Journal of the Mathematical Society of Japan Vol. 6, Nos. 3～4, December, 1954

On a conjecture of Kaplansky on quadratic forms

By Tosirô TSUZUKU

(Received April 20, 1654)

In his recent paper[1] Kaplansky took up some problems on quadratic forms over a not formally real field of characteristic different from two. Among others he made the following conjecture: Let F be a field of characteristic different from two which is not formally real, and let the multiplicative group of non-zero elements of F modulo squares be pricisely of order n. Then every quadratic form in $n+1$ variables over F represents zero (non-trivally). He affirmed this conjecture in the following two special caces: (1) $n\leqq 8$, (2) -1 is a sum of four or less squares in F. In the present paper we shall show on modifying and refining Kaplansky's methods that his conjecture is true; in fact we shall prove a more finer statement.

The writer wishes to express his gratitude to Prof. T. Nakayama and Mr. T. Ono for their valuable suggestions.

Let F be a field of characteristic different from two which is not formally real (that is, -1 is a sum of squares in F). We shall fix this field throughout this paper. After Kaplansky, we define three invariants of F as follows;

(a) A is the order of the multiplicative group of non-zero elements of F moduls squares. A may be infinite; if it is finite it is evidently a power of 2.

(b) B is the smallest integer n such that -1 is a sum of n squares in F.

(c) C is the smallest integer n such that every quadratic form in $n+1$ variables over F is a null form (i.e. a form which represents zero non-trivially).

On the value of B, we have the following

---

1) I. Kaplansky, "Quadratic forms" J. Math. Soc. Japan, vol. 5 (1953) pp. 200-207. We refer of this paper as K. Q.

PROPOSITION 1. (*Kaplansky*) *$B=1,2,4$ or a multiple of* 8[2)]

About the relationship of A and B, we prove the following

PROPOSITION 2.[3)] *If $B>1$, then*

$$A \geq \left[\frac{B}{B}\right]+\left[\frac{B}{B-1}\right]+\left[\frac{B}{B-2}\right]+\cdots+\left[\frac{B}{3}\right]+\left[\frac{B}{2}\right]+1$$

(*$[*]$ means the integral part of $*$*).

PROOF. Set $-1=a_1^2+a_2^2+\cdots+a_B^2$ with B minimal. Let σ and δ be any two partial sums of this expresion of -1, say $\sigma=a_{\sigma_1}^2+\cdots+a_{\sigma_i}^2$ and $\delta=a_{\delta_1}^2+\cdots+a_{\delta_j}^2$.

1° If $i\neq j$, then σ and δ must be in different classes of non-zero elements modulo squares, for otherwise the representation of -1 could be shortened.

2° If $1<i=j$ and $\{\sigma\}\cap\{\delta\}=\emptyset$ where $\{\sigma\}$ and $\{\delta\}$ denote the sets of indices $\sigma_1,\cdots,\sigma_i$ and $\delta_1,\cdots,\delta_j$ respectively, then σ and δ must be in different classes of non-zero elements modulo squares. Indeed, if σ and δ are in the same class of non-zero elements modulo squares, then we may write $\sigma=\delta\cdot a^2, a\in F$. Hence we get $\sigma+\delta=\delta(1+a^2)$. Here, by the assumption $\{\sigma\}\cap\{\delta\}=\emptyset$, $\sigma+\delta$ is a partial sum of $2i$ squares in the above expression of -1. On the other hand, $\delta(1+a^2)$ is the sum of i or $i+1$ squares according as i is even or odd. Since $2i>i+1$ by our assumption $i>1$, -1 is expressed as sum of $B-1$ or less squares.

From 1° and 2° we get our proposition easily.

As an immediate consequence of this proposition we have

COROLLARY 3. *If $A>2$, then $B<A$* [4)]

As for the relations of A, B and C, we prove the following

PROPOSITION 4.[5)]

(1) *$C\leq AB$ for any B.*
(2) *$C\leq AB/2$ if $B\geq 2$.*
(3) *$C\leq AB/4$ if $B\geq 4$.*
(4) *$C\leq A(B+2^{2t-1}+2^t-2)/2^{2t}$ if $2^{t+1}>B\geq 2^t$, $t>2$.*
(5) *$C\leq A(B+2^{3t-3}+2^{2t-2}+2^t-6)/2^{3t-1}$ if $2^{t+1}>B\geq 2^t$, $t>3$.*

2) The proof of this proposition is in K. Q.
3) This proposition is a refinement of Theorem 4 in K. Q.
4) This is Theorem 4 in K. Q.
5) This is a refinement of Theorem 5 in K. Q.

