A. 補遺

$x=(x_i)\in\mathbb{Z}^n$ に対して次のように定義する．

$$f(x)=\#\{i\mid x_i\equiv 1 \pmod 2\},$$
$$g(x)=\#\{i\mid x_i\equiv -1 \pmod 4\}.$$

以下 $x,y\in\mathbb{Z}^n$ に対して，特に断らない限り (x,y) は内積を表し，また $x\equiv y \pmod m$ はすべての i に対して $x_i\equiv y_i \pmod m$ であることを意味する．

補題 A.1. $x,y\in\mathbb{Z}^n$ に対して $x\equiv y \pmod 2$ とする．このとき

$$(x,y)\equiv\begin{cases} f(x) \pmod 4 & g(x)\equiv g(y) \pmod 2 \text{ のとき,}\\ f(x)+2 \pmod 4 & g(x)\not\equiv g(y) \pmod 2 \text{ のとき.}\end{cases} \tag{A.1}$$

特に，$(x,x)\equiv f(x) \pmod 4$ が成り立つ．

証明. $g(y)$ に関する帰納法により示す．$g(y)=0$ のとき，仮定より y_i が偶数ならば x_i も偶数であるから，

$$(x,y)\equiv[f(x)-g(x)]-g(x)=f(x)-2g(x) \pmod 4$$

となり (A.1) が成り立つ．一方 $g(y)>0$ のとき，$g(y')<g(y)$ となる $y'\in\mathbb{Z}^n$ に対して (A.1) が成り立つと仮定する．このとき y' を y のある $y_i\equiv -1 \pmod 4$ を $-y_i$ で置き換えたものとすると，$x\equiv y' \pmod 2$, $g(y')=g(y)-1$ であり，

$$(x,y)=(x,y')+2x_iy_i\equiv(x,y')+2 \pmod 4$$

であるから，(A.1) が成り立つ．これから主張が従う． □

ここで $\alpha=1+i+j+k\in Q\subset M_4(\mathbb{Z})$ とし，

$$A={}^t(a_1,\dots,a_5)=\begin{pmatrix}\alpha & 0\\ 0 & 2\end{pmatrix}\in M_5(\mathbb{Z})$$

とすると，${}^tAA=4E_5$ であり，$i=1,\dots,4$ に対して

$$a_i\equiv u':=\begin{pmatrix}u_4\\ 0\end{pmatrix} \pmod 2,\quad g(a_i)\equiv 0 \pmod 2$$

であることに注意する．

命題 A.2. $6\notin S$.

証明. $6\in S$ と仮定すると，(1) を満たす平方数 $s=r^2$ および $X\in M_{5,6}(\mathbb{Z})$ が存在する．ここで 2^e を r を割り切る 2 の最高巾とし，e が最小となる s および $X=(x_1,\dots,x_6)$ を取る．このとき

$$(x_i,x_j)=\begin{cases}5\cdot 2^{2e} \pmod{2^{2e+3}} & i=j \text{ のとき,}\\ -2^{2e} \pmod{2^{2e+3}} & i\neq j \text{ のとき}\end{cases}$$

となることに注意する．また $\Lambda_k=\{j\mid f(x_j)=k\}$ $(k=0,\dots,5)$ とする．

(1) $e=0$ のとき，任意の j に対して $f(x_j)\equiv(x_j,x_j)\equiv 5 \pmod 4$ であるから，

$$f(x_j)=1 \text{ または } 5.$$

(a) $\#\Lambda_5 > 2$ と仮定すると，$g(x_i) \equiv g(x_j) \pmod 2$ となる $i \neq j \in \Lambda_5$ が存在する．このとき $x_i \equiv x_j \pmod 2$ であるから，

$$-1 \equiv (x_i, x_j) \equiv f(x_j) = 5 \pmod 4$$

となり矛盾．したがって，$\#\Lambda_5 \leq 2$.

