Hall 矩阵的性质

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。

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。

定义 2：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。

1 规范本原勾股向量的表示

记 $H=\left\{(a,b,c)\middle|(a,b,c)\text{是规范本原向量}\right\}$。

定理 2：$H=\left\{(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})\middle|k>m>0,k,m\text{都是奇数，k与m互素}\right\}$。

证明：设 $\left|k>m>0,k,m\right.$都是奇数，k与m互素。容易验证 $(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})$ 是一个勾股向量，$km>0,\frac{k^2-m^2}{2}>0,\frac{k^2+m^2}{2}>0$ 并且 $\frac{k^2-m^2}{2}$ 是偶数。下面证明 $km,\frac{k^2-m^2}{2}$与$\frac{k^2+m^2}{2}$ 互素。假设 $km,\frac{k^2-m^2}{2}$与$\frac{k^2+m^2}{2}$ 不互素，则存在奇素数 p，使得 $p\left|km\right.$，$p\left|\frac{k^2-m^2}{2}\right.$。由于 k 和 m 互素，所以 $p\left|k\right.$ 或 $p\left|m\right.$。若 $p\left|k\right.$，由 $p\left|\frac{k^2-m^2}{2}\right.$ 可以推出 $p\left|m\right.$，因此奇素数 p 是 k 和 m 的公因子，与 k 和 m 互素矛盾。若 $p\left|m\right.$，由 $p\left|\frac{k^2-m^2}{2}\right.$ 可以推出 $p\left|k\right.$，因此奇素数 p 是 k 和 m 的公因子，与 k 和 m 互素矛盾。所以

$km,\frac{k^2-m^2}{2}$与$\frac{k^2+m^2}{2}$必互素。也就是说$(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})$是一个规范本原勾股向量。

从而$\left\{(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})\middle|k>m>0,k,m\text{都是奇数，k与m互素}\right\}\subset H$。

另外一方面，如果$\{a,b,c\}\in H$，则根据定义有a,b,c是互素的正整数，b是偶数，并且$a^2+b^2=c^2$。由引理 1 又可得a,c是奇数。由$a^2+b^2=c^2$可得$a^2=(c+b)(c-b)$，令$c-b=m^2t$，其中m和t都是正奇数，并且t无平方因子。则$c+b=k^2t$，k是某个大于m的正奇数。因此$a=kmt$，$b=\frac{k^2-m^2}{2}t$，$c=\frac{k^2+m^2}{2}t$。由a,b,c是互素的正整数，可以推出$t=1$，所以$a=km$，$b=\frac{k^2-m^2}{2}$，$c=\frac{k^2+m^2}{2}$。又a,b,c是互素，必有k和m互素。从而$\{a,b,c\}\in\left\{(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})\middle|k>m>0,k,m\text{都是奇数，k与m互素}\right\}$，即有$H\subset\left\{(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})\middle|k>m>0,k,m\text{都是奇数，k与m互素}\right\}$。

综上，有$H=\left\{(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})\middle|k>m>0,k,m\text{都是奇数，k与m互素}\right\}$。

设$Q=\left\{(k,m)'\middle|k>m>0,k,m\text{都是奇数，k与m互素}\right\}$。

作一个$H\to Q$的映射f（$(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})$）$=(k,m)'$。容易验证$f$是$H$到$Q$的一一映射。

容易验证下面定理成立。

定理 3：f（$(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})\ F_1$）$=(2k+m,k)'$；

f（$(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})\ F_2$）$=(2k-m,k)'$；

f（$(km,\frac{k^2-m^2}{2},\frac{k^2+m^2}{2})\ F_3$）$=(k+2m,m)'$；

f（$(3,4,5)$）$=(3,1)'$。

再作如下 3 个$Q\to Q$的映射：

$g_1((k,m)')=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}k\\m\end{pmatrix}$，$g_2((k,m)')=\begin{pmatrix}2&-1\\1&0\end{pmatrix}\begin{pmatrix}k\\m\end{pmatrix}$，$g_3((k,m)')=\begin{pmatrix}1&2\\0&1\end{pmatrix}\begin{pmatrix}k\\m\end{pmatrix}$。

