JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematics and Mathematical Physics
Vol. 69B, No. 4, October–December 1965

# Groups of Unimodular Circulants

**Richard H. Austing**

(August 12, 1965)

A method to determine a basis of the group of rational integral symmetric positive definite unimodular $n$x$n$ circulants for any $n$, is presented. This method uses the correspondence between unimodular circulants and units of the algebraic number field $R(\zeta)$, where $\zeta$ is a primitive $n$th root of unity. Known results are used to obtain generators of certain aperiodic subgroups of the abelian, finitely generated group of units in $R(\zeta)$. The correspondence, then, produces the desired basis elements. The number of basis elements for each $n$ is proved to be $\left[\frac{n}{2}\right]+1-\sigma_0(n)$, where $\sigma_0(n)$ is the number of positive divisors of $n$. In addition, an upper bound for the number of congruence classes of these circulants is obtained, where congruence is relative to rational symmetric unimodular $n$x$n$ circulants.

Key Words: Algebraic numbers, circulant matrices, abelian groups.

In 1956, M. Newman and O. Taussky [7][1] exhibited a rational integral symmetric positive definite unimodular $8\times 8$ circulant that was not of the form $AA'$, where $A$ is a rational integral $8\times 8$ circulant and $A'$ its transpose. The method they used in obtaining the positive definite circulant can be adapted to find generators of groups of rational integral symmetric positive definite unimodular circulants for particular values of $n$. However, difficult problems arise when the method is applied for arbitrary $n$.

This paper presents an alternate method of determining generators of these groups through the use of a correspondence, investigated by O. Taussky [8], between units of the algebraic number field $R(\zeta)$, where $\zeta$ is a primitive $n$th root of unity, and unimodular circulants. The group of units in $R(\zeta)$ is abelian and finitely generated. By restricting the discussion to certain aperiodic subgroups of this group, results conveniently compiled in Hecke [2, pp 38–44] can be used to determine generators of the subgroups. By the correspondence, then, generators of groups of rational integral symmetric positive definite unimodular $n$x$n$ circulants are obtained. In addition, the number of these generators is proved to be $\left[\frac{n}{2}\right]+1-\sigma_0(n)$, where $\sigma_0(n)$ is the number of positive divisors of $n$. Furthermore, an upper bound for the number of classes of these circulants is obtained for arbitrary $n$, where two of these circulants $A$ and $B$ are in the same class if and only if there is a rational symmetric unimodular $n$x$n$ circulant $S$ such that $A=S'BS$.

[1] Figures in brackets indicate the literature references at the end of this paper.

First, the notation used throughout this paper will be established. Let $P$ be the $n$x$n$ permutation matrix

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & \dots & & & \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Then $P$ is a full cycle. Since $P$ is normal there exists a unitary matrix $U$ such that $U^*\,P\,U=D_{P'}$ where $D_P$ is a diagonal matrix and $U^*$ is the conjugate transpose of $U$. Assume $\zeta$ is a primitive $n$th root of unity. Then $U$ may be taken as $\frac{1}{\sqrt{n}}(\zeta^{ij})$ for $1\leq i,\ j\leq n$. It follows that $D_P=\operatorname{diag}(\zeta,\zeta^2,\dots,\zeta^n)$ and the eigenvalues of $P$ are the $n$th roots of unity.

Let $C$ be an $n$x$n$ rational integral unimodular circulant given by $C=a_0I+a_1P+\dots+a_{n-1}P^{n-1}$. Denote by $G$ the group of all such circulants; $G_1$, the subgroup of symmetric elements of $G$; and $G_2$, the subgroup of positive definite elements of $G_1$. We will prove that $G$ is a finitely generated abelian group (Theorem 1). The subgroup $G_1$ and $G_2$ of $G$, then, are also finitely generated and abelian. It follows that each of the groups $G$, $G_1$, $G_2$ can be decomposed into the direct product of a periodic group and an aperiodic group [9, p. 91]. Let $R$ be the field of rationals and denote by $E$ the finitely generated multiplicative abelian group of units in $R(\zeta)$; $E_1$, the subgroup of real elements of $E$; and $E_2$, the subgroup of totally positive elements of $E_1$.

That is, $E_2$ consists of those elements of $E_1$ which are positive together with all their conjugates. (The notation and definitions of all groups in this paper are given in the appendix.)

With the above notation, Dirichlet's Theorem [2, p. 124] can be stated as follows:

If the defining polynomial of $R(\zeta)$ is $p(x)$, and if among the roots of $p(x)$ there are $r_1$ real and $2r_2$ imaginary ones, then the number of elements of infinite order in the basis of $E$ is $r=r_1+r_2-1$. There exist $r+1$ units $\zeta, \eta_1, \ldots, \eta_r$, where $\zeta$ is a primitive $w$th root of unity, such that any element $\epsilon$ of $E$ has a unique representation $\epsilon=\zeta^{a_0}\eta_1^{a_1}\ldots\eta_r^{a}r$, where $a_i$ are rational integers for $1\leqslant i\leqslant r$ and $a_0$ is a rational integer modulo $w$.

