中 国 科 学
1984 年 3 月　　A 辑　　第 3 期

一种 Goldbach 可换环的数论性质

王 世 强
（北京师范大学数学系）

摘　要

本文用模型论及数论方法讨论一种可换环 R 的数论性质. R 是整数环的扩环，它适合 Goldbach 性质，在其中有无限多个孪生的素数三元组. R 有很多与整数环 I 相同的性质，也有很多与 I 不同的性质. 这些说明一些数论命题间的和谐性以及它们对于整数环理论的部分和谐性.

在 [1—3] 中，我们用模型论及数论方法证明了，对于每一个二次代数整数环及很多三次代数整数环，都存在具有以及不具有 Goldbach 性质的可换扩环(该性质指：任一非零，非单位的元的 2 倍都是两个素元之和). 这些结果与数论中 Goldbach 问题的研究并无直接联系. 但是，从证明论的观点看，进一步考查这些扩环的数论性质，对于了解 Goldbach 性质等数论命题的相对和谐性及相对独立性有一定的意义. 另外，作为用模型论方法与通常的数论方法相结合地对一些环作较具体的研究，也有其方法论的意义.

本文考查整数环 I 的一种具有 Goldbach 性质的扩环 R. 讨论普通数论中一些定理在 R 中成立或不成立的情况. 整数环 I 的这类扩环是很多的，本文只取一种 R 作一些典型性的讨论(因为本工作目前的主要目的在于较进一步地揭示现象及说明方法，而不在于系统地研究这些环的自身).

关于模型论，只用到超积的概念及其基本性质（可参看文献[4]第 4.1 节).

一、R 的定义及一般性质

令 N 为正整数集. $F=\{X: X\subseteq N$ 且 $N\backslash X$ 有限$\}$ 为 N 上的 Fréchet 滤集. D 为由 F 任意一种方式扩大而成的 N 上的超滤集.

令 p_i 为第 i 个正有理素数 $(i\in N)$. K_n 为整数环 I 对于其理想子环 $(p_1^2p_2^2\cdots p_n^2)$ 的剩余类环 $(n\in N)$.

令 R 为超积 $\Pi_D K_n$, L 为形式语言 $\{+, \times, 0, 1\}$.

引理 1.1. 1) K_n 中元素 a 为单位的充分必要条件是：$p_1, p_2, \cdots, p_n$ 都不能整除 a. 2) K_n 中元素 a 为素元的充分必要条件是：a 与 $p_1, p_2, \cdots, p_n$ 之一相伴. 3) K_n 适合 Goldbach 性质. 4) 当 $n\geqslant 6$ 时，K_n 中至少有 $(218/385)p_1p_2\cdots p_n$ 个$(\pi, \pi+2, \pi+6)$形状的素元组，至少有 $(690/1001)p_1p_2\cdots p_n$ 个 $(\pi, \pi+4, \pi+6)$ 形状的素元组.

本文 1982 年 12 月 2 日收到.

下列二定理给出 R 的主要特点及其与 I 的一些相似之点.

定理 1.1. 1) R 是有 1 的可换环，它是 I 的扩环. 2) R 适合 Goldbach 性质. 3) R 中有无限多个 $(\pi, \pi+2, \pi+6)$ 形状的素元组，也有无限多个 $(\pi, \pi+4, \pi+6)$ 形状的素元组. 4) I 中每一素数都是 R 中的素元，I 中每一合数都是 R 中的合元.

定理 1.2. 1) L 中一切在 I 中成立的正命题 θ (即：θ 中的逻辑符号只有"与"、"或"及量词)都在 R 中成立. 2) L 中一切在 I 中成立的形状为 $(\exists x_1 \cdots x_n)\,\phi(x_1, \cdots, x_n)$ (ϕ 中无量词) 的命题都在 R 中成立. 3) L 中一切在 I 对于某一理想子环 $(p_1^{r_1}p_2^{r_2}\cdots p_n^{r_n})$ (其中 $0 \leqslant r_1, r_2, \cdots, r_n \leqslant 2$)的剩余类环中成立的形状为 $\neg(\exists x_1 \cdots x_n)(p(x_1, \cdots, x_n) = 0)$ (p 为整系数多项式)的命题都在 R 中成立.

关于 R 中元素的因式分解，有下列诸性质.

定理 1.3. 1) R 含有非零的零因子(在本文中，零算作零因子). 2) R 中任何有限多个素元的积不为零. 3) R 中存在非单位、非幂零的元 a 不能表示为有限个素元的积. 4) 在 R 中，若 π 为一素元且 π 整除 xy，则 π 整除 x 或 y. 5) 在 R 中，若一元素 a 能表示为有限个素元的积，则其表示法是唯一的. 6) 在 R 中，二元素 a, b 的公因子 d 为最大公因子的充分必要条件是 d 能表示为 $ar + bs$ 形状. 7) R 中任二元素 a, b 都有最大公因子(a, b)存在. 8) R 的任何有限生成的理想子环都是主理想子环. 9) 存在 R 的非主理想子环.