则 g_1， g_2， g_3 有逆映射： $g_1^{-1}\begin{pmatrix}k'\\m'\end{pmatrix}=\begin{pmatrix}m'\\k'-2m'\end{pmatrix}$（$3m'>k'>2m'>0$， k' 与 m' 互素。），$g_2^{-1}\begin{pmatrix}k'\\m'\end{pmatrix}=\begin{pmatrix}m'\\-k'+2m'\end{pmatrix}$（$2m'>k'>m'>0$， k' 与 m' 互素。），$g_3^{-1}\begin{pmatrix}k'\\m'\end{pmatrix}=\begin{pmatrix}k'-2m'\\m'\end{pmatrix}$（$k'>3m'>0$， k' 与 m' 互素。）。

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

定义 3：设 $\begin{pmatrix}k_1\\m_1\end{pmatrix}$，$\begin{pmatrix}k_2\\m_2\end{pmatrix}\in Q$，如果 $k_1<k_2$，或者虽然有 $k_1=k_2$ 但 $m_1<m_2$，我们称 $\begin{pmatrix}k_1\\m_1\end{pmatrix}\prec\begin{pmatrix}k_2\\m_2\end{pmatrix}$。

定理 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 $A\in W$，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 $c\geq 5$。

证明：任意 $A\in W$，由定理 1 可得 $(a,b,c)=(3,4,5)\,A$ 为本原勾股向量。容易验证 (a,b,c) 是规范本原勾股向量，并且 $c\geq 5$。

设 (a,b,c) 是任意一个规范本原勾股向量，并且 $c\geq 5$。设 f（(a,b,c)）$=\begin{pmatrix}k'\\m'\end{pmatrix}$。若 $k'>3m'>0$，则 g_3^{-1}（$\begin{pmatrix}k'\\m'\end{pmatrix}$）$=\begin{pmatrix}k'-2m'\\m'\end{pmatrix}$，有 $\begin{pmatrix}k'-2m'\\m'\end{pmatrix}\prec\begin{pmatrix}k'\\m'\end{pmatrix}$ 成立，此时令 $(a_1,b_1,c_1)=(a,b,c)\,F_3^{-1}$，有 f（(a_1,b_1,c_1)）$\prec f$（(a,b,c)）成立；若 $k'=3m'>0$，则必有 $\begin{pmatrix}k'\\m'\end{pmatrix}=\begin{pmatrix}3\\1\end{pmatrix}$。若 $3m'>k'>2m'>0$，则 $g_1^{-1}\begin{pmatrix}k'\\m'\end{pmatrix}=\begin{pmatrix}m'\\k'-2m'\end{pmatrix}$，有 $\begin{pmatrix}m'\\k'-2m'\end{pmatrix}\prec\begin{pmatrix}k'\\m'\end{pmatrix}$ 成立，此时令 $(a_1,b_1,c_1)=(a,b,c)\,F_1^{-1}$，有 f（(a_1,b_1,c_1)）$\prec f$（(a,b,c)）成立；若 $2m'>k'>m'>0$，则 $g_2^{-1}\begin{pmatrix}k'\\m'\end{pmatrix}=\begin{pmatrix}m'\\-k'+2m'\end{pmatrix}$，有 $\begin{pmatrix}m'\\-k'+2m'\end{pmatrix}\prec\begin{pmatrix}k'\\m'\end{pmatrix}$ 成立，此时令 $(a_1,b_1,c_1)=(a,b,c)\,F_2^{-1}$，有 f（(a_1,b_1,c_1)）$\prec f$（(a,b,c)）成立。即无论 k',m' 取什么值，均存在 X_1（$X_1\in\{F_1,F_2,F_3\}$），令 $(a_1,b_1,c_1)=(a,b,c)\,X_1^{-1}$，有 f（(a_1,b_1,c_1)）$\prec f$（(a,b,c)）成立，否则必有 f（(a,b,c)）$=\begin{pmatrix}k'\\m'\end{pmatrix}=\begin{pmatrix}3\\1\end{pmatrix}$。同理存在 X_2（$X_2\in\{F_1,F_2,F_3\}$），令 $(a_2,b_2,c_2)=(a_1,b_1,c_1)\,X_2^{-1}$，有 f（(a_2,b_2,c_2)）$\prec f$（(a_1,b_1,c_1)）成立，否则必有 f（(a_1,b_1,c_1)）$=\begin{pmatrix}3\\1\end{pmatrix}$。…，因此存在 $X_1,X_2,\cdots,X_n$（$X_i\in\{F_1,F_2,F_3\}$），有 f（$(a,b,c)\;X_1^{-1}\;X_2^{-1}\cdots X_n^{-1}$）$=\begin{pmatrix}3\\1\end{pmatrix}$，即存在 $X_1,X_2,\cdots,X_n$