PROOF. (1), (2) and (3) are proved in K. Q. So we shall prove (5), and indicate the modifications needed in proving (4) (which is easier than (5)).

Let F^* be the multiplicative group of non-zero elements in F. We denote by G the group $F^*/(F^*)^2$ and by $<a>$ the element of G represented by $a \in F^*$. By definition G is a group of order A. If $2^{t+1} > B \geqq 2^t$, then we may construct in a similar way as in the proof of proposition 2 a subgroup H_0 of G of order 2^t such that each element of H_0 is the sum of at most two squares. In fact, write $-1 = a_1^2 + \cdots + a_B^2$ with B minimal. (We shall fix this expression of -1 throughout the present proof.) Then $\frac{B}{2}$ $(\geqq 2^{t-1})$ elements $<a_1^2+a_2^2>$, $<a_3^2+a_4^2>$, $\cdots$, $<a_{B-1}^2+a_B^2>$ of G are different from each other (and from $<1>$), and therefore the order of the subgroup of G which is generated by these elements is at least 2^t. Each element of this subgroup is a sum of at most two squares (because a sum of two squares times a sum of two squares is a sum of two squares). Thus we have a subgroup H_0 of order 2^t such that each elements is a sum of at most two squares. By $<1>$, $<c_1>$, $<c_2>$, $\cdots$, $<c_{2^t-1}>$ we denote all the elements of H_0. Let H_1 be the subgroup of G generated by H_0 and $<-1>$. Since $<-1>$ is not in H_0, the order of H_1 is 2^{t+1}. Now, we consider the partial sum $a_1^2+a_2^2+a_3^2+a_4^2$ of the above fixed expression of -1 and denote it by d_1. Since $<d_1>$ is not in H_1, the order of the subgroup H_2 of G generated by H_1 and $<d_1>$ is 2^{t+2}. Similarly if we put $d_2 = a_5^2+a_6^2+a_7^2+a_8^2$, then $<d_2>$ is not in H_2. For, if $H_2 \ni <d_2>$, then $<d_2> = \pm <1>$, $\pm <c_i>$ or $\pm <d_1><c_i>$ and in each case we would obtain a shorten expression of -1 (as a sum of squares); observe that a sum of four squares times a sum of four squares is again a sum of four squares. Thus we obtain the subgroup H_3 of order 2^{t+3} of G which is generated by H_2 and $<d_2>$. Furthermore, on observing $B \geqq 2^t > 8$ by assumption, we consider $a_9^2+a_{10}^2+a_{11}^2+a_{12}^2$. Generally we cannot say that $<a_9^2+a_{10}^2+a_{11}^2+a_{12}^2>$ is outside of H_3. But either $<a_9^2+a_{10}^2+a_{11}^2+a_{12}^2>$ or $<a_{13}^2+a_{14}^2+a_{15}^2+a_{16}^2>$ is not in H_3. For, firstly, the above argument shows that $<a_9^2+a_{10}^2+a_{11}^2+a_{12}^2>$ and $<a_{13}^2+a_{14}^2+a_{15}^2+a_{16}^2>$ are different from $\pm <1>$, $\pm <c_i>$, $\pm <d_j>$, $\pm <d_j><c_i>$, $1 \geqq i \geqq 2^t-1$, $j=1$, 2. Further, $<a_9^2+a_{10}^2+a_{11}^2+a_{12}^2>$ can not be equal to $-<d_1><d_2>$ or $-<d_2><d_2><c_i>$ and $<a_{13}^2+a_{14}^2+a_{15}^2+a_{16}^2>$ can not be equal to $-\langle d_1\rangle\langle d_2\rangle$ or $-\langle d_1\rangle\langle d_2\rangle\langle c_j\rangle$, for in either case -1 would be a sum of less than eight squares. Therefore if both $\langle a_9^2+a_{10}^2+a_{11}^2+a_{12}^2\rangle$ and $\langle a_{13}^2+a_{14}^2+a_{15}^2+a_{16}^2\rangle$ were in H_3, we should have $\langle a_9^2+a_{10}^2+a_{11}^2+a_{12}^2\rangle=\langle d_1\rangle\langle d_2\rangle$ or $\langle d_1\rangle\langle d_2\rangle\langle c_i\rangle$ and $\langle a_{13}^2+a_{14}^2+a_{15}^2+a_{16}^2\rangle=\langle d_1\rangle\langle d_2\rangle$ or $\langle d_1\rangle\langle d_2\rangle\langle c_j\rangle$. In either case $\langle a_9^2+a_{10}^2+\cdots+a_{15}^2+a_{16}^2\rangle=\langle d_1\rangle\langle d_2\rangle\langle$a sum of at most 4 squares$\rangle$ $=\langle$a sum of at most 4-squares$\rangle$ and the expression of -1 could be shortend. Thus either $\langle a_9^2+a_{10}^2+a_{11}^2+a_{12}^2\rangle$ or $\langle a_{13}^2+a_{14}^2+a_{15}^2+a_{16}^2\rangle$ is not in H_3. Denote it by d_3 and let H_4 be the subgroup of G which is generated by H_4 and $\langle d_3\rangle$. The order of H_4 is 2^{t+4}.

