勾股矩阵的表示及性质

宋海洲

（华侨大学数学系，泉州 362021）

摘要：

关键词：勾股数；本原勾股数；群；有限生成

若整数a,b,c满足$a^2+b^2=c^2$，称$\{a,b,c\}$为一组（广义）勾股数组，如果勾股数组写成向量形式(a,b,c)，则称该向量为一个勾股向量。

1970年，Hall[1]构造了如下三个有趣的矩阵，得到了如下的定理1：

定理1：设$F_1=\begin{pmatrix}1&2&2\\2&1&2\\2&2&3\end{pmatrix}$，$F_2=\begin{pmatrix}-1&-2&-2\\2&1&2\\2&2&3\end{pmatrix}$，$F_3=\begin{pmatrix}1&2&2\\-2&-1&-2\\2&2&3\end{pmatrix}$，

(a,b,c)是任意一勾股向量，即$a^2+b^2=c^2$，则$(a,b,c)F_1$，$(a,b,c)F_2$，$(a,b,c)F_3$仍然为勾股向量。

一般地，一个3阶整数方阵A如果满足：（1）如果$\alpha=(a,b,c)$是任意的一个勾股向量，那么$\beta=(a,b,c)A$仍然是一个勾股向量；（2）$|A|^2=1$。则称方阵A为一个勾股矩阵。

记T是所有的勾股矩阵构成的集合，即$T=\{F|F\in Z^{3\times3},F\text{是勾股数矩阵}\}$。容易验证定理1的三个勾股矩阵$F_1$、$F_2$和$F_3$的行列式都等于1，也就是说，$F_1$、$F_2$和$F_3$都是勾股矩阵，即$F_1\in T$，$F_2\in T$，$F_3\in T$。

牛普选在文[2]中给出了一个3阶整数方阵$A\in T$的充要条件，有如下的定理2：

定理2：设$B=\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}$，那么3阶整数方阵$A\in T$的充要条件是$ABA'=B$。

本文给出了所有的勾股矩阵构成的集合T的表示。

1 一些准备工作：

定义1：若a,b,c满足$a^2+b^2=c^2$，且a,b,c互素，我们称$\{a,b,c\}$为一组本原勾股数组，对应的向量为一个本原勾股向量。

显然我们有如下的引理：

引理1：如果$\alpha=(a,b,c)$是任意的一个本原勾股向量，那么a,b之中必有一个是奇数，一个是偶数，而c必是奇数。

引理2：一个3阶整数方阵$A\in T$的充要条件是A满足：（1）如果$\alpha=(a,b,c)$是任意的一个本原勾股向量，那么$\beta=(a,b,c)A$仍然是一个本原勾股向量；（2）$|A|^2=1$。

记G是所有满足下列两个条件的3阶整数方阵A的集合：（1）$A\in T$；（2）如果任意一个b是偶数的本原勾股向量$\alpha=(a,b,c)$，那么$(a',b',c')=(a,b,c)A$仍然是一个本原勾股向量，而且b'是偶数。则有$G\subset T$。

2 G的表示：

引理3：T关于矩阵乘法构成一个群；

定理 3：$A \in T$ 的充要条件是 $A' \in T$ 。

由定理 2 容易推得定理 4 成立。

定理 4：设 $A=\left(a_{ij}\right) \in Z^{3\times 3}$，则 $A \in T$ 的充要条件是 a_{ij} 满足下面的方程组的整数解：

$$\begin{cases} a^2_{11}+a^2_{21}-a^2_{31}=1 & (1) \\ a^2_{12}+a^2_{22}-a^2_{32}=1 & (2) \\ -a^2_{13}-a^2_{23}+a^2_{33}=1 & (3) \\ a_{11}a_{12}+a_{21}a_{22}=a_{31}a_{32} & (4) \\ a_{11}a_{13}+a_{21}a_{23}=a_{31}a_{33} & (5) \\ a_{12}a_{13}+a_{22}a_{23}=a_{32}a_{33} & (6) \end{cases}$$

定理 5：设 $A=\left(a_{ij}\right) \in Z^{3\times 3}$，且 $A \in G$，那么 $\left|a_{33}\right|=\max\limits_{i,j}\left|a_{ij}\right|$；