（ $X_i \in \{F_1, F_2, F_3\}$ ），使得 $(a,b,c)\ X_1^{-1}\ X_2^{-1} \cdots\ X_n^{-1} = (3,4,5)$。所以存在 $X_1, X_2, \cdots, X_n$（ $X_i \in \{F_1, F_2, F_3\}$ ），使得 $(a,b,c) = (3,4,5)\ X_n X_{n-1} \cdots X_1$，故存在 $A \in W$，使得 $(a,b,c) = (3,4,5)\ A$。

引理 2：设 (a,b,c)，(a_1,b_1,c_1) 是任意两个（可以相等）规范本原勾股向量，则任意 $F_i, F_j\ (i = 1,\cdots,3,\ j = 1,\cdots,3, i \neq j)$ 有 $(a,b,c)\ F_i \neq (a_1,b_1,c_1)\ F_j$。

证明：f（(a,b,c)）$= \begin{pmatrix} k \\ m \end{pmatrix}$，$f$（$(a_1,b_1,c_1)$）$= \begin{pmatrix} k_1 \\ m_1 \end{pmatrix}$，显然有 $k > m > 0$ 及 $k_1 > m_1 > 0$。

由定理 3 可得：f（$(a,b,c)\ F_1$）$= \begin{pmatrix} 2k+m \\ k \end{pmatrix}$，$f$（$(a,b,c)\ F_2$）$= \begin{pmatrix} 2k-m \\ k \end{pmatrix}$，$f$（$(a,b,c)\ F_3$）$= \begin{pmatrix} k+2m \\ m \end{pmatrix}$，$f$（$(a_1,b_1,c_1)\ F_1$）$= \begin{pmatrix} 2k_1+m_1 \\ k_1 \end{pmatrix}$，$f$（$(a_1,b_1,c_1)\ F_2$）$= \begin{pmatrix} 2k_1-m_1 \\ k_1 \end{pmatrix}$，$f$（$(a_1,b_1,c_1)\ F_3$）$= \begin{pmatrix} k_1+2m_1 \\ m_1 \end{pmatrix}$。

若 $(a,b,c)\ F_1 = (a_1,b_1,c_1)\ F_2$，则 $\begin{pmatrix} 2k+m \\ k \end{pmatrix} = \begin{pmatrix} 2k_1-m_1 \\ k_1 \end{pmatrix}$，从而 $k = k_1$，$m = -m_1$ 矛盾。

若 $(a,b,c)\ F_1 = (a_1,b_1,c_1)\ F_3$，则 $\begin{pmatrix} 2k+m \\ k \end{pmatrix} = \begin{pmatrix} k_1+2m_1 \\ m_1 \end{pmatrix}$，从而 $k = m_1$，$m = k_1$，由 $k > m > 0$ 得 $k_1 < m_1$ 矛盾。

若 $(a,b,c)\ F_2 = (a_1,b_1,c_1)\ F_3$，则 $\begin{pmatrix} 2k-m \\ k \end{pmatrix} = \begin{pmatrix} k_1+2m_1 \\ m_1 \end{pmatrix}$，从而 $k = m_1$，$-m = k_1$ 矛盾。