Note that the basis elements $\eta_1, \ldots, \eta_r$ of infinite order can be taken to be real [1, p. 185].

Each group $E$, $E_1$, and $E_2$ can also be decomposed into a direct product of a periodic group and an aperiodic group. Let $E_1'$ be the largest aperiodic subgroup of $E_1$. Define $H$, $H_1$, and $H_2$ as follows: $H$ is the largest aperiodic subgroup of $G$; $H_1$ is the subset of elements of $H$ all of whose eigenvalues belong to $E_1'$; and $H_2=H_1\cap G_2$.

The following theorem will be of importance. A sketch of the proof was published as part of a paper by M. Newman [6]; the proof was suggested by O. Taussky. The proof is included here because some of the details in the proof will be used in later proofs.

THEOREM 1. *G is a finitely generated abelian group with respect to matrix multiplication.*

PROOF. It is clear that $G$ is an abelian group with respect to matrix multiplication. To show that $G$ is finitely generated, we embed it in a finitely generated group. Let $C=a_0I+a_1P+\ldots+a_{n-1}P^{n-1}=\epsilon(P)$ be an arbitrary element of $G$. Since $P=UD_pU^*$, then $C=UD_cU^*$, where $D_c=\operatorname{diag}(\epsilon(\zeta), \ldots, \epsilon(\zeta^n))$ and $U$ is the unitary matrix mentioned earlier. But $D_c$ can be written as a product in the following way:

$$D_c=\operatorname{diag}(\epsilon(\zeta), 1, \ldots, 1)\operatorname{diag}(1, \epsilon(\zeta^2), 1, \ldots, 1)\ldots \operatorname{diag}(1, \ldots, \epsilon(\zeta^n))$$

where $\epsilon(\zeta^j)\,\epsilon E$ for $1\leqslant j\leqslant n$ (since $\det D_c=\det C=\pm 1$).

With the notation in the above statement of Dirichlet's Theorem, each unit $\epsilon(\zeta^j)$, $1\leqslant j\leqslant n$, has the following unique representation:

$$\epsilon(\zeta^j)=\zeta^{a_{0j}}\eta_1^{a_{1j}}\eta_2^{a_{2j}}\ldots\eta_r^{a_{rj}}.$$

Then

$$\operatorname{diag}(1, \ldots, 1, \epsilon(\zeta^j), 1, \ldots, 1)=\operatorname{diag}(1, \ldots, 1, \zeta^{a_{0j}}, 1, \ldots, 1)\prod_{i-1}^{r}\operatorname{diag}(1, \ldots, 1, \eta_i^{a_{ij}}, 1, \ldots, 1),$$

where the elements $\epsilon(\zeta^j)$, $\zeta^{a_{0j}}$, $\eta_i^{a_{ij}}$ appear in the $j$th position on the diagonal for $1\leqslant j\leqslant n$. Let

$$A_{0j}=U\operatorname{diag}(1, \ldots, 1, \zeta, 1, \ldots, 1)\,U^*$$

$$A_{ij}=U\operatorname{diag}(1, \ldots, 1, \eta_i, \ldots, 1)\,U^*,$$

$1\leqslant i\leqslant r$, $1\leqslant j\leqslant n$ (i.e., the elements $\zeta$ and $\eta_i$, appear in the $j$th position on the diagonal of $A_{ij}$, $1\leqslant j\leqslant n$). Then there are finitely many matrices of the form $A_{ij}$ such that

$$C=\prod_{\substack{i=0, 1, \ldots, r\\ j=1, \ldots, n}} A_{ij}^{a_{ij}}.$$

However, the matrices $A_{ij}$ need not be circulants.

Consider the group $\Gamma$ generated by the $A_{ij}$'s defined above for $0\leqslant i\leqslant r$ and $1\leqslant j\leqslant n$. It is clear that $\Gamma$ is finitely generated. Furthermore, $\Gamma$ is abelian because diagonal matrices commute. Thus $\Gamma$ is a finitely generated abelian group which contains $G$ as a subgroup and the theorem is proved.

COROLLARY 1. All eigenvalues of an element of $G(G_i, i=1, 2)$ are elements of $E(E_i, i=1, 2)$.

A relationship between $G$ and a certain group of units will be established for which the following properties of units in $E$ are needed.

LEMMA 1. *Let $\Phi_n(x)$ be the cyclotomic polynomial of degree $\varphi(n)$ and let $\nu$ be a primitive $n^{\text{th}}$ root of unity. Then the sum of the coefficients of a unit $q(\nu)\epsilon E$ can be changed modulo $\Phi_n(1)$ without changing the unit.*

PROOF. Let $q(x)$ be an integral polynomial such that $q(\nu)$ is a unit in $E$. Define a polynomial $q_t(x)$ as follows: $q_t(x)=q(x)+t\Phi_n(x)$, where $t$ is an integer. Then $q_t(\nu)=q(\nu)$ and $q_t(1)=q(1)+t\Phi_n(1)$. Since $q(1)$ is the sum of the coefficients of $q(\nu)$ the lemma is proved.