证明：由于 $G \subset T$，而 $A \in G$，所以 $A \in T$。由定理 4 知，上面的等式（1）~（6）式成立。

由等式（3）可得 $\left|a_{33}\right| \geq \left|a_{13}\right|$，$\left|a_{33}\right| \geq \left|a_{23}\right|$，$\left|a_{33}\right| \geq 1$；　　（7）

又 $A \in T$ 可得 $A' \in T$，

所以 $\left|a_{33}\right| \geq \left|a_{31}\right|$，$\left|a_{33}\right| \geq \left|a_{32}\right|$；　　（8）

当 a_{11}、a_{12}、a_{21}、a_{22} 都不等于 0 时：

则由（1）可得 $\left|a_{31}\right| \geq \left|a_{11}\right|$，$\left|a_{31}\right| \geq \left|a_{21}\right|$；　　（9）

由（2）可得 $\left|a_{32}\right| \geq \left|a_{12}\right|$，$\left|a_{32}\right| \geq \left|a_{22}\right|$；　　（10）

由（7）、（8）、（9）和（10）可得 $\left|a_{33}\right|=\max\limits_{i,j}\left|a_{ij}\right|$ 成立。

当 a_{11}、a_{21} 中至少一个等于 0 而 a_{12}、a_{22} 都不等于 0 时：a_{12}、a_{22} 都不等于 0，由（2）可以推出不等式（10）成立；a_{11}、a_{21} 中至少一个等于 0，可以推出 $\max\limits_{i}\left|a_{i1}\right|=1$，而 $\left|a_{33}\right| \geq 1$，此时必有 $\left|a_{33}\right| \geq \max\limits_{i}\left|a_{i1}\right|$；由不等式（7）、（8）、（10）和 $\left|a_{33}\right| \geq \max\limits_{i}\left|a_{i1}\right|$ 可得 $\left|a_{33}\right|=\max\limits_{i,j}\left|a_{ij}\right|$ 成立。

当 a_{12}、a_{22} 中至少一个等于 0 而 a_{11}、a_{21} 都不等于 0 时：a_{11}、a_{21} 都不等于 0，由（1）可以推出不等式（9）成立；a_{12}、a_{22} 中至少一个等于 0，可以推出 $\max\limits_{i}\left|a_{i2}\right|=1$，而 $\left|a_{33}\right| \geq 1$，此时必有 $\left|a_{33}\right| \geq \max\limits_{i}\left|a_{i2}\right|$；由不等式（7）、（8）、（9）和 $\left|a_{33}\right| \geq \max\limits_{i}\left|a_{i2}\right|$ 可得 $\left|a_{33}\right|=\max\limits_{i,j}\left|a_{ij}\right|$ 成立。

当 a_{12}、a_{22} 中至少一个等于 0 并且 a_{11}、a_{21} 中至少一个等于 0 时：a_{11}、a_{21} 中至少一个等于 0，可以推出 $\max\limits_{i}\left|a_{i1}\right|=1$，而 $\left|a_{33}\right| \geq 1$，此时必有 $\left|a_{33}\right| \geq \max\limits_{i}\left|a_{i1}\right|$；$a_{12}$、$a_{22}$ 中至少一个等于 0，可以推出 $\max\limits_{i}\left|a_{i2}\right|=1$，而 $\left|a_{33}\right| \geq 1$，此时必有 $\left|a_{33}\right| \geq \max\limits_{i}\left|a_{i2}\right|$；由不等式（7）、$\left|a_{33}\right| \geq \max\limits_{i}\left|a_{i1}\right|$ 和 $\left|a_{33}\right| \geq \max\limits_{i}\left|a_{i2}\right|$ 可得 $\left|a_{33}\right|=\max\limits_{i,j}\left|a_{ij}\right|$ 成立。

定理 6：设 $A=\left(a_{ij}\right) \in Z^{3\times 3}$，且 $A \in G$，那么 $a_{ii} \equiv 1 \pmod 2$（$i=1,2,3$），$a_{ij} \equiv 0 \pmod 2$（$i \neq j$，$i=1,2,3$，$j=1,2,3$）。

