} = \Pi^\lambda \mathbf{A}_1^{\lambda_1}\cdots\mathbf{A}_n^{\lambda_n},\ \mathbf{y} = \Pi^\mu \mathbf{A}_1^{\mu_1}\cdots\mathbf{A}_n^{\mu_n},$$

where

$$0\le\lambda_i<p, \qquad 0\le\mu_i<p,$$
$$\sum\lambda_i\le 2\lambda, \qquad \sum\mu_i\le 2\mu+1.$$

We may suppose that $\lambda+\mu<\frac{1}{2}n(p-1)$, for (D) is obvious otherwise. Let k be the integral part of $(p-1)^{-1}\sum(\lambda_i+\mu_i)$. Since

$$k(p-1)\le\sum(\lambda_i+\mu_i)\le 2\lambda+2\mu+1<n(p-1),$$

we have

(4.1.13) $$k<n,\ \frac{1}{2}k(p-1)<\lambda+\mu.$$

Let r be the number of indices i such that $\lambda_i+\mu_i\neq(p-1)$. Clearly $(n-r)(p-1)\le\sum(\lambda_i+\mu_i)$, so that

(4.1.14) $$r\ge n-k.$$

Now
$$\mathbf{x}\cdot\mathbf{y} = \overline{\Pi}^\lambda\Pi^\mu\sum_{\alpha\in\Gamma}\alpha_1'^{\lambda_1+\mu_1}\cdots\alpha_n'^{\lambda_n+\mu_n}$$
$$= \overline{\Pi}^\lambda\Pi^\mu s_{\lambda_1+\mu_1}\cdots s_{\lambda_n+\mu_n},$$

where

$$s_0 = p,\ s_k = 1^k+2^k+\cdots+(p-1)^k \qquad (k>0).$$

Since, for $k>0$, $s_k\equiv -1$ or $0 \pmod p$ according as $(p-1)\,|\,k$ or not, we have

$$\mathbf{x}\cdot\mathbf{y}\equiv 0 \pmod{\Pi^{\lambda+\mu+r(p-1)}}.$$

(D) now follows from (4.1.13), (4.1.14). This proves (4.1.10).

4.2. The real metric. E, as defined in §2.2, is a p^n-dimensional metric space over P. We now describe a natural way of defining it as a $(p-1)$ p^n-dimensional metric space over R_0.

Consider first the degenerate case $n=0$, where $E=P$ and $\Gamma=\Omega$. P is a $(p-1)$-dimensional vector space over R_0. It becomes a metric space over R_0 if we define the real scalar product by

$$\lambda * \mu = tr\, \bar{\lambda}\, \mu. \tag{4.2.1}$$

Since the Galois group G of P over R_0 is abelian,

$$\lambda * \lambda = \sum_{\sigma \in G} (\bar{\lambda} \lambda)^\sigma = \sum_{\sigma \in G} \bar{\lambda}^\sigma \lambda^\sigma \tag{4.2.2}$$

whence $\lambda * \mu$ is positive definite.

Ω becomes a $(p-1)$-dimensional lattice in the usual sense. The roots of unity $\omega^i (1 \leq i \leq p-1)$ form a lattice basis. By evaluating $\det(\mathrm{tr}\ \omega^{i-j})$, we get

$$D(\Omega) = p^{p-2}. \tag{4.2.3}$$

The inequality of the arithmetic and geometric means shows that $(p-1)|N(\lambda)|^2 \leq \lambda * \lambda$, with equality if, and only if, all conjugates of λ have the same modulus. Hence the minimal vectors of Ω are the roots of unity $\pm \omega^i$ and

$$M(\Omega) = p-1. \tag{4.2.4}$$

In the general case, E is a vector space over R_0 of dimension $N=(p-1)p^n$, and we define the real metric $\mathbf{x} * \mathbf{y}$ by

$$(x_\alpha) * (y_\alpha) = \sum_{\alpha \in V} x_\alpha * y_\alpha = \mathrm{tr}\,(x_\alpha) \cdot (y_\alpha). \tag{4.2.5}$$