Now, for a natural number k with $B\geqq 4k$, assume that we have a subgroup H_{k+1} of order 2^{t+k+1} of G generated by $H_1, \langle d_1\rangle, \cdots, \langle d_k\rangle$, where each d_i is a partial sum of four terms in our expresion of -1 and different d_i have no common term. We may suppose $-1=d_1+d_2+\cdots+d_k+a_{4k+1}^2+\cdots+a_B^2$ by enumerating a_i suitably. If here $B\geqq 4k+4(2^k-k)=2^{k+2}$, then we see, in the same way as above, that for at least one of $a_{4k+1}^2+\cdots+a_{4k+4}^2$, $a_{4k+5}^2+\cdots+a_{4k+8}^2$, $\cdots$, $a_{4k+4(2^k-k-1)+1}^2+\cdots+a_{4k+4(2^k-k)}^2$ its class modulo squares is outside of H_{k+1}. For, otherwise each of those 2^k-k classes would be either a product of at least two $\langle d\rangle$'s or a product of at least two $\langle d\rangle$'s and one $\langle c_i\rangle$. But the number of the products of at least two $\langle d\rangle$'s is $\binom{k}{k}+\binom{k}{k-1}+\cdots+\binom{k}{2}=2^k-k-1$. Therefore, there should exist two among our classes, say $\langle a_{4r+1}^2+\cdots+a_{4r+4}^2\rangle$ and $\langle a_{4s+1}^2+\cdots+a_{4s+4}^2\rangle$ $(r\neq s)$, such that $\langle a_{4r+1}^2+\cdots+a_{4r+4}^2\rangle=\langle d_{i_1}\rangle\cdots\langle d_{i_\kappa}\rangle$ or $\langle d_{i_1}\rangle\cdots\langle d_{i_\kappa}\rangle\langle c_i\rangle$, $\langle a_{4s+1}^2+\cdots+a_{4s+4}^2\rangle=\langle d_{i_1}\rangle\cdots\langle d_{i_\kappa}\rangle$ or $\langle d_{i_1}\rangle\cdots\langle d_{i_\kappa}\rangle\langle c_j\rangle$, with a common set $d_{i_1},\cdots, d_{i_\kappa}$. Then

$$\begin{aligned}&\langle a_{4r+1}^2+\cdots+a_{4r+4}^2+a_{4s+1}^2+\cdots+a_{4s+4}^2\rangle\\ &=\langle d_{i_1}\rangle\cdots\langle d_{i_\kappa}\rangle\langle\text{the sum of at most four squares}\rangle\\ &=\langle\text{the sum of at most four squares}\rangle\end{aligned}$$

and the expression of -1 could be shortend. Therefore at least one of our classes is not in H_{k+1}. Denoting the corresponding sum of four elements by d_{k+1}, we get a subgroup H_{k+2} of order 2^{t+k+2} of G which is generated by H_{k+1} and $\langle d_{k+1}\rangle$. In this way, for the maximum k such that $B/4\geqq k+2^k-k=2^k$, we can form a subgroup $H_{k+2}=\{H_1,\langle d_1\rangle, \cdots,\langle d_{k+1}\rangle\}$ of order 2^{t+k+2} of G. If $2^{t+1}>B\geqq 2^t$, then $k=t-2$. Thus we can form the subgroup $H_t=\{H_1,\langle d_1\rangle,\cdots,\langle d_{t-1}\rangle\}$ of order 2^{2t} of