证明：由$A\in G$知，上面的等式（1）~（3）式成立。

由$-a^2_{13}-a^2_{23}+a^2_{33}=1$可得，$a_{33}\equiv 1$（mod 2），$a_{13}\equiv 0$（mod 2），$a_{23}\equiv 0$（mod 2）。又$A\in T$可得$A'\in T$，因此$a_{31}\equiv 0$（mod 2），$a_{32}\equiv 0$（mod 2）。设$\alpha=(a,b,c)$是任意一个$b$是偶数的本原勾股向量，由引理 1 可得$a,c$是奇数；由于$A\in G$，所以$(a',b',c')=(a,b,c)$ A仍然是一个本原勾股向量，而且b'是偶数，由引理 1 可得a',c'是奇数；由b是偶数，$a_{31}\equiv 0$（mod 2）和a是奇数，以及$a'=aa_{11}+ba_{21}+ca_{31}$可得$a_{11}\equiv 1$（mod 2）。由$a_{11}\equiv 1$（mod 2）、$a_{31}\equiv 0$（mod 2）及等式（1）可得：$a_{21}\equiv 0$（mod 2）。由$a$是奇数，$b$是偶数，$a_{32}\equiv 0$（mod 2），以及$b'=aa_{12}+ba_{22}+ca_{32}$可得：$a_{12}\equiv 0$（mod 2）。由$a_{12}\equiv 0$（mod 2）、$a_{32}\equiv 0$（mod 2）及等式（2）可得：$a_{22}\equiv 1$（mod 2）。综上，有$a_{ii}\equiv 1$（mod 2）$(i=1,2,3)$，$a_{ij}\equiv 0$（mod 2）$(i\neq j,\ i=1,2,3,\ j=1,2,3)$成立。

推论 1：（1）G关于矩阵乘法构成一个群；

（2）G是T的一个子群。

证明：（1）任意A、$B\in G$，显然有A、$B\in T$，所以$A*B\in T$；设$\alpha=(a,b,c)$是任意一个b是偶数的本原勾股向量，由于$A\in G$，所以(a,b,c) A也是一个第 2 个元素是偶数的本原勾股向量，又$B\in G$，所以(a,b,c) A B也是一个第 2 个元素是偶数的本原勾股向量，因此有$A*B\in G$，即G对于矩阵乘法运算封闭。显然矩阵乘法运算满足结合律。且 3 阶单位阵就是G中的单位元。

下面证明G对于矩阵逆封闭。

任意$A\in G$，$A=\left(a_{ij}\right)\in Z^{3\times 3}$，由定理 6 有：$a_{ii}\equiv 1$（mod 2）$(i=1,2,3)$，$a_{ij}\equiv 0$（mod 2）$(i\neq j,\ i=1,2,3,\ j=1,2,3)$成立。设$\alpha=(a,b,c)$是任意一个$b$是偶数的本原勾股向量，设$(a',b',c')=(a,b,c)$ A^{-1}，由于$A\in T$，T关于矩阵乘法构成一个群，所以$A^{-1}\in T$，从而(a',b',c')是本原勾股向量。由引理 1 可得a',b'中一个是奇数，一个是偶数。由于(a,b,c)是任意一个b是偶数的本原勾股向量，根据引理 1 可得a是奇数。由$(a',b',c')=(a,b,c)$ A^{-1}得$(a,b,c)=(a',b',c')$ A，可以推出$a=a'a_{11}+b'a_{21}+c'a_{31}$，由于$a$是奇数，$a_{21},a_{31}$是偶数，故$a'$是奇数，从而$b'$必是偶数，即$(a',b',c')=(a,b,c)$ A^{-1}是第 2 个元素是偶数的本原勾股向量，因此$A^{-1}\in G$。

综上G关于矩阵乘法构成一个群；

（2）由$G\subset T$，G关于矩阵乘法构成一个群，可以推出G是T的一个子群。

2　G_i的表示

定理 7：记$G_1=\left\{A\middle|\ A=\left(a_{ij}\right)\in Z^{3\times 3}\right.$，且$A\in G$，且$\max\limits_{i,j}\left|a_{ij}\right|=1\ \}$，则：$G_1=\{\ D_1=diag[1,1,1]$，$D_2=diag[-1,1,1]$，$D_3=diag[1,-1,1]$，$D_4=diag[1,1,-1]$，$D_5=diag[-1,-1,1]$，$D_6=diag[-1,1,-1]$，$D_7=diag[1,-1,-1]$，$D_8=diag[-1,-1,-1]\}$。

