Williamson matrices and a conjecture of Ito's

Bernhard, Schmidt.

1999

Bernhard, S. (1999). Williamson matrices and a conjecture of Ito's. Journal of designs codes and cryptography, 17(1-3), 61-68.

<https://hdl.handle.net/10356/92273>

<https://doi.org/10.1023/A:1008398319853>

Designs codes and cryptography © copyright 1999 Springer Netherlands. The journal's website is located at <http://www.springerlink.com/content/m70j6m607k1630g2>.

Downloaded on 26 Apr 2023 08:12:03 SGT

Williamson Matrices and a Conjecture of Ito's

Bernhard Schmidt
Department of Mathematics
253-37 Caltech
Pasadena, CA 91125
email: schmidt@cco.caltech.edu

April 25, 2001

Dedicated to the memory of E.F. Assmus

Abstract

We point out an interesting connection between Williamson matrices and relative difference sets in nonabelian groups. As a consequence, we are able to show that there are relative $(4t, 2, 4t, 2t)$ -difference sets in the dicyclic groups $Q_{8t} = \langle a, b | a^{4t} = b^4 = 1, a^{2t} = b^2, b^{-1}ab = a^{-1} \rangle$ for all t of the form $t = 2^a \cdot 10^b \cdot 26^c \cdot m$ with $a, b, c \geq 0$, $m \equiv 1 \pmod{2}$, whenever $2m - 1$ or $4m - 1$ is a prime power or there is a Williamson matrix over $\mathbb{Z}_m$. This gives further support to an important conjecture of Ito [11] which asserts that there are relative $(4t, 2, 4t, 2t)$ -difference sets in Q_{8t} for every positive integer t . We also give simpler alternative constructions for relative $(4t, 2, 4t, 2t)$ -difference sets in Q_{8t} for all t such that $2t - 1$ or $4t - 1$ is a prime power. Relative difference sets in Q_{8t} with these parameters had previously been obtained by Ito [6]. Finally, we verify Ito's conjecture for all $t \leq 46$.

Keywords: Hadamard matrices, relative difference sets, Williamson matrices, Ito's conjecture, dicyclic groups

1 Introduction

Let G be a group of order m . An $m \times m$ matrix A is called G -invariant if the rows and columns of $A = (a_{g,h})$ can be indexed with elements g, h of G such that $a_{gk,hk} = a_{g,h}$ for all $g, h, k \in G$.

A Hadamard matrix of order v is a $v \times v$ -matrix H with entries ± 1 satisfying $HH^t = vI_v$ where I_v is the identity matrix of size v . It is well known that $v \equiv 0 \pmod{4}$ if a Hadamard matrix of order $v > 2$ exists.

A Hadamard matrix H of order $4m$ is said to be a Williamson matrix over an abelian group G of order m if H is of the form

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix} \quad (1)$$

where A, B, C, D are G -invariant $m \times m$ matrices with entries ± 1 . We remark that this definition slightly differs from the usual one which requires that $XY^t = YX^t$ holds for all 2-subsets $\{X, Y\}$ of $\{A, B, C, D\}$. This property is stronger than the orthogonality of the rows of H .

For the study of Williamson matrices and relative difference sets we will use the following group ring notation. We will always identify a subset A of a group G with the element $\sum_{g \in A} g$ of the integral group ring $\mathbb{Z}[G]$. For $B = \sum_{g \in G} b_g g \in \mathbb{Z}[G]$ we write $B^{(-1)} := \sum_{g \in G} b_g g^{-1}$. We may identify any element $S = \sum_{g \in G} s_g g$ of the group ring $\mathbb{Z}[G]$ with the G -invariant matrix $(m_{g,h})$ where $m_{g,h} = s_{gh^{-1}}$. We note that $S^{(-1)}$ corresponds to the matrix S^t . In terms of the group ring, necessary and sufficient conditions for a matrix of the form (1) to be a Hadamard matrix are

$$AA^{(-1)} + BB^{(-1)} + CC^{(-1)} + DD^{(-1)} = 4m \quad (2)$$

and

$$XY^{(-1)} - X^{(-1)}Y + TZ^{(-1)} - T^{(-1)}Z = 0 \quad (3)$$

for $(X, Y, T, Z) = (A, B, C, D), (A, D, B, C), (A, C, D, B)$.