G. Obviously, each element of H_t is a sum of at most 4 squares.

Next, on considering the partial sums of eight squares in our fixed expression of -1 instead of the sum of four squares, we can form in a similar manner as above a subgroup $H=\{H_t, \langle e_1\rangle, \cdots, \langle e_{t-2}\rangle\}$ of order $2^{2t+t-2}=2^{3t-2}$ of G where each e_σ is a partial sum $a_{\sigma_1}^2+a_{\sigma_2}^2+\cdots+a_{\sigma_8}^2$ of eight term in our fixed expression of -1 and for $\sigma\neq\tau$ e_σ and e_τ have no common term; we omit details. Denote the elements of H by $\pm\langle 1\rangle, \pm\langle c_i\rangle, \pm\langle d_{j_1}\rangle\cdots\langle d_{j_s}\rangle, \pm\langle d_{j_1}\rangle\cdots\langle d_{j_s}\rangle\langle c_i\rangle$,
$\pm\langle e_{k_1}\rangle\cdots\langle e_{k_r}\rangle, \pm\langle e_{k_1}\rangle\cdots\langle e_{k_r}\rangle\langle c_i\rangle$,
$\pm\langle e_{k_1}\rangle\cdots\langle e_{k_r}\rangle\langle d_{j_1}\rangle\cdots\langle d_{j_s}\rangle$ and
$\pm\langle e_{k_1}\rangle\cdots\langle e_{k_r}\rangle\langle d_{j_1}\rangle\cdots\langle d_{j_s}\rangle\langle c_i\rangle$ where $i=1, \cdots, 2^t-1, 1\leqq s\leqq t-1, 1\leqq r\leqq t-2$.

Now let there be given a quadratic form $f=\sum b_i x_i^2$ in $A(B+2^{3t-3}+2^{2t-2}+2^t-6)/2^{3t-2}$ variables. If we map the coefficents b_i of f into G/H of order $A/2^{3t-2}$ by natural mapping $b_i\to\langle b_i\rangle$ mod H, at least $B+2^{3t-2}+2^{2t-2}+2^t-6$ of the b's must be mapped into a same class, in G/H. After multiplying by a suitable constant, we may assume that $B+2^{3t-3}+2^{2t-2}+2^t-6$ of b's are actually in H. We denote these element by $b_{\lambda(i)}, i=1, \cdots, B+2^{3t-3}+2^{2t-2}+2^t-6$. Now if $\langle c_i\rangle$ (or $-\langle c_i\rangle$, $\pm\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle c_i\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$) occurs twice among $\langle b\rangle$'s that is, if for some k_1, k_2 $(\neq)$ $\langle b_{\lambda(k_1)}\rangle=\langle b_{\lambda(k_2)}\rangle=\langle c_i\rangle$ (or $-\langle c_i\rangle$, $\pm\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle c_i\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$), the $(b_{\lambda(k_1)}, b_{\lambda(k_2)})$[6] $\sim(c_i, c_i)\sim(1,1)$ (or $-(1,1)$, $\pm(d_{\sigma_1}\cdots d_{\sigma_s}, d_{\sigma_1}\cdots d_{\sigma_s})$, $(e_{\tau_1}\cdots e_{\tau_r}, e_{\tau_1}\cdots e_{\tau_r})$, $(e_{\tau_1}\cdots e_{\tau_r}\cdot d_{\sigma_1}\cdots d_{\sigma_s}, e_{\tau_1}\cdots e_{\tau_r}\cdot d_{\sigma_1}\cdots d_{\sigma_s})$. Hence, on transforming f to a congruent form, we can assume that each of $\pm\langle c_i\rangle$, $\pm\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ occurs at most once among $\langle b\rangle$'s. Further, if $\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ (or $-\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$) occurs 4-times among $\langle b\rangle$'s, that is, if for some k_1, k_2, k_3, k_4 $\langle b_{\lambda(k_1)}\rangle=\langle b_{\lambda(k_2)}\rangle=\langle b_{\lambda(k_3)}\rangle=\langle b_{\lambda(k_4)}\rangle=\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ (or $-\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$), then $(b_{\lambda(k_1)}, b_{\lambda(k_2)}, b_{\lambda(k_3)}, b_{\lambda(k_4)})\sim(d_{\sigma_1}\cdots d_{\sigma_s}, *, *, d_{\sigma_1}\cdots d_{\sigma_s})\sim(1,1,1,1)$ (or $-(1,1,1,1)$, $\pm(e_{\tau_1}\cdots e_{\tau_r}, *, *, e_{\tau_1}\cdots e_{\tau_r})$). Hence, on transforming f to

6) $(a_1, \cdots, a_n)$ stands for the quadratic form $\sum a_i x_i^2$. Equivalence of quadratic forms $(a_1, \cdots, a_n)$, $(b_1, \cdots, b_n)$ (or congruence of the corresponding matrices) will be indicated by $(a_1, \cdots, a_n)\sim(b_1, \cdots, b_n)$.