证明：由定理 5 和定理 6 知，若$A\in G$，且$\max\limits_{i,j}\left|a_{ij}\right|=1$，则$A$只能是下列矩阵之一：$D_1=diag[1,1,1]$，$D_2=diag[-1,1,1]$，$D_3=diag[1,-1,1]$，

$D_4 = diag[1,1,-1]$， $D_5 = diag[-1,-1,1]$， $D_6 = diag[-1,1,-1]$， $D_7 = diag[1,-1,-1]$，$D_8 =$ $diag[-1,-1,-1]$。又容易验证$D_i(i=1,..,8) \in G$，所以定理 7 成立。

定理 8：设 $A=\left(a_{ij}\right) \in Z^{3\times3}$，且 $A \in G$，且 $\max\limits_{i,j}\left|a_{ij}\right|$=3，则：$\left|a_{33}\right|$=3，$\left|a_{31}\right|=\left|a_{32}\right|=\left|a_{13}\right|=\left|a_{23}\right|=\left|a_{12}\right|=\left|a_{21}\right|$=2，$\left|a_{11}\right|=\left|a_{22}\right|$=1。

证明：由定理 6 知，若 $A \in G$，且 $A \in G$，且 $\max\limits_{i,j}\left|a_{ij}\right|$=3，则：$\left|a_{33}\right|=\max\limits_{i,j}\left|a_{ij}\right|$=3。由 $A \in G$ 知，上面的等式（1）~（3）式成立。由等式（3）知 $\left|a_{13}\right|=\left|a_{23}\right|$=2 成立。又 $A \in T$ 可得 $A' \in T$，从而 $\left|a_{31}\right|=\left|a_{32}\right|$=2 成立。由定理 5 可得 $\left|a_{11}\right|$ 和 $\left|a_{22}\right|$ 只能是 1 或 3；又 $\left|a_{13}\right|=\left|a_{23}\right|=\left|a_{31}\right|=\left|a_{32}\right|$=2，及由等式（1）和（2），我们可推得 $\left|a_{11}\right|=\left|a_{22}\right|$=1。此时必有 $\left|a_{12}\right|=\left|a_{21}\right|$=2。综上，定理 8 成立。

定理 9：记 $G_3=\left\{A \middle|\ A=\left(a_{ij}\right) \in Z^{3\times3}\right.$，且 $A \in G$，且 $\left.\max\limits_{i,j}\left|a_{ij}\right|=3\ \right\}$，

$F_1 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$，$D_i\ (i=1,..,8)$ 如定理 7 所示。则：

$G_3 = \left\{A \middle| A=D_iF_1D_j, D_i \in G_1, D_j \in G_1\right\}$。

证明：任意的 $D_i\ (i=1,..,8)$ 和 $D_j\ (j=1,..,8)$，由定理 7 得 D_i 和 D_j 都 $\in G$；容易验证 $F_1 \in G$；由推论 1（1）可推得 $D_iF_1D_j \in G$。又容易验证矩阵 $D_iF_1D_j$ 元素的绝对值最大等于 3。所以对任意的 $D_i\ (i=1,..,8)$ 和 $D_j\ (j=1,..,8)$，$D_iF_1D_j \in G_3$。

另外一方面，如果 $A \in G_3$，则：$\left|a_{33}\right|$=3，$\left|a_{11}\right|=\left|a_{22}\right|$=1，$\left|a_{31}\right|=\left|a_{32}\right|=\left|a_{13}\right|=\left|a_{23}\right|=\left|a_{12}\right|=\left|a_{21}\right|$=2。

对于 A，一定存在 D_i 和 D_j，使得矩阵 D_iAD_j（记矩阵 D_iAD_j 为 C，并设 $C=\left(c_{ij}\right)$）的第 1、2 列 6 个元素中最多有两个元素小于 0，而且这些小于 0 的元素不在同一行。由于 D_i、D_j 和 F_1 都属于 G，所以 $C = D_iAD_j \in G$，从而 $C \in G_3$，故 $\left|c_{33}\right|$=3，$\left|c_{31}\right|=\left|c_{32}\right|=\left|c_{13}\right|=\left|c_{23}\right|=\left|c_{12}\right|=\left|c_{21}\right|$=2，$\left|c_{11}\right|=\left|c_{22}\right|$=1。由 $C \in G$ 及定理 4 得：$c_{11}c_{12}+c_{21}c_{22}=c_{31}c_{32}$，又 C 的第 1、2 列 6 个元素中最多有两个元素小于 0，而且这些小于 0 元素不在同一行，可得 $c_{ij}>0\ (i=1,2,3,\ j=1,2)$。