Let G be a (possibly nonabelian) group of order mn , and let N be a normal subgroup of G of order n . A k -subset R of G is called an (m, n, k, λ) -difference set in G relative to N if every $g \in G \setminus N$ has exactly λ representations

$g = r_1 r_2^{-1}$ with $r_1, r_2 \in R$, and no nonidentity element of N has such a representation. The following is a translation of this definition into the group ring notation.

Lemma 1.1 *A k -subset R of a group G of order mn is a relative (m, n, k, λ) -difference set in G relative to a normal subgroup N of order n if and only if*

$$RR^{(-1)} = k + \lambda(G - N)$$

in $\mathbb{Z}[G]$.

A relative $(4t, 2, 4t, 2t)$ -difference set is a special kind of semiregular relative difference set, see [2, 12]. Such a relative difference set R contains exactly one element of each coset of the subgroup N . Since N has order 2, we may identify N with $\{-1, 1\}$. Let $g_1, \dots, g_{4t}$ be a system of coset representatives of N in G . Let h_{ij} be the unique element of $Rg_i g_j^{-1} \cap N$. Then the definition of a relative difference sets implies that (h_{ij}) is a Hadamard matrix of order $4t$. These Hadamard matrices can also be obtained from 2-cocycles, see [5], and thus are sometimes called cocyclic. Ito [11] conjectured that relative $(4t, 2, 4t, 2t)$ -difference sets in the dicyclic groups $Q_{8t} = \langle a, b | a^{4t} = b^4 = 1, a^{2t} = b^2, b^{-1}ab = a^{-1} \rangle$ exist for all positive integers t . Ito's conjecture is a very interesting strengthening of the outstanding Hadamard conjecture which asserts that a Hadamard matrix of order $4t$ exists for every positive integer $4t$. In [5], Ito's conjecture was shown to be true for $t \leq 11$ by a computer search. We will verify Ito's conjecture for all $t \leq 46$.

2 The connection

Let $Q_8 := \langle x, y | x^4 = y^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle$ be the quaternion group of order 8. We first show that a Williamson matrix over an abelian group G of order m is equivalent to a $(4m, 2, 4m, 2m)$ -relative difference set in $G \times Q_8$ relative to $\langle 1 \rangle \times \langle x^2 \rangle$.

Theorem 2.1 *A Williamson matrix over an abelian group G of order m exists if and only if there is a $(4m, 2, 4m, 2m)$ -relative difference set in $T := G \times Q_8$ relative to $N := \langle 1 \rangle \times \langle x^2 \rangle$.*

Proof Let R be a subset of T containing exactly one element of each coset of N . Write $U := G \times \langle x^2 \rangle$ and $R = E + Fx + Ky + Lxy$ with $E, F, K, L \subset U$. Computing $RR^{(-1)}$ and using Lemma 1.1 we see that R is a $(4m, 2, 4m, 2m)$ -relative difference set in T if and only if

$$EE^{(-1)} + FF^{(-1)} + KK^{(-1)} + LL^{(-1)} = 4m + 2m(U - N) \quad (4)$$

$$E^{(-1)}F + K^{(-1)}L + (EF^{(-1)} + KL^{(-1)})x^2 = 2mU \quad (5)$$

$$FL^{(-1)} + E^{(-1)}K + (EK^{(-1)} + F^{(-1)}L)x^2 = 2mU \quad (6)$$

$$F^{(-1)}K + E^{(-1)}L + (EL^{(-1)} + FK^{(-1)})x^2 = 2mU. \quad (7)$$

Since each of the sets E, F, K, L contains exactly one element of each coset of N in U , we can write $X = X_1 + X_2x^2$ with $X_1, X_2 \subset G$ and $X_1 + X_2 = G$ for $X = E, F, K, L$. Define $A := E_1 - E_2$, $B := F_1 - F_2$, $C := K_1 - K_2$, $D := L_1 - L_2$. It is straightforward to verify that equations (4) through (7) hold if and only if A, B, C, D satisfy (2) and (3) which proves Theorem 2.1. For instance, assume that A, B, C, D satisfy (2). We will show that this implies (4). We have to show