Γ is an N-dimensional lattice with basis $\omega^i \mathbf{e}_\alpha$ $(\alpha \in V, 1 \leq i \leq p-1)$. By (4.2.3), (4.2.4),

$$D(\Gamma) = p^{(p-2)p^n},\ M(\Gamma) = p-1. \tag{4.2.6}$$

Hence, by (4.1.12),

$$D(\Lambda^{(i)}) = p^{(p-2)p^n + 2k_i} \qquad (i=1,\ 2), \tag{4.2.7}$$

where k_i is given by (4.1.11).

The following results are noted for future reference. Let $\lambda \in \Omega$ and let k be the rational integer in $[0, p-1]$ such that $\lambda \equiv k \pmod{\Pi}$. By (4.2.2), $\lambda * \lambda$ is even and $\equiv -k^2 \pmod{p}$. Hence

$$(4.2.8) \qquad \lambda * \lambda \quad \left.\begin{array}{ll} \geq 2p & \text{if } k=0,\ \lambda \neq 0, \\ \geq p-1 & \text{if } k=1,\ p-1 \\ \geq p+1 & \text{otherwise.} \end{array}\right\}$$

In particular, when $p=5$ and $k=2$, 3, equality holds if, and only if, λ is one of the 20 numbers $\pm(\omega^i+\omega^j)$ $(0 \leq i < j \leq 4)$.

4.3. Minima, minimal vectors. We now determine the minimal vectors of $\Lambda^{(1)}$, $\Lambda^{(2)}$. Let $\mathbf{x} = \Pi^s \mathbf{y} \in \Lambda^{(2)}$ $(s \geq 0)$, where $\mathbf{y} \in \Lambda^{(2)}$ but $\Pi^{-1}\mathbf{y} \notin \Lambda^{(2)}$. By the original definition of $\Lambda^{(2)}$, there is an $X \in \mathscr{C}\mathscr{T}$ such that $\mathbf{z} = X\mathbf{y} \notin \Pi\Gamma$. Let

$$\mathbf{z} \sim \sum_0^\infty Q_i(\mathbf{A}_1, \ldots, \mathbf{A}_n)\Pi^i,$$

and let

$$\tilde{Q}_i(\alpha_1, \ldots, \alpha_n) = \sum a_{\lambda_1 \ldots \lambda_n} \alpha_1^{\lambda_1} \cdots \alpha_n^{\lambda_n} \qquad (i=0,\ 1, \ldots)$$

be the unique standard polynomial over $GF(p)$ such that

$$\sum a'_{\lambda_1 \ldots \lambda_n} \alpha_1'^{\lambda_1} \cdots \alpha_n'^{\lambda_n} = Q_i(\alpha'_1, \ldots \alpha'_n).$$

If Y is the transformation (2.2.5), $Y\mathbf{w} = \mathbf{z}$ and

$$\mathbf{w} \sim \sum_0^\infty R_i(\mathbf{A}_1, \ldots, \mathbf{A}_n)\Pi^i,$$

then

$$\tilde{R}_0(\boldsymbol{\alpha}) = \tilde{Q}_0(\boldsymbol{\alpha}D+\mathbf{t}),\ \tilde{R}_1(\boldsymbol{\alpha}) = \tilde{Q}_1(\boldsymbol{\alpha}D+\mathbf{t}) - g(\boldsymbol{\alpha})\tilde{Q}_0(\boldsymbol{\alpha}D+\mathbf{t}).$$

After applying such a transformation we may therefore suppose that either (a) $Q_0 = k\mathbf{1}$ $(k \neq 0)$ or (b) $Q_0 = \mathbf{A}_1$. Notice that $\mathbf{z} \notin \Lambda^{(1)}$ in case (b), by (4.1.4).