下面列举 R 的一些简单数论性质.

定理 1.4. 1) 在 R 中，方程 $ax = b$ 当有解时，其解的个数可为有限或无限多. 2)对任何 $a_1, \cdots, a_m, a \in R$，不定方程 $a_1x_1 + \cdots + a_mx_m = a$ 在 R 中有解的充分必要条件是 $(a_1, \cdots, a_m)$整除a. 3) 在 R 中，为使 x, y, z 适合不定方程 $x^2 + y^2 = z^2$，"存在 $u, v \in R$，使 $z = \pm(u^2 + v^2)$，并且 x, y 中有一个为 $\pm(u^2 - v^2)$，而另一个为 $\pm 2uv$" 只是充分条件而非必要条件. 4) 对任何 $a, b, m \in R$，同余式 $ax \equiv b \pmod{m}$ 有解的充分必要条件是(a, m) 整除 b. 5) 若 m 为 I 中正整数，$a \in R$，且$(a, m) = 1$，则 m 整除 $a^{\phi(m)} - 1$($\phi(m)$ 为 Euler 函数).

在 R 中，以素元为模的平方剩余，其性质与 I 中有很大的不同. 初步列举一些事例如下.

定理 1.5. 在 R 中：1) 存在 $8k + 3$ 形及 $8l + 5$ 形的素元以 2 为平方剩余. 2) 存在 $8k + 1$ 形及 $8l + 7$ 形的素元不以 2 为平方剩余. 3) 存在 $10k + 3$ 形及 $10l + 7$ 形的素元以 5 为平方剩余. 4) 存在 $10k + 1$ 形及 $10l + 9$ 形的素元不以 5 为平方剩余. 5) 存在 $4k + 3$ 形的素元以 -1 为平方剩余. 6) 存在 $4k + 1$ 形的素元不以 -1 为平方剩余. 7) 存在 $6k + 5$ 形的素元以 -3 为平方剩余. 8) 存在 $6k + 1$ 形的素元不以 -3 为平方剩余.

以上的一些结果的证明都比较直接(虽然有的并不简短)，因限于篇幅而略去.

二、一种弱形式的 Dirichlet 定理

首先，由 I 中的 Dirichlet 定理和 $I \subset R$ 以及 R 的性质 (I 中素元在 R 中仍为素元)，显见，R 中有一个直接由 I 中继承来的弱形式的 Dirichlet 定理. 下面证明另一个弱形式的 Dirichlet 定理，它包括了上述定理(这一点不难说明，略去).

定理 2.1. 在 R 中，若 $\alpha \neq 0$，且 $(\alpha, \beta) = 1$，并且 α 的互不相伴的素因子只有有限多种，则存在无限多个形状为 $\alpha x + \beta (x \in R)$ 的素元.

证. 1) 先在诸 K_n 中考虑.

对任何自然数 $m \geqslant 0$ 及 $r \geqslant 2$，令 $\theta_{m,r}$ 为下列的 1 阶命题（指：$\theta_{m,r}$ 为 L 中表达下列内容的任一 1 阶语句．以下仿此）：

“对一切 a, b．若 $a \neq 0$，且 $(a, b) = 1$，并且 a 恰有 m 个互不相伴的素因子，则（至少）存在 $\phi(p_2^2 \cdots p_r^2)$ 个 $ax + b$ 形状的素元．”

现在证明，若 $n = m + r$，则 $\theta_{m,r}$ 在 K_n 中成立．

设 K_n 中的元 a, b 适合 $a \neq 0$ 及 $(a, b) = 1$，并且 a 在 K_n 中恰有 m 个互不相伴的素因子，则在 K_n 的 n 个互不相伴的素元 $p_1, p_2, \cdots, p_n$ 中有 r 个不是 a 的因子．

1.1) 若 $p_1, \cdots, p_r \nmid a$．

当 x 取值 $0, 1, 2, \cdots p_1^2 \cdots p_r^2 - 1$ 时，诸 ax 互不相等（在 K_n 中）．[因：若在 K_n 中有 $ax_1 = ax_2$，则在 I 中有 $p_1^2 \cdots p_n^2 \mid a(x_1 - x_2)$，从而有 $p_1^2 \cdots p_r^2 \mid x_1 - x_2$，故必 $x_1 = x_2$]．从而诸 $ax + b$ 也互不相等．