$$\chi(EE^{(-1)} + FF^{(-1)} + KK^{(-1)} + LL^{(-1)}) = \chi(4m + 2m(U - N)) \quad (8)$$

for all characters χ of U . If χ is trivial on $N = \langle x^2 \rangle$, then (8) follows from the fact that E, F, K, L contain exactly one element of each coset of N in U . If χ is nontrivial on N , then $\chi(x^2) = -1$ implying $\chi(E) = \chi|_G(A)$, $\chi(F) = \chi|_G(B)$, $\chi(K) = \chi|_G(C)$, and $\chi(L) = \chi|_G(D)$. Thus (8) follows from (2) in this case. The proof of all remaining implications is similar. $\square$

Let G be an abelian group of order m . By $Q(G)$ we denote the semidirect product of G with the quaternion group $Q_8 = \langle x, y | x^4 = y^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle$ which is given by $G \triangleleft Q(G)$, $x^{-1}gx = g$ and $y^{-1}gy = g^{-1}$ for all $g \in G$. Note that for odd m , the dicyclic group $Q_{8m} := \langle a, b | a^{4m} = b^4 = 1, a^{2m} = b^2, b^{-1}ab = a^{-1} \rangle$ coincides with $Q(\mathbb{Z}_m)$. By the same arguments as in the proof of Theorem 2.1 we obtain the following.

Theorem 2.2 *Let G be an abelian group of order m . A $(4m, 2, 4m, 2m)$ -difference set in $Q(G)$ relative to $\langle y^2 \rangle$ exists if and only if there is a Hadamard matrix of the form*

$$\begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C^t & D^t & A^t & -B^t \\ -D^t & -C^t & B^t & A^t \end{pmatrix} \quad (9)$$

where A, B, C, D are G -invariant $m \times m$ matrices with entries ± 1 .

Note that a matrix of the form (9) is a Hadamard matrix if and only if $AA^{(-1)} + BB^{(-1)} + CC^{(-1)} + DD^{(-1)} = 4m$ and $A^{(-1)}B - AB^{(-1)} + C^{(-1)}D - CD^{(-1)} = 0$ in the group ring. These conditions are weaker than (2) and (3) and thus we get the following result, a special case of which was obtained in [8, Prop. 3].

Corollary 2.3 *The existence of a Williamson matrix over an abelian group G implies the existence of $(4m, 2, 4m, 2m)$ -relative difference sets in $G \times Q_8$ and $Q(G)$.*

3 Relative difference sets in Q_{8m}

We want to study relative $(4m, 2, 4m, 2m)$ -difference sets in dicyclic groups $Q_{8m} = \langle a, b \mid a^{4m} = b^4 = 1, a^{2m} = b^2, b^{-1}ab = a^{-1} \rangle$ in more detail. The following lemma is from [11]. For the convenience of the reader, we include a proof.

Lemma 3.1 *A $(4m, 2, 4m, 2m)$ -difference set in Q_{8m} relative to $N := \langle b^2 \rangle$ exists if and only if there are polynomials f, g of degree $2m-1$ and coefficients ± 1 only such that*

$$f(x)f(x^{-1}) + g(x)g(x^{-1}) \equiv 4m \pmod{x^{2m} + 1}. \quad (10)$$

Proof Let R be a subset of Q_{8m} containing exactly one element of each coset of N and write $R = F + Gb$ with $F, G \subset \langle a \rangle$. Computing $RR^{(-1)}$ and applying Lemma 1.1 shows that R is a $(4m, 2, 4m, 2m)$ -difference set in Q_{8m} relative to N if and only if

$$FF^{(-1)} + GG^{(-1)} = 4m + 2m(\langle a \rangle - N). \quad (11)$$

The equivalence of (10) and (11) can be verified by using the characters of $\langle a \rangle$ similar to the proof of Theorem 2.1. $\square$

We recall that a pair of Golay polynomials is a pair of polynomials f, g of degree $2m - 1$ and coefficients ± 1 only such that

$$f(x)f(x^{-1}) + g(x)g(x^{-1}) = 4m \quad (12)$$

in $\mathbb{Z}[x, x^{-1}]$. Golay polynomials of degree $2m - 1$ are known for all m such that $2m = 2^r \cdot 10^s \cdot 26^t$ with $r, s, t \geq 0$, see [4], and it is conjectured that there are no Golay polynomials for any other m . Of course, Lemma 3.1 shows that the existence of a pair of Golay polynomials of degree $2m - 1$ implies the existence of a $(4m, 2, 4m, 2m)$ -relative difference set in Q_{8m} , but we can say more. The following construction is based on the observation that an idea of Turyn [15, Lemma 5] still works in a slightly more general situation.