对于 C，一定存在 D_k，使得矩阵 $C\ D_k$（记矩阵 $C\ D_k$ 为 H，并设 $H=\left(h_{ij}\right)$）的第 1、2 列向量与 C 的第 1、2 列向量相同，并且 H 的第 3 列向量最多有 1 个元素小于 0。同样可得 $\left|h_{33}\right|$=3，$\left|h_{31}\right|=\left|h_{32}\right|=\left|h_{13}\right|=\left|h_{23}\right|=\left|h_{12}\right|=\left|h_{21}\right|$=2，$\left|h_{11}\right|=\left|h_{22}\right|$=1，以及 $h_{11}h_{13}+h_{21}h_{23}=h_{31}h_{33}$。注意到 $h_{i1}=c_{i1}>0\ (i=1,2,3)$，所以 $h_{i3}>0\ (i=1,2,3)$。从而 $H=F_1$。

所以存在 D_i、D_j 和 D_k 使得 $D_iAD_j\ D_k=F_1$。令 $P_1=D_i^{-1}$，$P_2=(D_j\ D_k)^{-1}$，容易验证 P_1 和 P_2 都属于 G_1，而 $A=P_1\ F_1\ P_2$。

综上有：$G_3 = \{A \mid A = D_i F_1 D_j, D_i \in G_1, D_j \in G_1\}$。

直接验证就可以得到如下的定理 10。

定理 10：设 $F_1 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_2 = \begin{pmatrix} -1 & -2 & -2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_3 = \begin{pmatrix} 1 & 2 & 2 \\ -2 & -1 & -2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_4 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ -2 & -2 & -3 \end{pmatrix}$，$D_i (i = 1,..,8)$ 如定理 7 所示，则 $D_1 = F_1 * F_1^{-1}$，$D_2 = F_1 * F_2^{-1}$，$D_3 = F_1 * F_3^{-1}$，$D_4 = F_1 * F_4^{-1}$，$D_5 = F_2 * F_3^{-1}$，$D_6 = F_2 * F_4^{-1}$，$D_7 = F_3 * F_4^{-1}$，$D_8 = F_2 * F_3^{-1} * F_1 * F_4^{-1}$。

由定理 9 及定理 10，我们可以得到：

定理 11：（1）$G_3 \subset L(F_1, F_2, F_3, F_4)$；

（2）$G_1 \subset L(F_1, F_2, F_3, F_4)$。

3 G 的表示

定理 12：设 $F_1 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_2 = \begin{pmatrix} -1 & -2 & -2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_3 = \begin{pmatrix} 1 & 2 & 2 \\ -2 & -1 & -2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_4 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ -2 & -2 & -3 \end{pmatrix}$，任意 $A = (a_{ij}) \in G$，设 A 的元素的绝对值最大值为 y，并且 $y > 3$，记 $H_i = A\ F_i$（$i = 1,...,4$），则一定存在一个 H_i，它的元素的绝对值最大值小于 y。

证明：由于 F_i（$i = 1,...,4$）$\in G$，$A \in G$，所以 $H_i = A\ F_i \in G$（$i = 1,...,4$）。由定理 5 知 A 的元素的绝对值最大值为 $y = |a_{33}|$，H_1 的元素的绝对值最大值为 $|2a_{31} + 2a_{32} + 3a_{33}|$，$H_2$ 的元素的绝对值最大值为 $|-2a_{31} + 2a_{32} + 3a_{33}|$，$H_3$ 的元素的绝对值最大值为 $|2a_{31} - 2a_{32} + 3a_{33}|$，$H_4$ 的元素的绝对值最大值为 $|2a_{31} + 2a_{32} - 3a_{33}|$。

我们先考虑 $a_{31} \geq 0$，$a_{32} \geq 0$，$a_{33} > 0$ 情形。

由 $A \in G$，可得 $A' \in G$，所以 $-a^2_{31} - a^2_{32} + a^2_{33} = 1$ 成立；由于 $|a_{33}| > 3$，所以必有 $a_{31} \neq 0$，$a_{32} \neq 0$，从而有 $a_{31} > 0$，$a_{32} > 0$。因此有 $a_{33} > a_{31}$，$a_{33} > a_{32}$。所以 $2a_{31} + 2a_{32} - 3a_{33} < a_{33}$ 成立。