同理可证明若 $(a,b,c)\ F_2 = (a_1,b_1,c_1)\ F_1$，$(a,b,c)\ F_3 = (a_1,b_1,c_1)\ F_1$ 与 $(a,b,c)\ F_3 = (a_1,b_1,c_1)\ F_2$ 都会导出矛盾。

综上，任意 $F_i, F_j\ (i = 1,\cdots,3,\ j = 1,\cdots,3, i \neq j)$ 有 $(a,b,c)\ F_i \neq (a_1,b_1,c_1)\ F_j$。

由引理 2 容易得到如下的引理 3。

引理 3：设 (a,b,c)，(a_1,b_1,c_1) 是任意两个规范本原勾股向量，若 $F_i, F_j\ (i = 1,\cdots,3,\ j = 1,\cdots,3)$ 使得 $(a,b,c)\ F_i = (a_1,b_1,c_1)\ F_j$ 成立，则必有 $(a,b,c) = (a_1,b_1,c_1)$，及 $F_i = F_j$ 成立。

定理 5：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 $(a,b,c) = (3,4,5)\ A$。

证明：：设 (a,b,c) 是任意一个规范本原勾股向量，并且 $c \geq 5$。由定理 4 知，存在 $A \in W$，使得 $(a,b,c) = (3,4,5)\ A$。下面证明惟一性。

假设 $B \in W$，也使得 $(a,b,c) = (3,4,5)\ B$。设 $A = X_1X_2\cdots X_m$（$X_i \in \{F_1,F_2,F_3\}$），$B = Y_1Y_2\cdots Y_n$（$Y_j \in \{F_1,F_2,F_3\}$），则 $(3,4,5)\ X_1X_2\cdots X_m = (3,4,5)\ Y_1Y_2\cdots Y_n$。若 $m>n$，由引理 3 有 $X_m = Y_n$，且 $(3,4,5)\ X_1X_2\cdots X_{m-1} = (3,4,5)\ Y_1Y_2\cdots Y_{n-1}$；不断利用引理 3 可得 $X_m = Y_n$，$X_{m-1}=Y_{n-1}$，…，$X_{m-n+1}=Y_1$及 $(3,4,5)\ X_1X_2\cdots X_{m-n} = (3,4,5)$ 成立。又容易验证 $X_1X_2\cdots X_{m-n} = (3,4,5)$ 是不可能成立的，所以 $m>n$ 不可能成立。同理可证 $n>m$ 不可能成立，故有 $m=n$。当 $m=n$ 时，不断利用引理 3 可得 $X_m = Y_n$，$X_{m-1}=Y_{n-1}$，…，$X_1=Y_1$，所以 $X_1X_2\cdots X_m = Y_1Y_2\cdots Y_n$，从而 $A=B$。

综上，若 (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 $(a,b,c) = (3,4,5)\ A$。

引理 4：$(1,0,1) = (3,4,5)\ F_1^{-1}$。

记 $G_1 = \{\ D_1 = diag[1,1,1]$，$D_2 = diag[-1,1,1]$，$D_3 = diag[1,-1,1]$，$D_4 = diag[1,1,-1]$，$D_5 = diag[-1,-1,1]$，$D_6 = diag[-1,1,-1]$，$D_7 = diag[1,-1,-1]$，$D_8 = diag[-1,-1,-1]\}$。

定理 6：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，由定理 5 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 $(3,4,5)\ A = (x,y,z)$，$(3,4,5)\ A_1 = (x_1,y_1,z_1)$，由定理 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 $(3,4,5)\ A = (3,4,5)\ A_1$，再由定理 5 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 4 和定理 6 可以得到如下的定理：

定理 7：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：（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) 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，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，$C_1\in G_1$）及 $p\in Z$，使得 $(a',b',c') = p\ (a,b,c)\ C\ A^{-1}\ A_1\ C_1$。

（3）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，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，$C_1 \in G_1$）及$p \in Z$和$q \in Z$，使得$(a',b',c') = \frac{p}{q}(a,b,c)\ C\ A^{-1}\ A_1\ C_1$。