Theorem 3.2 *If there is a pair k, l of Golay polynomials of degree $2m - 1$, and if there is a $(4m', 2, 4m', 2m')$ -relative difference set in $Q_{8m'}$ relative to $\langle b^2 \rangle$, then there is also an $(8mm', 2, 8mm', 4mm')$ -difference set in $Q_{16mm'}$ relative to $\langle b^2 \rangle$.*

Proof Let u, w be the polynomials corresponding to the relative difference set in $Q_{8m'}$ via Lemma 3.1. Define

$$\begin{aligned} f(x) : &= \frac{1}{2} \left\{ u(x^{2m})[k(x) + l(x)] + x^{4mm' - 2m} w(x^{-2m})[k(x) - l(x)] \right\}, \\ g(x) : &= \frac{1}{2} \left\{ w(x^{2m})[k(x) + l(x)] + x^{4mm' - 2m} u(x^{-2m})[-k(x) + l(x)] \right\}. \end{aligned}$$

It is easy to check that f and g are polynomials of degree $4mm' - 1$ with coefficients $-1, 1$ only. We compute

$$\begin{aligned} f(x)f(x^{-1}) + g(x)g(x^{-1}) &= \frac{1}{2} [k(x)k(x^{-1}) + l(x)l(x^{-1})] \cdot \\ &\quad [u(x^{2m})u(x^{-2m}) + w(x^{2m})w(x^{-2m})] \\ &= 2m[u(x^{2m})u(x^{-2m}) + w(x^{2m})w(x^{-2m})] \\ &\equiv 8mm' \pmod{x^{4mm'} + 1} \end{aligned}$$

since $k(x)k(x^{-1}) + l(x)l(x^{-1}) = 4m$ and $u(x)u(x^{-1}) + w(x)w(x^{-1}) \equiv 4m' \pmod{x^{2m'} + 1}$. By Lemma 3.1, f and g describe the desired relative difference set. $\square$

Ito [6] constructed relative $(4t, 2, 4t, 2t)$ -difference sets in Q_{8t} for all t such that $4t-1$ is a prime power. This construction is of special interest since these relative difference sets *cannot* be derived from known families of Williamson matrices. It is not known whether Williamson matrices of order $4t$, $4t-1$ a prime power, exist in general. A computer search [3] showed that there is no Williamson matrix of order $4 \cdot 35$ such that the four matrices A, B, C, D are *symmetric*. However, it seems quite plausible that (without the symmetry condition) Williamson matrices exist for all orders $4t$ even for general t . In the following, we give a simpler alternative to Ito's construction of relative $(4t, 2, 4t, 2t)$ -difference sets in Q_{8t} for all t such that $4t-1$ is a prime power.

Theorem 3.3 ([6]) *There is a relative $(4t, 2, 4t, 2t)$ -difference set in Q_{8t} for all t such that $q := 4t-1$ is a prime power.*

Proof Let U be the subgroup of order $(q-1)/2$ of $\mathbb{F}_{q^2}^*$ where $\mathbb{F}_{q^2}$ is the finite field of order q^2 . Let tr denote the trace function of $\mathbb{F}_{q^2}$ relative to $\mathbb{F}_q$. We choose $\alpha \in \mathbb{F}_{q^2}$ with $tr(\alpha) = 0$ and denote the set of nonzero squares in $\mathbb{F}_q$ by Q . Then [12, Thm. 2.2.12] implies that

$$R := \{Ux : tr(\alpha x) \in Q\}$$

is a relative $(q+1, 2, q, (q-1)/2)$ -difference set in $W := \mathbb{F}_{q^2}^*/U$. Let g be a generator of W and write

$$R = R_1 + R_2g \tag{13}$$

with $R_i \subset \langle g^2 \rangle$. Lemma 1.1 implies

$$R_1R_1^{(-1)} + R_2R_2^{(-1)} = q + \frac{q-1}{2}(\langle g^2 \rangle - \langle g^{4t} \rangle). \tag{14}$$