由 $-a^2_{31} - a^2_{32} + a^2_{33} = 1$ 可得 $a_{33} - a_{31} = (1 + a_{32}^2) / (a_{33} + a_{31})$，而 $(1 + a_{32}^2) / (a_{33} + a_{31}) < (a_{32}a_{31} + a_{32}a_{33}) / (a_{33} + a_{31}) = a_{32}$，从而有 $a_{33} - a_{31} < a_{32}$，即 $a_{33} < a_{32} + a_{31}$，故 $-a_{33} < 2a_{31} + 2a_{32} - 3a_{33}$ 成立。

由 $2a_{31} + 2a_{32} - 3a_{33} < a_{33}$ 和 $-a_{33} < 2a_{31} + 2a_{32} - 3a_{33}$ 可得 $|2a_{31} + 2a_{32} - 3a_{33}| < y$ 成立。即 H_4 的元素的绝对值最大值小于 y，此时定理 12 成立。

同理可以证明在 $a_{31} \geq 0$，$a_{32} \leq 0$，$a_{33} > 0$ 等情形下，定理 12 仍然成立。

定理 13：设 $F_1=\begin{pmatrix}1&2&2\\2&1&2\\2&2&3\end{pmatrix}$，$F_2=\begin{pmatrix}-1&-2&-2\\2&1&2\\2&2&3\end{pmatrix}$，$F_3=\begin{pmatrix}1&2&2\\-2&-1&-2\\2&2&3\end{pmatrix}$，$F_4=\begin{pmatrix}1&2&2\\2&1&2\\-2&-2&-3\end{pmatrix}$，则 $G=L\left(F_1,F_2,F_3,F_4\right)$。也就是说 G 是有限生成群。

证明：显然 $L\left(F_1,F_2,F_3,F_4\right)\subset G$。

设任意 $A=\left(a_{ij}\right)\in G$，若 $\left|a_{33}\right|\le 3$，则由定理 6 知，要么 $\left|a_{33}\right|$=1，要么 $\left|a_{33}\right|$=3。当 $\left|a_{33}\right|$=1 时，有 $A\in G_1$，由定理 11 有 $A\in L\left(F_1,F_2,F_3,F_4\right)$。当 $\left|a_{33}\right|$=3 时，有 $A\in G_3$，由定理 11 有 $A\in L\left(F_1,F_2,F_3,F_4\right)$。

若 $\left|a_{33}\right|>3$，则由定理 12 可知，存在 P_1，P_2，...，P_k（其中 $P_i\in\left\{F_1,F_2,F_3,F_4\right\}$），使得 $A*P_1*P_2*\cdots*P_k$ 的元素的绝对值最大值 ≤ 3。而 $A*P_1*P_2*\cdots*P_k\in G$，所以 $A*P_1*P_2*\cdots*P_k\in L\left(F_1,F_2,F_3,F_4\right)$，从而 $A\in L\left(F_1,F_2,F_3,F_4\right)$。

于是有 $G\subset L\left(F_1,F_2,F_3,F_4\right)$。

综上有 $G=L\left(F_1,F_2,F_3,F_4\right)$。

推论 2： 记 $D_1=diag[1,1,1]$，$D_2=diag[-1,1,1]$，$D_3=diag[1,-1,1]$，$D_4=diag[1,1,-1]$，$D_6=diag[-1,-1,1]$，$D_6=diag[-1,-1,1]$，$D_7=diag[-1,-1,1]$，$D_8=diag[-1,-1,-1]$，$F_1=\begin{pmatrix}1&2&2\\2&1&2\\2&2&3\end{pmatrix}$，$F_2=\begin{pmatrix}-1&-2&-2\\2&1&2\\2&2&3\end{pmatrix}$，$F_3=\begin{pmatrix}1&2&2\\-2&-1&-2\\2&2&3\end{pmatrix}$，$F_4=\begin{pmatrix}1&2&2\\2&1&2\\-2&-2&-3\end{pmatrix}$。则