Case (a). Every coordinate z_α is non-zero, whence by (4.2.4),

$$\mathbf{x} * \mathbf{x} = (\Pi^s\mathbf{z}) * (\Pi^s\mathbf{z}) \geq (p-1)p^n$$

with equality if, and only if, $s=0$ and z_α is a $(2p)$-th root of unity for each α. Suppose that equality holds. After replacing $\mathbf{z}$ by $-\mathbf{z}$ if necessary, we have $k=1$ and $\mathbf{z} = [V;\ f]$ for some standard polynomial $f(\alpha_1, \ldots, \alpha_n)$. Then, expanding $z_\alpha = (1+\Pi)^f$ by the binomial theorem, we get

$$\tilde{Q}_i(\alpha_1, \ldots, \alpha_n) = \binom{f(\alpha_1, \ldots, \alpha_n)}{i} \qquad (i=1, \ldots, p-2).$$

Therefore, since $\tilde{Q}_1$ and f are standard, $\tilde{Q}_1(\xi_1, \ldots, \xi_n) = f(\xi_1, \ldots, \xi_n)$ identically in independent variables ξ_i. After applying a suitable transformation (2.2.5), we may suppose that all terms in f of degree ≤ 2 are zero.

Suppose now that $\mathbf{x} \in \Lambda^{(1)}$. Then $\mathbf{z} \in \Lambda^{(1)}$ and so, by (4.1.4), the degree of $\tilde{Q}_1 \leq 2$. Hence $f = 0$ and $\mathbf{z} = [V]$. Suppose secondly that $\mathbf{x} \in \Lambda^{(2)}$, $\mathbf{x} \notin \Lambda^{(1)}$. Then, by (4.1.9), the degree of $\tilde{Q}_1 \leq 3$, so that f is a homogeneous cubic. If $p \geq 7$,

$$\tilde{Q}_2(\xi_1, \dots, \xi_n) = \binom{f(\xi_1, \dots, \xi_n)}{2}$$

since the latter is standard. This is impossible because $\binom{f}{2}$ has degree 6, $\tilde{Q}_2$ degree ≤ 5. Hence $p = 3$ or 5. We need not consider the case $p = 3$, because case (b) shows that $\mathbf{z} * \mathbf{z} > M^{(2)} = 4.3^{n-1}$. Suppose then that $p = 5$. After a suitable transformation (2.2.5), we may suppose that

$$f(\alpha_1, \dots, \alpha_n) = \alpha_1^3 + \alpha_1 q(\alpha_2, \dots, \alpha_n) + r(\alpha_2, \dots, \alpha_n),$$

where q, r are homogeneous of degrees 2, 3 respectively. Then, after reduction to standard form, $\binom{f}{2}$ contains the sextic terms $\alpha_1^4 q + \alpha_1^3 r$, so that $q = r = 0$. Thus $\mathbf{z} = [V;\ \alpha_1^3]$. It is easy to see that this vector is actually in $\Lambda^{(2)}$.

Case (*b*). We have $z_\alpha \equiv \alpha_1^t \pmod{\Pi}$, whence, by (4.2.8),

$$\mathbf{x} * \mathbf{x} \geq (p-1)p^n \times 2p = 2(p-1)p^n \qquad \text{if } s > 0$$

$$\mathbf{x} * \mathbf{x} \geq (p-3)p^{n-1} \times (p+1) + 2p^{n-1} \times (p-1) = (p^2-5)p^{n-1} \qquad \text{if } s = 0.$$

By case (a), $\mathbf{x}$ cannot be a minimal vector of $\Lambda^{(2)}$ unless $s = 0$ and $p = 3$ or 5. Notice that in these cases $\mathbf{x} \notin \Lambda^{(1)}$ because $s = 0$ and $\mathbf{z} \notin \Lambda^{(1)}$. Let C^λ denote the $(n-1)$-dimensional coset in V defined by the equation $\alpha_1 = \lambda$. Suppose first that $p = 3$ and $\mathbf{x} * \mathbf{x} = (3^2 - 5)3^{n-1} = 4.3^{n-1}$. By (4.2.4), and since $Q_0 = \mathbf{A}_1$,