LEMMA 2. $\Phi_n(1)=\begin{cases} p \text{ if } n=p^\alpha \\ 1 \text{ otherwise,} \end{cases}$ *where $p$ is a prime and $\alpha$ is a positive integer.* [5, p. 160]

PROOF. Let $\mu(d)$ be the Möbius function and let $\zeta$ be a primitive $n$th root of unity. Then

$$\Phi_n(x)=\prod_{(r, n)=1}(x-\zeta^r)=\prod_{d|n}(x^{n/d}-1)^{\mu(d)}$$

$$=\prod_{d|n}\left(\frac{x^{n/d}-1}{x-1}\right)^{\mu(d)},\quad n>1.$$

The last equality follows because

$$\prod_{d|n}(x-1)^{\mu(d)}=(x-1)^{\sigma}=1 \text{ for } n>1 \text{ and } \sigma=\sum_{d|n}\mu(d).$$

Thus, for $n>1$

$$\Phi_n(1)=\prod_{(r, n)=1}(1-\zeta^r)=\prod_{d|n}\left(\frac{n}{d}\right)^{\mu(d)}=\prod_{d|n}d^{-\mu(d)}$$

$$=\begin{cases} p \text{ if } n=p^\alpha \\ 1 \text{ otherwise.} \end{cases}$$

From Lemma 1 it follows that the representation of a unit $q(\nu)$ in $E$ can be uniquely given either by specifying $q(\eta)$ for some nonprimitive $n$th root of unity (for example, $\eta=1$) or by specifying the polynomial $q(x)$.

EXAMPLE. A primitive 5th root of unity $\nu$ satisfies the relation $\nu^4+\nu^3+\nu^2+\nu+1=0$. Consider the distinct polynomials $q_1(x)=1-x-x^4$ and $q_2(x)=2+x^2+x^3$. Then

$$q_1(\nu)=1-\nu-\nu^4=2+\nu^2+\nu^3=q_2(\nu)$$

$$q_1(\nu^2)=1-\nu^2-\nu^3=2+\nu+\nu^4=q_2(\nu^2)$$

$$q_1(\nu^3)=q_1(\nu^2)=q_2(\nu^3)$$

$$q_1(\nu^4)=q_1(\nu)=q_2(\nu^4)$$

$$q_1(\nu^5)=q_1(1)=-1,\ q_2(\nu^5)=q_2(1)=4.$$

Let $\epsilon(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ be the integral polynomial such that $\epsilon(\zeta^k)$, $1\leq k\leq n$, are eigenvalues of the circulant $\epsilon(P)$ in $G$. (Let $\zeta=\exp\frac{2\pi i}{n}$ for definiteness.) From the proof of Theorem 1 it follows that these eigenvalues have a fixed ordering and, since their representation is fixed by $\epsilon(x)$, uniquely determine $\epsilon(P)$. These eigenvalues occur precisely once among the numbers $\epsilon(\zeta^{r\,n/d})$, where $d$ runs over the positive divisors of $n$, and $r$ runs over those integers such that $1\leq r\leq d$, $(r,\ d)=1$. Denote the divisors, including 1 and $n$, by $d_1,\ \ldots,\ d_m$, where $1=d_1<d_2<\ldots<d_m=n$ and $m=\sigma_0(n)$.

Corresponding to each $\epsilon(x)$ as defined above there is an $m$-tuple $(\epsilon(\zeta^{d_1}),\ \ldots,\ \epsilon(\zeta^{d_m}))$ of units of $E$. (When $n$ is a prime $p$, for example, $d_1=1$, $d_2=d_m=p$ and the $m$-tuples have the form $(\epsilon(\zeta),\ \epsilon(1))$.) Let $\mathscr{F}$ be the set of all such $m$-tuples. Define the mapping $\theta$ of $G$ into $\mathscr{F}$ by

$$\theta\colon\ \epsilon(P)\longrightarrow(\epsilon(\zeta^{d_1}),\ \ldots,\ \epsilon(\zeta^{d_m}))$$

and multiplication of elements of $\mathscr{F}$ by

$$(\epsilon(\zeta^{d_1}),\ \ldots,\ \epsilon(\zeta^{d_m}))\cdot(\delta(\zeta^{d_1}),\ \ldots,\ \delta(\zeta^{d_m}))$$

$$=(\epsilon(\zeta^{d_1})\cdot\delta(\zeta^{d_1}),\ \ldots,\ \epsilon(\zeta^{d_m})\cdot\delta(\zeta^{d_m})).$$

THEOREM 2. *$\theta$ is an isomorphism of* G *onto* $\mathscr{F}$.