（1）$G=L\left(F_1,D_2,D_3,D_4\right)$；

（2）$G=L\left(F_1,D_2,D_4,D_5\right)$；

（3）$G=L\left(F_i,D_2,D_3,D_4\right)$。

证明：只证明（1）成立，其它可以类似证明。

显然 $L\left(F_1,D_2,D_3,D_4\right)\subset G$。

任意 $A=\left(a_{ij}\right)\in G$，由定理 13 有 $A\in L\left(F_1,F_2,F_3,F_4\right)$，又根据定理 10 有 $D_2=F_1*F_2^{-1}$，$D_3=F_1*F_3^{-1}$，$D_4=F_1*F_4^{-1}$，从而有 $F_2=D_2^{-1}*F_1$，$F_3=D_3^{-1}*F_1$，$F_4=D_4^{-1}*F_1$。所以 $A\in L\left(F_1,D_2,D_3,D_4\right)$。

综上，$G=L\left(F_1,D_2,D_3,D_4\right)$成立。

4 T 的表示

定义 2：设 H 是有限生成群，$X_1,X_2,...,X_n$ 满足：$H=L$（$X_1,X_2,...,X_n$），我们称 $X_1,X_2,...,X_n$ 为 H 的一个生成元组。若 $X_1,X_2,...,X_n$

是 H 的一个生成元组，并且是元素最少的一个生成元组，我们称 $X_1, X_2, ..., X_n$ 为 H 的一个极小生成元组，n 称为 H 基数，并记 $n = d(H)$。

定理 14：记 $D_1 = diag[1,1,1]$，$D_2 = diag[-1,1,1]$，$D_3 = diag[1,-1,1]$，$D_4 = diag[1,1,-1]$，$D_6 = diag[-1,-1,1]$，$D_6 = diag[-1,1,-1]$，$D_7 = diag[1,-1,-1]$，$D_8 = diag[-1,-1,-1]$，$F_1 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_2 = \begin{pmatrix} -1 & -2 & -2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_3 = \begin{pmatrix} 1 & 2 & 2 \\ -2 & -1 & -2 \\ 2 & 2 & 3 \end{pmatrix}$，$F_4 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ -2 & -2 & -3 \end{pmatrix}$，$D_9 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$。则 $T = L(F_1, D_2, D_4, D_9)$。也就是说 T 是有限生成群，且 $d(T) \le 4$。

证明：容易验证 $D_9 \in T$，所以 $L(F_1, D_2, D_4, D_9) \subset T$。

由于 $D_3 = D_9\ D_2\ D_9$，所以 $G = L(F_1, D_2, D_3, D_4) \subset L(F_1, D_2, D_4, D_9)$。

设任意 $A = (a_{ij}) \in T$，设 $(x, y, z) = (3,4,5)\ A$。则 x, y 中一个是奇数，一个是偶数。

（1）x 是奇数，y 是偶数时：

由 $(x, y, z) = (3,4,5)\ A$ 得：$y = 3a_{12} + 4a_{22} + 5a_{32}$。由于 y 是偶数，所以 a_{12}, a_{32} 要么同是奇数，要么同是偶数。

设 (a,b,c) 是任意一个 b 是偶数的本原勾股向量，记 $(a',b',c') = (a,b,c)\ A$，则 (a',b',c') 也是本原勾股向量。由于 (a,b,c) 是任意一个 b 是偶数的本原勾股向量，所以 a,c 都是奇数。由 $b' = aa_{12} + ba_{22} + ca_{32}$，$b$ 是偶数，a_{12}, a_{32} 要么同是奇数，要么同是偶数，以及 a,c 都是奇数，可得 b' 是偶数。所以 $A \in G$，从而 $A \in (F_1, D_2, D_3, D_4)$。又 $L(F_1, D_2, D_3, D_4) \subset L(F_1, D_2, D_4, D_9)$，所以 $A \in L(F_1, D_2, D_4, D_9)$。

（2）y 是奇数，x 是偶数时：

令 $(x', y', z') = (x, y, z)\ D_9 = (3,4,5)\ A\ D_9$，有 x' 是奇数，y' 是偶数。由 $A \in T$，$D_9 \in T$ 得 $A\ D_9 \in T$，因此 $A\ D_9 \in L(F_1, D_2, D_4, D_9)$，从而 $A \in L(F_1, D_2, D_4, D_9)$。