$$\mathbf{z} = [C^1;\ f] - [C^{-1};\ g]$$

where f, g are standard polynomials in $\alpha_2, \dots, \alpha_n$. Using the equations

$$|C^1| = 2\,\mathbf{A}_1 - \mathbf{A}_1^2,\ |C^{-1}| = \frac{1}{2}(\mathbf{A}_1^2 - \mathbf{A}_1),$$

we get

$$\tilde{Q}_1 = \alpha_1^2(g-f) - \alpha_1(g+f),$$

whence the degrees of $g-f$, $g+f$ are ≤ 1, 2 respectively. Then the element

$$Y\mathbf{e}_\alpha = \omega^{-\frac{1}{2}[(f+g)+\alpha_1(f-g)]}\mathbf{e}_\alpha$$

of $\mathscr{C}\mathscr{T}$ maps $\mathbf{z}$ onto

$$[C^1]-[C^{-1}]=\mathbf{A}_1+3/2(\mathbf{A}_1-\mathbf{A}_1^2).$$

The Π-adic expansion shows that this vector is in $\Lambda^{(2)}$.

Suppose now that $p=5$ and $\mathbf{x}*\mathbf{x}=(5^2-5)5^{n-1}=4.5^n$. By (4.2.8), and since $Q_0=\mathbf{A}_1$,

$$\mathbf{z}=[C^1;\ f]-[C^{-1};\ g]+([C^2;\ h_1]+[C^2;\ h_2])-([C^{-2};\ k_1]+[C^{-2};\ k_2])$$

where $f, g, \ldots$ are standard polynomials in $\alpha_2, \ldots, \alpha_n$ and neither h_1-h_2 nor k_1-k_2 assumes the value 0. Then

$$\begin{aligned}\tilde{Q}_1=\alpha_1^4(-f+g-h+k)+\alpha_1^3(-f-g-2h-2k)\\ +\alpha_1^2(-f+g+h-k)+\alpha_1(-f-g+2h+2k)\end{aligned}$$

where $h=h_1+h_2$, $k=k_1+k_2$. Since the degree of $\tilde{Q}_1\leq 3$, the coefficient of $\alpha_1^4=0$ and those of α_1^3, α_1^2, α_1 have degrees ≤ 0, 1, 2 respectively. After applying the transformation

$$Y\mathbf{e}_\alpha=\omega^{-\frac{1}{2}(f+g)-\frac{1}{2}\alpha_1(f-g)-c(\alpha_1^2-1)}\mathbf{e}_\alpha,$$

where c is the constant $h+2f+g$, we have $f=g=h=k$, so that $h_1=-h_2$, $k_1=-k_2$. The next term of the Π-adic expansion now gives

$$\tilde{Q}_2=(\alpha_1^3-\alpha_1)[(k_1^2-h_1^2)\alpha_1-2(h_1^2+k_1^2)].$$

Since the functions $h_1-h_2=2h_1$ and $k_1-k_2=2k_1$ do not assume the value 0, it follows that h_1^2, k_1^2 are functions of degree ≤ 2 which can assume only the values 1, -1. It is easy to see that every function of degree 1 or 2 assumes at least 3 values, so that h_1^2, k_1^2 are constants. Hence, after applying the transformation $Y\mathbf{e}_\alpha=-\mathbf{e}_{-\alpha}$ if necessary, $\mathbf{z}$ becomes one of the 4 vectors

$$\mathbf{v}_{r,s}=[C^1]-[C^{-1}]+(\omega^r+\omega^{-r})[C^2]-(\omega^s+\omega^{-s})[C^{-2}],$$

where $(r, s)=(1, 1)$, $(1, 2)$, $(2, 1)$ or $(2, 2)$. The Π-adic expansion shows that $\mathbf{v}_{r,s}\in\Lambda^{(2)}$. The transformation

$$Y\mathbf{e}_{(\lambda,\alpha_2,\ldots,\alpha_n)}=\theta^{-1}\sum_{\mu}\omega^{(\lambda-\mu)^2}\mathbf{e}_{(\mu,\alpha_2,\ldots,\alpha_n)}$$

belongs to $\mathscr{C}\mathscr{T}$ and maps $\mathbf{v}_{12}$, $\mathbf{v}_{21}$ into vectors with all coordinates non-zero. Hence the minimal vector pairs $\pm[V;\ \alpha_1^3]$, $\pm\mathbf{v}_{12}$, $\pm\mathbf{v}_{21}$ are equivalent under $\mathscr{C}\mathscr{T}$. It can be shown, though we omit the proof, that no two of the pairs