(b) $\#\Lambda_1 > 2$ と仮定すると，$g(x_i) \equiv g(x_j) \pmod 2$ となる $i \neq j \in \Lambda_1$ が存在する．このとき $(x_i, x_j) \equiv 1 \pmod 2$ より $x_i \equiv x_j \pmod 2$ であるから，

$$-1 \equiv (x_i, x_j) \equiv f(x_j) = 1 \pmod 4$$

となり矛盾．したがって，$\#\Lambda_1 \leq 2$.

このとき $6 = \#\Lambda_1 + \#\Lambda_5 \leq 4$ となり矛盾．

(2) $e = 1$ のとき，任意の j に対して $f(x_j) \equiv (x_j, x_j) \equiv 0 \pmod 4$ であるから，

$$f(x_j) = 0 \text{ または } 4.$$

ここで $\Lambda_4 = \emptyset$ と仮定すると，$s' = (r/2)^2 \in \mathbb{Z}$ および $X' = \frac{1}{2}X \in M_{5,6}(\mathbb{Z})$ は (1) を満たすから，e の最小性に反する．したがって $\Lambda_4 \neq \emptyset$ であるから，必要ならば添字を取り替えて $f(x_1) = 4$ とする．さらに必要ならば基底の順序および向きを取り替えて，$x_1 \equiv u' \pmod 2$, $g(x_1) = 0$ とする．

(a) $f(x_j) = 4$ のとき，$(x_1, x_j) \equiv 0 \pmod 2$ より，$x_j \equiv x_1 \equiv u' \pmod 2$. このとき $(x_1, x_j) \equiv 0 \equiv f(x_1) \pmod 4$ より，$g(x_j) \equiv g(x_1) = 0 \pmod 2$. したがって，$Ax_j \equiv 0 \pmod 4$.

(b) $f(x_j) = 0$ のとき，$y = \frac{1}{2}x_j \in \mathbb{Z}^5$ とおくと，$f(y) \equiv (y, y) \equiv 5 \pmod 4$ であるから，

$$f(y) = 1 \text{ または } 5.$$

(i) $f(y) = 5$ のとき，$x_j \equiv 2u_5 \pmod 4$ であるから，$Ax_j \equiv 0 \pmod 4$.

(ii) $f(y) = 1$ のとき，$(x_1, y) \equiv 0 \pmod 2$ より，$y - x_1 \equiv u_5 \pmod 2$, すなわち $x_j \equiv 2(x_1 + u_5) \pmod 4$. したがって，$Ax_j \equiv 0 \pmod 4$.

このとき，$s' = (r/2)^2 \in \mathbb{Z}$ および $X' = \frac{1}{4}AX \in M_{5,6}(\mathbb{Z})$ は (1) を満たすから，e の最小性に反する．

(3) $e \geq 2$ のとき，任意の j に対して $f(x_j) \equiv (x_j, x_j) \equiv 0 \pmod 4$ であるから，

$$f(x_j) = 0 \text{ または } 4.$$

ここで上と同様に $f(x_1) = 4$ とし，$x_1 \equiv u' \pmod 2$, $g(x_1) = 0$ とする．

(a) $f(x_j) = 4$ のとき，上と同様に $Ax_j \equiv 0 \pmod 4$.

(b) $f(x_j) = 0$ のとき，$y = \frac{1}{2}x_j \in \mathbb{Z}^5$ とおくと，$f(y) \equiv (y, y) \equiv 0 \pmod 4$ であるから，

$$f(y) = 0 \text{ または } 4.$$

(i) $f(y) = 0$ のとき，$x_j \equiv 0 \pmod 4$ であるから，$Ax_j \equiv 0 \pmod 4$.

(ii) $f(y) = 4$ のとき，$(x_1, y) \equiv 0 \pmod 2$ より，$y \equiv x_1 \pmod 2$，すなわち $x_j \equiv 2x_1 \pmod 4$. したがって，$Ax_j \equiv 0 \pmod 4$.

このとき，上と同様の矛盾が導かれる．

以上より，$6 \notin S$ を得る． □