PROOF. The mapping $\theta$ is onto. Let $\epsilon(x)$ be an integral polynomial such that $\epsilon(\zeta^d)\epsilon E$ for each $d|n$ and define $\Lambda_d=\operatorname{diag}(\zeta^{r_1n/d},\ \ldots,\ \zeta^{r_kn/d})$, where $k=\varphi(d)$ and $1=r_1<r_2<\ldots<r_k\leq d$ are the numbers relatively prime to $d$. (That is, the diagonal elements of $\Lambda_d$ are the primitive $d$th roots of unity.) Form the direct sum $\sum_{d|n}{}'\Lambda_d$. For a suitable permutation matrix $Q$,

$$Q\sum_{d|n}{}'\Lambda_dQ'=\operatorname{diag}(\zeta,\ \ldots,\ \zeta^n)=D_\epsilon.$$

Also

$$\epsilon(\Lambda_d)=\operatorname{diag}(\epsilon(\zeta^{r_1n/d}),\ \ldots,\ \epsilon(\zeta^{r_kn/d}))$$

so that

$$Q\left(\sum_{d|n}{}'\epsilon(\Lambda_d)\right)Q'=\operatorname{diag}(\epsilon(\zeta),\ \ldots,\ \epsilon(\zeta^n))=D_\epsilon$$

and

$$UQ\left(\sum_{d|n}{}'\epsilon(\Lambda_d)\right)Q'U^*=\epsilon(P)\epsilon G.$$

The mapping $\theta$ is 1–1. Let $\epsilon_1(P)$ and $\epsilon_2(P)$ be elements of $G$ such that the $m$-tuples $\theta(\epsilon_1(P))$ and $\theta(\epsilon_2(P))$ are identical elements of $\mathscr{F}$. Then $\epsilon_1(P)$ and $\epsilon_2(P)$ have the same eigenvalues ordered in the same way, hence $\epsilon_1(P)=\epsilon_2(P)$.

Finally, if $\epsilon(P)$ and $\delta(P)$ are any two elements in $G$, then $\theta(\epsilon(P))\cdot\theta(\delta(P))=(\epsilon(\zeta^{d_1}),\ \ldots,\ \epsilon(\zeta^{d_m}))\cdot(\delta(\zeta^{d_1}),\ \ldots,\ \delta(\zeta^{d_m}))=(\epsilon(\zeta^{d_1})\cdot\delta(^{d_1}),\ \ldots,\ \epsilon(\zeta^{d_m})\cdot\delta(\zeta^{d_m}))=\theta(\epsilon(P)\cdot\delta(P))$, hence $\theta$ preserves multiplication.

COROLLARY 2. *If* $\delta(\mathrm{P})\epsilon\mathrm{G_i}$, $\mathrm{i}=1,\ 2$, *then* $\theta(\epsilon(\mathrm{P}))$ *is an* m*-tuple of elements of* $\mathrm{E_i}$, $\mathrm{i}=1,\ 2$.

PROOF. Assume $\epsilon(P)\epsilon G_1$. Then $\epsilon(P)=\epsilon(P)^*=UD_\epsilon^*U^*=UD_\epsilon U^*$ so that $D_\epsilon=D_\epsilon^*$, which implies $\epsilon(\zeta^k)$, $1\leq k\leq n$, is real.

Assume $\epsilon(P)\epsilon G_2$. Then $D_\epsilon=D_\epsilon^*$ and $D_\epsilon$ is positive definite, hence $\epsilon(\zeta^k)\epsilon E_2$, $1\leq k\leq n$.

In order that the results on aperiodic groups [2, pp. 38–44] can be used it is necessary to consider the restriction of $\theta$ to an aperiodic subgroup $H_1$ of $G$ defined as follows: $H_1$ is the set of elements of $G_1$ all of whose eigenvalues belong to the largest aperiodic subgroup $E_1'$ of $E_1$.

THEOREM 3. *If* $\mathrm{n}\neq\mathrm{p}^\alpha$, *where* p *is a prime and* $\alpha$ *is a positive integer, then* $\theta$ *maps* $\mathrm{H_1}$ *onto the subset* $\mathrm{F_1}$ *of* $\mathscr{F}$ *consisting of* m*-tuples* $(\epsilon(\zeta^{\mathrm{d_1}}),\ \ldots,\ \epsilon(\zeta^{\mathrm{d_m}}))$ *of elements of* $E_1'$. *If* $\mathrm{n}=\mathrm{p}^\alpha$, *then* $\theta$ *maps* $\mathrm{H_1}$ *onto a subset* $\mathrm{F_1'}$ *of* $\mathrm{F_1}$, *where* $\mathrm{F_1'}$ *consists of* m*-tuples of elements of a subgroup* $\mathrm{E_1''}$ *of* $\mathrm{E_1}$ *defined as follows:*

$$\mathrm{E_1''}=\{\epsilon(\zeta)\epsilon\mathrm{E_1'}\,|\,\epsilon(1)\equiv1\ (mod\ \mathrm{p})\},$$

*where* $\epsilon(\mathrm{x})$ *is an integral polynomial such that* $\epsilon(\mathrm{P})$ *is a circulant in* $\mathrm{H_1}$ *with eigenvalues* $\epsilon(\zeta^{\mathrm{k}})$, $1\leq\mathrm{k}\leq\mathrm{n}$.