If the multiplicative order of $d \in \mathbb{F}_{q^2}^*$ divides $q+1$, then $tr(\alpha d) = \alpha d + \alpha^q d^q = \alpha d - \alpha d^{-1} = -tr(\alpha d^{-1})$ since $tr(\alpha) = 0$. Thus $R_1^{(-1)} = g^{4t}R_1$. Note $1 \notin R_1$ since $tr(\alpha) = 0$. Thus

$$R_1 + R_1^{(-1)} = \langle g^2 \rangle - \langle g^{4t} \rangle. \tag{15}$$

We identify the cyclic subgroup of order $4t$ of Q_{8t} with $\langle g^2 \rangle$, i.e. we write $Q_{8t} = \langle a, b \mid a^{4t} = b^4 = 1, a^{2t} = b^2, b^{-1}ab = a^{-1} \rangle$ with $a = g^2$. Define $S := (R_1 + 1) + R_2b \in \mathbb{Z}[Q_{8t}]$. Using Lemma 1.1, equations (14), (15), and the

fact that both $R_1 + 1$ and R_2 contain exactly one element of each coset of $N := \langle a^{2t} \rangle$ in $\langle a \rangle$, it is straightforward to verify that S is a $(4t, 2, 4t, 2t)$ -difference set in Q_{8t} relative to N . $\square$

Remark 3.4 The arguments above can be used to give an interesting proof of the well known number theoretic fact that every prime power $q \equiv 3 \pmod{8}$ is a sum of three odd squares two of which are equal. To see this, we first note that $t = (q+1)/4$ is odd if $q \equiv 3 \pmod{8}$. Thus we may write $R = R_1 + R_2 g^t$ with $R_i \subset \langle g^2 \rangle$ instead of (13). From the proof of Theorem 3.3 we know

$$R_1^{(-1)} = R_1 h \quad (16)$$

where $h := g^{4t}$. In the same way, we obtain

$$(R_2 g^t)^{(-1)} = R_2 g^t. \quad (17)$$

Now we write $R_1 = X_1 + X_2 g^{2t}$ and $R_2 = X_3 + X_4 g^{2t}$ with $X_i \subset \langle g^4 \rangle$. From (16) and (17) we get

$$\begin{aligned} X_1^{(-1)} &= X_1 h, \\ X_3^{(-1)} &= X_4 h. \end{aligned} \quad (18)$$

Equation (14) implies

$$\sum_{i=1}^4 X_i X_i^{(-1)} = q + \frac{q-1}{2} (\langle g^4 \rangle - \langle h \rangle). \quad (19)$$

Let χ be a character of $\langle g \rangle$ of order eight. Then $\chi(h) = -1$ and $\chi(f) = \chi(f^{-1}) \in \{-1, 1\}$ for all $f \in \langle g^4 \rangle$. Thus $\chi(X_i) = \chi(X_i^{(-1)})$ for all i . Moreover, $\chi(X_1) = 0$ and $\chi(X_3) = -\chi(X_4)$ by (18). Note that $\chi(X_i)$ is odd for $i = 2, 3, 4$ since X_i has exactly t elements for $i = 2, 3, 4$. Now (19) implies

$$q = \chi(X_2)^2 + 2\chi(X_3)^2$$

which is the desired decomposition of q into the sum of three odd squares.

Ito [7] obtained relative $(4t, 2, 4t, 2t)$ -difference sets in Q_{8t} for all t such that $q := 2t - 1 \equiv 1 \pmod{4}$ is a prime power. We give a simpler alternative construction which also works for $q \equiv 3 \pmod{4}$.

Theorem 3.5 *There is a relative $(4t, 2, 4t, 2t)$ -difference set in Q_{8t} for all t such that $q := 2t - 1$ is a prime power.*

Proof Let $G = \langle a \rangle$ be cyclic of order $4t$. By [12, Thm. 2.2.12] there is a $(q + 1, 2, q, (q - 1)/2)$ -difference set R in G relative to $N := \langle a^{2t} \rangle$. Replacing R by Rg for some appropriate $g \in G$ if necessary, we may assume $R \cap N = \emptyset$. We define

$$S := (R + 1) + (R + a^{2t})b \in \mathbb{Z}[Q_{8t}]$$

where $Q_{8t} = \langle a, b \mid a^{4t} = b^4 = 1, a^{2t} = b^2, b^{-1}ab = a^{-1} \rangle$. Using Lemma 1.1 it is straightforward to verify that S is the desired relative difference set. $\square$.