综上，有 $T \subset L(F_1, D_2, D_4, D_9)$。

因此有 $T = L(F_1, D_2, D_4, D_9)$，且 $d(T) \le 4$ 成立。

推论 3：$T = L(F_1, D_2, D_4, D_9) = L(F_1, D_3, D_4, D_9) = L(F_1, F_2, F_4, D_9)$

$= L(F_1, F_3, F_4, D_9) = L(F_2, F_3, F_4, D_9)$。

5　勾股向量 的表示

定义 3：如果正整数 a,b,c 满足：$a^2 + b^2 = c^2$，且 a,b,c 互素，并且 b 是偶数，我们称 $\{a,b,c\}$ 为一组规范本原勾股数组，对应的向量为一个规范本原勾股向量。

记$W=\left\{A\middle|A=X_1^{t_1}X_2^{t_2}\cdots X_n^{t_n},X_i\in\{F_1,F_2,F_3\},t_i\in Z,t_i\geq 0\right\}$，显然$W\subset G$。

引理 4：设(a,b,c)是任意一个规范本原勾股向量，并且$c\geq 5$，则存在惟一的$A\in W$，使得$(a,b,c)=(3,4,5)\ A$。另外，任意$A\in W$，则$(a,b,c)=(3,4,5)\ A$为规范本原勾股向量，并且$c\geq 5$。

注：引理 4 我们将在另一文进行发表。

引理 5：$(1,0,1)=(3,4,5)\ F_1^{-1}$。

定理 15：设(a,b,c)是任意一个本原勾股向量，并且$|c|\geq 5$，则存在惟一的一组矩阵A，C（$A\in W$，$C\in G_1$），使得$(a,b,c)=(3,4,5)\ A\ C$。

证明：先证明存在性：设(a,b,c)是任意一个本原勾股向量，并且$|c|\geq 5$。显然存在$C\in G_1$，使得$(a,b,c)\ C$为规范本原勾股向量，由引理 4 可得，存在$A\in W$，使得$(a,b,c)\ C=(3,4,5)\ A$。注意到$C^{-1}=C$，所以有$(a,b,c)=(3,4,5)\ A\ C$成立。

再证明惟一性：假设$A_1\in W$，$C_1\in G_1$也使得$(a,b,c)=(3,4,5)\ A_1\ C_1$成立，则有$(3,4,5)\ A\ C=(3,4,5)\ A_1\ C_1$，因此$(3,4,5)\ A=(3,4,5)\ A_1\ C_1\ C$。设$(3,4,5)\ A=(x,y,z)$，$(3,4,5)\ A_1=(x_1,y_1,z_1)$，由引理 4 知$x>0,y>0,z>0$，$x_1>0,y_1>0,z_1>0$，而$C_1\ C$为主对角线元素是 1 或-1 的对角矩阵，所以$(3,4,5)\ A=(3,4,5)\ A_1$，再由引理 4 得$A=A_1$，从而$C_1\ C=E_3$（3 阶单位阵），故$C_1=C$。惟一性得到证明。

由引理 5 和定理 15 可以得到如下的定理：

定理 16：设(a,b,c)是任意一个本原勾股向量，则存在惟一的一组矩阵A，C（$A\in W$或者$A=F_1^{-1}$，$C\in G_1$），使得$(a,b,c)=(3,4,5)\ A\ C$。

推论 4：（1）设(a,b,c)，(a',b',c')是任意两个本原勾股向量，则存在A，C，A_1，C_1（$A\in W$或者$A=F_1^{-1}$，$A_1\in W$或者$A_1=F_1^{-1}$，C，$C_1\in G_1$），使得$(a',b',c')=(a,b,c)\ C\ A^{-1}\ A_1\ C_1$。

（2）设(a,b,c)，(a',b',c')是任意两个本原勾股向量，则存在$A\in T$，使得$(a',b',c')=(a,b,c)\ A$。

（3）设(a,b,c)是任意一个本原勾股向量，(a',b',c')是任意一个勾股向量，则存在$A\in T$及$p\in Z$，使得$(a',b',c')=p\ (a,b,c)\ A$。

（4）设(a,b,c)是任意一个不为 0 的勾股向量，(a',b',c')是任意一个勾股向量，则存在$A\in T$及$p\in Z$和$q\in Z$，使得$(a',b',c')=\frac{p}{q}(a,b,c)\ A$。