$\pm[V]$, $\pm[V;\ \alpha_1^3]$, $\pm \mathrm{v}_{11}$, $\pm \mathrm{v}_{22}$ are equivalent under $\mathscr{C}\mathscr{T}$.

We have proved

THEOREM 4.3.1. *The minimal vector pairs of $\Lambda^{(i)}$ are given by* (4.1.1) *except when $i=2$ and $p=3$ or 5. When $i=2$, $p=3$, every minimal vector pair is equivalent under $\mathscr{C}\mathscr{T}$ to $\pm([C^1]-[C^{-1}])$, where C^λ is the $(n-1)$-dimensional coset defined by $\alpha_1=\lambda$. When $i=2$, $p=5$, every minimal vector pair is equivalent under $\mathscr{C}\mathscr{T}$ to one, and only one, of the pairs $\pm[V]$, $\pm[V;\ \alpha_1^3]$ and*

$$\pm\{[C^1]-[C^{-1}]+(\omega^i+\omega^{-i})([C^2]-[C^{-2}])\} \qquad (i=1,\ 2).$$

where C^λ has the same meaning as in the case $p=3$.

THEOREM 4.3.2. *The relative minima $\gamma^{(1)}$, $\gamma^{(2)}$ of $\Lambda^{(1)}$, $\Lambda^{(2)}$ are given by*

$$\gamma^{(1)}=(p-1)p^{\frac{1}{2}n-1+\frac{1}{2}(p-1)^{-1}(1+p^{-n})} \qquad (p\geq 3)$$

$$\gamma^{(2)}=(p-1)p^{\frac{1}{2}n-1+\frac{1}{2}(p-1)^{-1}(3-p^{-n})} \qquad (p>3)$$

$$\gamma^{(2)}=4.3^{\frac{1}{2}n-\frac{5}{4}-\frac{1}{4}3^{-n}} \qquad (p=3).$$

We can compare our forms with the original ones in 2^n variables by computing $\rho_i(p)=\lim_{n\to\infty}\gamma^{(i)}\Big/\left(\frac{1}{2}N\right)^{\frac{1}{2}}$. We have:

$$\rho_1(3)\approx 0.9,\ \rho_1(5)\approx 0.7,\ \ldots$$

$$\rho_2(3)=4.3^{-\frac{5}{4}}\approx 1.01,\ \rho_2(5)=2^{15/8}5^{-5/8}\approx 1.03,\ \rho_2(7)\approx 0.8,\ \ldots$$

$$\lim_{p\to\infty}\left(\frac{1}{2}p\right)^{\frac{1}{2}}\rho_i(p)=1 \qquad (i=1,\ 2).$$

The lowest values of $(p-1)\ p^n$ are 6, 18, 20 corresponding to $p^n=3,9,5$ respectively. The forms in 6 variables are the absolutely extreme and "next best" extreme. The relative minima of the forms in 18, 20 variables for $i=2$ are

$$4/3^{5/18}\approx 2.95,\ 4/5^{3/20}\approx 3.1.$$

These are comparable with the value $8^{\frac{1}{2}}\approx 2.8$ for the 16-variable form of EF.

4.4. Extreme Forms. Two points can be made at once.

(1) $\Lambda^{(i)}$ is invariant under the R_0-irreducible[12] group $\mathscr{C}\mathscr{T}$. *Therefore it is eutactic* (Coxeter [4], p. 402).