PROOF. It follows from Corollary 2 that the units in the $m$-tuples of $F_1$ are real. Also, $\epsilon(\zeta^n)=\epsilon(1)=1$ since $\epsilon(\zeta^n)$ is a real eigenvalue of a unimodular matrix with integral coefficients and an element of an aperiodic group. By Lemma 1, any polynomial $\epsilon_t(x)$ of the form $\epsilon_t(x)=\epsilon(x)+t\Phi_n(x)$ and such that $\epsilon_t(P)$ is a circulant in $H_1$ has coefficient sum $\epsilon_t(1)\equiv(1)\ (\mathrm{mod}\ \Phi_n(1))$. The theorem follows from Lemma 2.

Theorems related to the number of basis elements of the aforementioned groups will now be established.

THEOREM 4. *If* $\mathrm{n}=\mathrm{p}^\alpha$, *then* $(\mathrm{F_1}:\mathrm{F_1'})=\mathrm{p}-1$.

PROOF. Let $k$ be an odd primitive root modulo $p$

and define the function $\mu_{2k}(x)$ as follows:

$$\mu_{2k}(x)=\begin{cases}\dfrac{1-x^k}{1-x}\cdot\dfrac{1-x^{-k}}{1-x^{-1}}=x^{1-k}\left(\dfrac{1-x^k}{1-x}\right)^2, & x\neq 1\\ (1+x+\ldots+x^{k-1})^2, & x=1.\end{cases}$$

Then $\mu_{2k}(\zeta)\epsilon E_1$, where $\zeta$ is a primitive $p^\alpha$th root of unity. Let $\mu_k(x)$ be the positive square root of $\mu_{2k}(x)$. Then

$$\mu_k(\nu)=\nu^{\frac{1-k}{2}}\cdot\frac{1-\nu^k}{1-\nu}\epsilon E_1', \text{ for } \nu=\zeta,\ \zeta^p,\ \ldots,\ \zeta^{p^{\alpha-1}},$$

and $\mu_k(1)=k$, hence $\mu_k(1)^r=k^r$.

Now, let $q(x)$ be an integral polynomial such that $(q(\zeta),\ q(\zeta^p),\ \ldots,\ q(\zeta^{p^\alpha}))\epsilon F_1$. Then $(q(1),\ p)=1$. For, if $(q(1),\ p)=p$, then $q(1)=c\cdot p$ for some integer $c$. Consider the polynomial $g(x)=q(x)-c\Phi_{p^\alpha}(x)$. Since $g(1)=0$, $(x-1)|g(x)$ and $q(x)=c\Phi_{p^\alpha}(x)+r(x)(x-1)$, where $r(x)$ is a polynomial with rational integral coefficients. Then $q(\zeta)=r(\zeta)(\zeta-1)$ so that $\pm 1=\Pi q(\zeta)=\Pi r(\zeta)(\zeta-1)=p\Pi r(\zeta)$ where the products are taken over all primitive $p^\alpha$th roots of unity. But this implies $p|1$ which is a contradiction. Thus $(q(1),\ p)=1$ and there exists an $r$, $1\leq r\leq p-1$, such that $q(1)\mu_k(1)^r\equiv 1 \pmod p$. Thus $q(\nu)\cdot\mu_k(\nu)^r\epsilon E_1''$, for this value of $r$ and for $\nu=\zeta,\ \zeta^p,\ \ldots,\ \zeta^{p^\alpha}$, hence $(F_1:F_1')\leq p-1$.

From the above result it follows that $F_1$ can be written as a set theoretic sum with at most $p-1$ summands of the form $\mu_k^i\cdot F_1'$, where $\mu_k^i$ is defined as $\mu_k^i=(\mu_k(\zeta)^i,\ \ldots,\ \mu_k(\zeta^p)^i)\epsilon F_1$ for $0\leq i\leq p-2$. But there must be at least $p-1$ summands. Assume $F_1=\sum_{i=0}^{p-2}\mu_k^i\cdot F_1'$ and $\mu_k^t\cdot F_1'=\mu_k^s\cdot F_1'$, where $0\leq t,\ s\leq p-2$. Then $\mu_k^t\cdot\mu_k^{-s}\epsilon F_1'$ and $\mu_k(1)^t\cdot\mu_k(1)^{-s}=k^{t-s}\equiv 1 \pmod p$. This implies $(p-1)|(r-s)$, hence $r=s$ and $(F_1:F_1')\geq p-1$ which proves the theorem.

NOTE. Let $F=\theta(H)$. Then it is also true that $(F:F_1')=p-1$ since the basis elements of the group $E$ can be chosen to be real.

The following theorem is one of the principal results in this paper.