a congruent form, we can assume that each of $\pm\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ occurs at most 3 times among $\langle b\rangle$'s. Finally if $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$ (or $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$) occurs 8-times among $\langle b\rangle$'s, that is, for some $k_1, \cdots, k_8$ $(\neq)$ $\langle b_{\lambda(k_1)}\rangle=\cdots=\langle b_{\lambda(k_8)}\rangle=\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$ (or $=-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$), then $(b_{\lambda(k_1)}, \cdots, b_{\lambda(k_8)})\sim(e_{\tau_1}\cdots e_{\tau_r}, \cdots, e_{\tau_1}\cdots e_{\tau_r})\sim(1, 1, \cdots, 1)$ (or $-(1, 1, \cdots, 1)$). Hence, again on transforming f to a congruent form, we can assume that each of $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$ occurs at most 7-times among $\langle b\rangle$'s. If both $\langle 1\rangle$ and $-\langle 1\rangle$ or both $\langle c_i\rangle$ and $-\langle c_i\rangle$ or both $\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ and $-\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ or both $\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ and $-\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ or both $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$ and $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$ or both $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle c_i\rangle$ and $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle c_i\rangle$ or both $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_1}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ and $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ or both $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ and $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ occur among $\langle b\rangle$'s, then f represents 0. Otherwise, 1 (or -1) occurs at least $(B+2^{3t-3}+2^{2t-2}+2^t-6)-(2^{3t-3}+2^{2t-2}+2^t-7)=B+1$ times among $\langle b\rangle$'s. Indeed, since $\langle c_i\rangle$ or $-\langle c_i\rangle$, $\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ or $-\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$, $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle c_i\rangle$ or $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle c_i\rangle$ and $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ or $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ are occurs at most once among $\langle b_\lambda\rangle$'s and the total number of $\langle c_i\rangle$, $\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$, $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle c_i\rangle$, $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$ is $(2^t-1)+(2^{t-1}-1)(2^t-1)+(2^{t-2}-1)(2^t-1)+(2^{t-2}-1)(2^{t-1}-1)(2^t-1)=(2^t-1)2^{2t-3}$, there are at most $(2^t-1)2^{2t-3}$ among $\langle b_\lambda\rangle$'s where are one of $\pm\langle c_i\rangle$, $\pm\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle c_i\rangle$, $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle\langle c_i\rangle$. Similarly, since $\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ or $-\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ and $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ or $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ occur at most 3 times among $\langle b_\lambda\rangle$'s and the total number of $\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ and $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ is $(2^{t-1}-1)+(2^{t-2}-1)(2^{t-1}-1)=(2^{t-1}-1)2^{t-2}$, there are at most $3(2^{t-1}-1)2^{t-2}$ among $\langle b_\lambda\rangle$'s which are one of $\pm\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ and $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle\langle d_{\sigma_1}\rangle\cdots\langle d_{\sigma_s}\rangle$ and since $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$ or $-\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$ occurs at most 7-times in $\langle b_\lambda\rangle$'s and the total number of $\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$ is $2^{t-2}-1$, there are at most $7(2^{t-2}-1)$ among $\langle b_\lambda\rangle$'s which are one of $\pm\langle e_{\tau_1}\rangle\cdots\langle e_{\tau_r}\rangle$. Hence, at least $(B+2^{3t-3}+2^{2t-2}+2^t-6)-\{(2^t-1)2^{2t-3}+3(2^{t-1}-1)2^{t-2}+7(2^{t-2}-1)\}=B+1$ among $\langle b\rangle$'s are 1 or -1. By definition of B, f represents 0.

(4) is obtained simpler that (5) by using H_t instead of H.

From our proposition we deduce easily the following

THEOREM.

(1) *If* $B \leqq 4$, *then* $A \geqq C$.

(2) *If* $B > 4$, *then* $A > C$.

(3) *If* $2^4 > B \geqq 2^3$, *then* $\frac{23}{32} A > C$.

(4) *If* $2^{t+1} > B \geqq 2^t$, $t > 3$, *then*

$$\left(\frac{1}{2} + \frac{2^{2t-2}+2^{t+1}+2^t-14}{2^{3t-2}}\right) A > C.$$

PROOF. (1), (2) are obtained easily from (1), (2), (3) and (4) (or (5)) of propesition 4. Also, (3) and (4) is obtained easily from (4) and (5) respectively, since B is at most $2^{t+1}-8$.

Mathematical Institute, Nagoya University.