(2) Let S be the automorphism of P such that $\omega^S = \omega^2$ and let $\mathbf{a}$ be any element of V. Then it is easily verified that, if $p > 3$, every vector (4.1.1) satisfies the quadratic relation

$$x_{3\mathbf{a}}^S x_{-3\mathbf{a}} = x_{-\mathbf{a}}^S x_{5\mathbf{a}}.$$

Therefore, if $p>3$, $\Lambda^{(i)}$ cannot be perfect when the vectors (4.1.1) and their negatives are its minimal vectors; i.e., $\Lambda^{(i)}$ *cannot be perfect unless* $p=3$ *or* $p=5$, $i=2$. We shall see, however, that $\Lambda^{(i)}$ *is* perfect in a modified sense now to be defined.

Let Λ be a sublattice of the N-dimensional lattice Γ. Let $G(\mathbf{x}, \mathbf{y})$ stand generically for an R_0-bilinear function defined on E and with complex values. Then, according to the usual definition, Λ is perfect if the equations

(4.4.1) $\qquad G(\mathbf{m}, \mathbf{m}) = 0$ for all minimal vectors $\mathbf{m}$ of Λ,

imply that

(4.4.2) $\qquad G(\mathbf{x}, \mathbf{x}) = 0$ for all $\mathbf{x} \in E$.

We may, without loss of generality, suppose in the definition that the values of $G(\mathbf{x}, \mathbf{y})$ are in R_0.

Let now $t(\neq 0) \in GF(p)$ and let T be the automorphism of P such that $\omega^T = \omega^t$. We call Λ *t-perfect* if the implication (4.4.1) $\Rightarrow$ (4.4.2) holds for functions of the form

(4.4.3) $$G(\mathbf{x}, \mathbf{y}) = \sum_{\alpha, \beta} g_{\alpha,\beta} x_\alpha^T y_\beta \qquad (g_{\alpha,\beta} \in P).$$

Clearly, if Λ is perfect it is t-perfect for all t. The converse is also true. In fact, let G be as in the previous paragraph. Then

$$G_t(\mathbf{x}, \mathbf{y}) = \sum_{i,j=0}^{p-1} \omega^{-ti-j} G(\omega^i \mathbf{x}, \omega^j \mathbf{y})$$

has the form (4.4.3), and

$$p^2 G(\mathbf{x}, \mathbf{y}) = tr\Big(\sum_{t=1}^{p-1} G_t(\mathbf{x}, \mathbf{y})\Big).$$

---

12) $\mathscr{C}\mathscr{T}$ is R_0-irreducible because it is P-irreducible (CGI, theorem 1) and contains the scalars ωI.

Therefore the implication (4.4.1) $\Rightarrow$(4.4.2) is valid for G if it is valid for each G_t.

We call A *P-perfect* if it is 1-and (-1)-perfect, i.e., if it is perfect with respect to symmetric P-bilinear, and Hermitian, forms. We now prove

THEOREM 4.4. *$A^{(i)}$ is eutactic and P-perfect. It is perfect only for $p=3$, $i=1$, 2 and $p=5$, $i=2$.*

Proof. Let G be the function (4.4.3). We seek the conditions that $G(\mathrm{x}, \mathrm{x})=0$ for all vectors $\mathrm{x}=|V;\ \phi|$, where ϕ has the form

$$\phi(\alpha)=\sum_{i\leq j} a_{ij}\alpha_i\alpha_j+\sum_i a_i\alpha_i.$$

The equation $G(\mathrm{x}, \mathrm{x})=0$ gives

$$\sum_{\alpha, \beta} g_{\alpha, \beta}\,\omega^{t\phi(\alpha)+\phi(\beta)}=0. \tag{4.4.4}$$