THEOREM 5. *The number* b(n) *of basis elements of the largest aperiodic subgroup* H *of* G *is given by*

$$\mathrm{b(n)}=\sum_{\substack{d|n\\ d>2}}\left(\tfrac{1}{2}\varphi(\mathrm{d})-1\right)=\left[\frac{\mathrm{n}}{2}\right]+1-\sigma_0(\mathrm{n}),$$

*where* $\sigma_0$(n) *is the number of positive divisors of* n.

PROOF. Let $\epsilon(x)$ be an integral polynomial such that $\epsilon(P)\epsilon H$ has eigenvalues $\epsilon(\zeta),\ \ldots,\ \epsilon(\zeta^n)$ in $E$. Denote the image of $H$ under the mapping $\theta$ by $F$. Then $F$ is an aperiodic subgroup of $\mathfrak{F}$ consisting of $m$-tuples of the form

$$(\epsilon(\zeta^{d_1}),\ \ldots,\ \epsilon(\zeta^{d_m}))=\prod_{j=1}^{m}(1,\ \ldots,\ 1,\ \epsilon(\zeta^{d_j}),\ 1,\ \ldots,\ 1),$$

where $d_1,\ \ldots,\ d_m$ are the positive divisors of $n$. (Note that $\zeta^{d_i}$ is a primitive $\frac{n}{d_i}$th root of unity, $1\leq i\leq m$, and that both $\frac{n}{d_i}$ and $d_i$ run through all positive divisors of $n$.)

Let $d>2$ be a divisor of $n$. The defining polynomial of a primitive $d$th root of unity $\nu$ is $\Phi_d(x)$. This polynomial has $\varphi(d)$ complex roots and no real ones. By Dirichlet's theorem there are $\frac{1}{2}\varphi(d)-1$ basis elements of infinite order in the group of units in $R(\nu)$. (The group is trivial when $d=1$ or 2.) A basis of the aperiodic group $F$, then, consists of $\Sigma(\frac{1}{2}\varphi(d)-1)$ elements, where the summation is over all positive divisors $d$ of $n$ greater than 2, and the first equality is proved.

The second equality can be proved by considering two cases.

(i) $n$ is odd. Then

$$\sum\left(\tfrac{1}{2}\varphi(d)-1\right)=\tfrac{1}{2}\sum\varphi(d)-(\sigma_0(n)-1)=\tfrac{1}{2}(n-1)\sigma_0(n)+1=\left[\frac{n}{2}\right]+1-\sigma_0(n).$$

(ii) $n$ is even. Then

$$\sum\left(\tfrac{1}{2}\varphi(d)-1\right)=\tfrac{1}{2}\sum\varphi(d)-(\sigma_0(n)-2)=\tfrac{1}{2}(n-2)-\sigma_0(n)+2=\left[\frac{n}{2}\right]+1-\sigma_0(n).$$

By a direct application of Theorem 5 it follows that $b(p)=\dfrac{p-3}{2}$, where $p$ is a prime greater than 2, and that $b(2p)=2\cdot b(p)=p-3$. More generally, if $n$ is odd, then $b(2n)=2\cdot b(n)$.

The following table gives the values of $b(n)$ for $1\leq n\leq 16$.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b(n)$ | 0 | 0 | 0 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 4 | 1 | 5 | 4 | 4 | 4 |

Assume $f_1,\ \ldots,\ f_r$ is a basis of $F$. That is, $f_i$, $1\leq i\leq n$, is an $m$-tuple of units of $E$ as defined above. Then bases for $F_1(F_1')$ and $F_2=\theta(H_2)$ of the following form can be found [2]:

$$f_1^{(1)}=f_1^{k}{}_{11}\quad f_2^{k}{}_{12}\cdots f_r^{k}{}_{1r}$$

$$f_2^{(1)}=\quad f_2^{k}{}_{22}\cdots f_r^{k}{}_{2r}$$

$$f_r^{(1)}=\quad f_r^{k}{}_{rr}$$

and

$$f_1^{(2)}=f_1^{(1)1}{}_{11}\quad f_2^{(1)1}{}_{12}\ \ldots\ f_r^{(1)1}{}_{1r}$$

$$f_2^{(2)}=\quad f_2^{(1)1}{}_{22}\ \ldots\ f_r^{(1)1}{}_{2r}$$

$$f_r^{(2)}=\quad f_r^{(1)1}{}_{rr},$$

respectively, where $|k_{11}k_{22} \cdots k_{rr}| = (F:F_1)$ or $(F:F_1')$ and $|1_{11}1_{22} \cdots 1_{rr}| = (F_1:F_2)$ or $(F_1':F_2)$. These bases are not necessarily unique but when one is known it is possible to determine bases for $H$, $H_1$, and $H_2$ by the correspondence in Theorem 2. Then $r = b(n)$. Furthermore it will be shown in Theorem 8 that an upper bound for the value of $|1_{11}1_{22} \cdots 1_{rr}|$, that is, for $(H_1:H_2)$ is $2^r$.

As examples, consider the cases $n=5$ and 7. The case $n=5$ has been worked out by O. Taussky [8] by a different method.