Combining Corollary 2.3 and Theorems 3.2, 3.3, 3.5, we get the following result.

Corollary 3.6 *Let m be a positive integer such that $2m - 1$ or $4m - 1$ is a prime power or m is odd and there is a Williamson matrix over $\mathbb{Z}_m$. Then there is a relative $(4t, 2, 4t, 2t)$ -difference set in Q_{8t} for every t of the form*

$$t = 2^a \cdot 10^b \cdot 26^c \cdot m$$

with $a, b, c \geq 0$.

Remark 3.7 Williamson matrices over $\mathbb{Z}_m$ are known for many m including all m of the form $m = q^r(q + 1)/2$ where $q \equiv 1 \pmod{4}$ is a prime power and r is any nonnegative integer, see [13, 14, 16]. Moreover, Williamson matrices over $\mathbb{Z}_m$ exist for all $m \leq 33$ and for $m = 39, 43$, see [1, 3].

In [5], a computer search was carried out which showed that $(4t, 2, 4t, 2t)$ -difference sets in Q_{8t} exist for $t \leq 11$. Combining Corollary 3.6 and Remark 3.7 we can improve this result considerably.

Corollary 3.8 *There are relative $(4t, 2, 4t, 2t)$ -difference sets in Q_{8t} for all $t \leq 46$.*

Acknowledgement

I would like to thank Thomas Kölmel for several useful discussions and for convincing me that Ito's conjecture is true.

References

- [1] L.D. Baumert: Hadamard matrices of Williamson type. *Math. Comp.* 19 (1965), 442-447.
- [2] J.A. Davis and J. Jedwab: A unifying construction of difference sets. *J. Combin. Theory A* 80 (1997), 13-78.
- [3] D.Z. Dokovic: Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete Math.* 115 (1993), 267-271.
- [4] S. Eliahou, M. Kervaire, B. Saffari: A new restriction on the length of Golay complementary sequences. *J. Comb. Theory A* 55 (1990), 49-59.
- [5] D.L. Flannery: Cocyclic Hadamard Matrices and Hadamard Groups are Equivalent. *J. Algebra* 192 (1997), 749-779.
- [6] N. Ito: On Hadamard groups. *J. Algebra* 168 (1994), 981-987.
- [7] N. Ito: On Hadamard groups, II. *J. Algebra* 169 (1994), 936-942.
- [8] N. Ito: Some remarks on Hadamard groups. In: *Groups-Korea 94*, de Gruyter, Berlin/New York 1995, 149-155.
- [9] N. Ito: Remarks on Hadamard groups. *Kyushu J. Math.* 50 (1996), 83-91.
- [10] N. Ito: Remarks on Hadamard groups, II. *Rep. Fac. Sci. Technol. Meijo Univ. No. 37* (1997), 1-7.
- [11] N. Ito: On Hadamard groups III. *Kyushu J. Math.* 51 (1997), 369-379.
- [12] A. Pott: *Finite geometry and character theory*. Springer Lecture Notes 1601, New York (1995).
- [13] E. Spence: An Infinite Family of Williamson Matrices. *J. Austral. Math. Soc.* 24 A (1977), 252-256.
- [14] R.J. Turyn: An infinite class of Williamson matrices. *J. Combin. Theory A* 12 (1972), 319-321.

- [15] R.J. Turyn: Hadamard Matrices, Baumert-Hall Units, Four-Symbol Sequences, Pulse Compression, and Surface Wave Encodings. J. Comb. Theory A 16 (1974), 313-333.
- [16] A.L. Whiteman: An infinite family of Hadamard matrices of Williamson type. J. Combin. Theory A 14 (1973), 334-340.
- [17] J. Williamson: Hadamard's determinant problem and the sum of four squares. Duke Math. J. 11 (1944), 65-81.