If
$$\Psi(\alpha)=\sum_{i\leq j} b_{ij}\alpha_i\alpha_j+\sum b_i\alpha_i,$$

we write

$$\phi*\Psi=\sum_{i\leq j} a_{ij}b_{ij}+\sum_i a_i b_i,$$

$$g_\Psi=\sum g_{\alpha, \beta},$$

where summation is over the α, β such that

$$t\alpha_i\alpha_j+\beta_i\beta_j=b_{ij}, t\alpha_i+\beta_i=b_i \qquad (\text{all } i,\ j) \tag{4.4.5}$$

and where $g_\Psi=0$ when (4.4.5) has no solutions. Then (4.4.4) becomes

$$\sum_{\Psi}\omega^{\phi*\Psi}g_\Psi=0 \qquad (\text{all } \phi).$$

The matrix $(\omega^{\phi*\Psi})$ is non-singular, being a direct power of the $p\times p$ matrix (ω^{ij}), and so the vector (g_Ψ) is zero. If $t=-1$, (4.4.5) has at most one solution α, β whence $G(\mathrm{x}, \mathrm{y})=0$. If $t=1$, it has either no solution or a unique solution α, α or exactly two solutions α, β and β, α. Hence $g_{\alpha,\beta}+g_{\beta,\alpha}=0$ for all α, β and so $G(\mathrm{x}, \mathrm{x})\equiv 0$.

We have now proved that $A^{(i)}$ is P-perfect whenever the $[V;\ \phi]$ are minimal vectors, i.e., except when $p=3$, $i=2$. The conclusion is still true in this case.

In fact, let $\mathrm{v}_i=[C^i;\ \phi]$ $(i=0, 1, 2)$ with ϕ as above and C^i as in § 4.3. Then it is easily seen that because $G(\mathrm{x}, \mathrm{x})$ vanishes for

$$\mathbf{v}_0 - \omega^i \mathbf{v}_1,\ \mathbf{v}_1 - \omega^i \mathbf{v}_2,\ \mathbf{v}_2 - \omega^i \mathbf{v}_0 \qquad (i = 1, 2, 3),$$

it also vanishes for $\mathbf{v}_0 + \mathbf{v}_1 + \mathbf{v}_2 = [V;\ \phi]$. The previous argument now shows that $G(\mathbf{x}, \mathbf{x}) \equiv 0$. Hence $\Lambda^{(i)}$ is P-perfect in all cases.

When $p = 3$, $\Lambda^{(i)}$ is 1-and (-1)-perfect and so perfect. It remains to prove only that $\Lambda^{(2)}$ is 2-and (-2)-perfect when $p = 5$. This is done by applying our previous argument to $[V;\ \alpha_\kappa^3 + \phi]$ instead of $[V;\ \phi]$. It is readily seen that the solution of (4.4.5) plus the equation $t\alpha_\kappa^3 + \beta_\kappa^3 = b$ is unique if either $\boldsymbol{\alpha}, \boldsymbol{\alpha}$ is a solution or there is a solution $\boldsymbol{\alpha}, \boldsymbol{\beta}$ with $\alpha_\kappa \neq \beta_\kappa$. Therefore $g_{\boldsymbol{\alpha},\boldsymbol{\beta}} = 0$ unless $\alpha_\kappa = \beta_\kappa$ and $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$. Since this holds for all κ, $g_{\boldsymbol{\alpha},\boldsymbol{\beta}} = 0$ for all $\boldsymbol{\alpha}, \boldsymbol{\beta}$ and so $G(\mathbf{x}, \mathbf{x}) \equiv 0$. This proves the theorem.

References

[1] Barnes, E. S. and Wall, G. E., Some extreme forms defined in terms of Abelian groups, *J. Australian Math. Soc.* **1** (1959), 47–63.

[2], [3] Bolt, Beverley, Room, T. G. and Wall, G. E., On the Clifford collineation, transform and similarity groups (I) and (II), *J. Australian Math. Soc.* **2** (1961), 60–96.

[4] Coxeter, H. S. M., Extreme forms, *Canad. J. Maths.* **3** (1951), 391–441.

[5] Coxeter, H. S. M. and Moser, W. O. J., *Generators and relations for discrete groups* (Springer, 1957).

[6] Dieudonné, J., *La geometrie des groupes classiques* (Springer, 1955).

University of Sydney
New South Wales