(1) $n=5$. Let $\zeta$ be a primitive 5th root of unity. From Theorem 5, $b(5)=1=r$. Fueter [1, p. 186] showed that $\epsilon(\zeta)=\zeta^2+\zeta^3$ is a fundamental unit of $E$ of infinite order, hence $(\epsilon(\zeta), \epsilon(1))=f_1$ can be chosen as a basis of $F$. From Theorem 4, $(F:F_1')=4$ so that $f_1^{(1)}=f_1^4=(\epsilon(\zeta)^4, \epsilon(1)^4)$, where $\epsilon(\zeta)^4=6+4\zeta+\zeta^2+\zeta^3+4\zeta^4 = 3+\zeta-2\zeta^2-2\zeta^3+\zeta^4$. (Note that, since $\epsilon(1)=2$, the smallest exponent $k$ such that $2^k \equiv 1 \pmod 5$, is $k=4$.) The group of nonzero residues modulo $p$ is cyclic so that $f_1^{(1)}$ can be taken as a basis of $F_1'$ and the circulant $C=[3, 1, -2, -2, 1]$ is a basis of $H_1$. But $C$ is positive definite so that for the case $n=5$, $H_1=H_2$. Furthermore, $C=[1, 0, -1, -1, 0]^2$ which implies that there is only one class of symmetric positive definite unimodular $5\times5$ circulants with respect to congruence over rational integral circulants.

(2) $n=7$. Let $\zeta$ be a primitive 7th root of unity. From Theorem 5, $b(7)=2=r$. Fueter [1, p. 186] showed that $\epsilon(\zeta)=1+\zeta+\zeta^6$ and $\delta(\zeta)=1+\zeta^3+\zeta^4$ are fundamental units of $E$ of infinite order, hence $(\epsilon(\zeta), \epsilon(1))=f_1$ and $(\delta(\zeta), \delta(1))=f_2$ can be chosen as a basis of $F$. From Theorem 4, $(F:F_1')=6$ so that

$$f_1^{(1)}=f_1^{k_{11}} \cdot f_2^{k_{12}}$$

and

$$f_2^{(1)}= \qquad f_2^{k_{22}}.$$

where $|k_{11} \cdot k_{22}|=6$ form a basis of $F_1'$. Since $\delta(1)=3$ it follows that $k_{22}$ must satisfy $3^{k_{22}} \equiv 1 \pmod 7$, hence $k_{22}=6$ and $f_2^{(1)}=f_2^6$ is a basis element of $F_1'$. Also, $k_{11}=\pm1$. Let $k_{11}=1$. Since $\epsilon(1)=3$ it follows that $k_{12}$ must satisfy $3 \cdot 3^{k_{12}} \equiv 1 \pmod 7$, hence $k_{12}=5$ and $f_1^{(1)}=f \cdot f_2^5$ is a second basis element of $F_1'$. Now

$$f_1^{(1)}=113+102\zeta+96\zeta^2+110\zeta^3+110\zeta^4+96\zeta^5+102\zeta^6$$

$$=9-2\zeta-8\zeta^2+6\zeta^3+6\zeta^4-8\zeta^5-2\zeta^6,$$

since $\epsilon(1) \cdot \delta(1)^5=3^6=1+104 \cdot 7$, and

$$f_2^{(1)}=141+96\zeta+71\zeta^2+127\zeta^3+127\zeta^4+71\zeta^5+96\zeta^6$$

$$=37-8\zeta-33\zeta^2+23\zeta^3+23\zeta^4-33\zeta^5-8\zeta^6,$$

since $\delta(1)^6=3^6=1+104.7$.

Thus the circulants

$$C_1=[9, -2, -8, 6, 6, -8, -2]$$

$$C_2=[37, -8, -33, 23, 23, -33, -8]$$

can be taken as a basis of $H_1$.

In a similar manner it can be shown that

$$f_1^{(2)}=f_1^{(1)2} \text{ and } f_2^{(2)}=f_2^{(1)}$$

form a basis of $F_2$ so that

$$D_1=C_1^2=[289, -64, -260, 180, 180, -260, -64]$$

$$D_2=C_2=[37, -8, -33, 23, 23, -33, -8]$$

form a basis of $H_2$. A more convenient choice of basis would be

$$D_1'=C_1^2 \cdot C_2^{-1}=[3, 0, -2, 1, 1, -2, 0]$$

$$D_2'= \qquad C_2=[37, -8, -33, 23, 23, -33, -8].$$

In the latter case,

$$D_1'=[-1, 0, 1, 0, 0, 1, 0]^2$$

$$D_2'=[-3, 1, 3, -2, -2, 3, 1]^2$$

so that there is only one class of symmetric positive definite unimodular $7\times7$ circulants with respect to congruence over rational integral circulants.

*Number of Classes of Circulants.* M. Kneser [3, p. 250] lists the class number of positive definite quadratic forms in $n$ variables for $1 \leq n \leq 16$ and with determinant 1. The number of classes of circulants in $H_2$ is less than or equal to this class number for each $n$. In particular, it is shown that there is only one class $H_2$ for $n \leq 7$. M. Newman and O. Taussky [7] showed there are two classes for $n=8$. In private communications M. Kneser proved there is one class for $n=9$; M. Newman proved there are two classes for $n=12$; and E. C. Dade and O. Taussky found one class for all prime $p<100$ except $p=29$. The number of classes for other values of $n$ is not known but an upper bound can be obtained.

THEOREM 8. $(H_1:H_2) \leq 2^r$, *where* r *is the number of basis elements of* $H_1$.

PROOF: Let $H_0$ be the set of all elements $C$ of $H_1$ such that $C \equiv I$; that is $C=A'A$ where $A$ is an $n\times n$ unimodular rational integral circulant. Then

(i) If $C \epsilon H_1$, then $C^2 \epsilon H_0$ (since $C^2=C'IC$).

(ii) $H_0$ is a subgroup of $H_1$.

(iii) $(H_1:H_0)$ is the number of classes of circulants of $H_1$, where congruence is over the unimodular rational integral circulants.

By Theorem 5, the number of basis elements of $H_1$ is $r=\left[\frac{n}{2}\right]+1-\sigma_0(n)$. If $C_1, \ldots, C_r$ are basis elements

of $H_1$, then because of (i) and (ii) any element $C$ of $H_1$ can be written in the form

$$C = C_1^{\theta_1} \cdot C_2^{\theta_2} \cdot \cdot \cdot C_r^{\theta_r} \cdot C_0$$

where $C_0 \epsilon H_0$ and $\theta_i = 0$ or 1 for $1 \leq i \leq r$. This implies that the order of $H_1/H_0$ is $2^s$ where $s \leq r$, hence $2^r$ is an upper bound for the class number in (iii). But the number of circulants of $H_1$ with respect to integral congruence is not greater than the number of classes with respect to congruence over circulants, so that $2^r$ is actually an upper bound for this class number. Thus $(H_1 : H_0) \leq 2^r$ and since $H_0$ is a subgroup of $H_2$ it follows that $(H_1 : H_2) \leq 2^r$.

## Appendix

The following list includes the notation and definitions of all sets referred to in the paper.

Set Definition

$G$ = All rational integral unimodular $n \times n$ circulants.

$G_1$ = Symmetric elements of $G$.

$G_2$ = Positive definite elements of $G_1$.

$E$ = All units in $R(\zeta)$.

$E_1$ = Real elements of $E$.

$E_2$ = Totally positive elements of $E_1$.

$E_1'$ = Largest aperiodic subgroup of $E_1$.

$E_1'' = \{\epsilon(\zeta) \epsilon E_1' | \epsilon(1) \equiv 1 \pmod{p}\}$.

$H$ = Largest aperiodic subgroup of $G$.

$H_1$ = Elements of $H$ all of whose eigenvalues are elements of $E_1'$.

$H_2 = H_1 \cap G_2$.

$\mathcal{F} = \theta(G) = \{(\epsilon(\zeta^{d_1}), \ . \ . \ ., \ \epsilon(\zeta^{d_m})) | d_1, \ . \ . \ ., \ d_m$ are positive divisors of $n$; $\epsilon(\zeta) \epsilon E\}$.

$F = \theta(H)$.

$F_1' = \theta(H_1)$, when $n \neq p^\alpha, = \{(\epsilon(\zeta^{d_1}), \ . \ . \ ., \ \epsilon(\zeta^{d_m})) | \epsilon(\zeta^{d_i}) \epsilon E_1', \ 1 \leq i \leq m\}$.

$F' = \theta(H_1)$, when $n = p^\alpha, = \{(\epsilon(\zeta^{d_1}), \ . \ . \ ., \ \epsilon(\zeta^{d_m})) | \epsilon(\zeta^{d_i}) \epsilon E_1'', \ 1 \leq i \leq m\}$.

$F_2 = \theta(H_2)$.

## References


[1] R. Fueter, Synthetische Zahlentheorie, Berlin (1921).
[2] E. Hecke, Vorlesungen uber die Theorie der algebraischen Zahlen, Chelsea, New York (1948).
[3] M. Kneser, Klassenzahlen definiter quadratischer formen, Arch. Math. **VIII**, 241–250 (1957).
[4] W. LeVeque, Topics in Number Theory, Vol. **I** (Addison-Wesley, Reading, Mass., 1956).
[5] T. Nagell, Introduction to Number Theory, (John Wiley & Sons, New York, N.Y., 1951).
[6] M. Newman, Circulant quadratic forms, Proc. Boulder Conference, 1959.
[7] M. Newman and O. Taussky, Classes of positive definite unimodular circulants, Canad. J. Math. **9**, 71–73 (1957).
[8] O. Taussky, Unimodular integral circulants, Math. Z. **63**, 286–289 (1955).
[9] H. Zassenhaus, The Theory of Groups (Chelsea, New York, 1949).


(Paper 69B4–160)