在 I 中来看等差数列 $S_1: ax + b (x = 0, 1, 2, \cdots, p_1^2 \cdots p_r^2 - 1)$．

i) 由 a, b 在 K_n 中互素及 K_n 中素元情况可知，a，b 在 I 中不以 $p_1, \cdots, p_n$ 为公因子．再由 $p_{r+1}, \cdots, p_n \mid a$ 可知 $p_{r+1}, \cdots, p_n \nmid ax + b$（对每一 x）．

ii) 由 $2 (= p_1) \nmid a$ 可知，S_1 中含有一半偶数，其中又有一半是 2 的倍数而非 4 的倍数，它们组成 S_1 的子等差数列 S_2，其公差为 $4a$，项数为 $p_2^2 \cdots p_r^2$．

再由 $p_2, \cdots, p_r \nmid 4a$ 可知，当以 $p_2^2 \cdots p_r^2$ 为模时，S_2 构成一个完全剩余系．由此易见，S_2 中与 $p_2 \cdots p_r$ 互素者的个数 $\nu = \phi(p_2^2 \cdots p_r^2)$．此外由 ii) 可知，$S_2$ 中的 ν 个与 $p_2 \cdots p_r$ 互素的数都是 $2u$（u 为奇数）形状．再由 i) 即知，u 与 $p_1, p, \cdots, p_r, \cdots p_n$ 都互素．

把以上的讨论放到 K_n 中来看，易见其诸结论也都成立．所以，S_2 中的上述 ν 个数（由 S_2 及 S_1 的定义可知它们在 K_n 中互不相等）都是 $2u$ 形状，且由上可知，u 为 K_n 中的单位，从而这 ν 个数 $2u$ 都是 K_n 中的素元．所以，K_n 中至少已含有这 ν 个 $ax + b$ 形状的素元．

1.2) 若 $p_{i_1}, \cdots, p_{i_r} \nmid a (1 \leqslant i_1 < \cdots < i_r \leqslant n)$．可以仿 1.1) 讨论，所得的 ν 将更大．

所以，$\theta_{m,r}$ 在 K_{m+r} 中成立．

2) 由 1) 及超积性质可知，对每个 $m \geqslant 0$（令 r 无限增大），在 R 中有下列（非 1 阶的）命题成立：

“对一切 α, β．若 $\alpha \neq 0$ 且 $(\alpha, \beta) = 1$ 并且 α 恰有 m 个互不相伴的素因子，则存在无限多个 $\alpha x + \beta$ 形状的素元．”

又由于 m 是任意的自然数，所以定理 2.1 成立．

下列一般形式的 “Dirichlet 命题”在 R 中不成立：“若 $\alpha \neq 0$ 且 $(\alpha, \beta) = 1$，则存在无限多个形状为 $\alpha x + \beta$ 的素元．”因为有如下的事实：

定理 2.2. 存在 $\alpha \in R$，$\alpha \neq 0$，并且对一切 $x \in R$，$\alpha x + 1$ 都是 R 中的单位．

证．易证相应的命题在每一 K_n 中成立，从而在 R 中成立．

三、 Fermat 命题

关于 Fermat 命题，在一般可换环时可以有不同的提法，例如下列几种：

$\theta_m^{(1)}$：“对任何 x, y, z，若 $x^m + y^m = z^m$，则 $xyz = 0$”$(m \geqslant 3)$．

$\theta_m^{(2)}$：“对任何 x, y, z，若 $x^m + y^m = z^m$，则 xyz 是幂零元”$(m \geqslant 3)$．

$\theta_m^{(3)}$："对任何 x, y, z，若 $x^m + y^m = z^m$，则 xyz 是零因子"（$m \geqslant 3$）.

还可以把$\theta_m^{(1)}$中的结论改为"$x = 0$ 或 $y = 0$ 或$z = 0$"，而得命题 $\rho_m^{(1)}$，以及由 $\theta_m^{(2)}$，$\theta_m^{(3)}$ 类似地得到 $\rho_m^{(2)}$，$\rho_m^{(3)}$（其中 $\theta_m^{(2)}$，$\rho_m^{(2)}$ 不是 1 阶命题）. 在这里，"u 是零因子"的含意是"存在非零元 v 使 $uv = 0$"（按此含意，零自身也是零因子，除了在只含 1 个元的不足道的环中之外）. 这几种提法，在 I 时虽然互相等价，在一般可换环时则未必等价.

定理 3.1.　对任何 $m \geqslant 1$，在 R 中都有 $\rho_m^{(3)}$ 成立，从而也有 $\theta_m^{(3)}$ 成立.

证. 易见 $\rho_m^{(3)}$ 在每个 K_n 中成立，从而在 R 中也成立.

定理 3.2.　对任何 $m \geqslant 1$，在 R 中 $\theta_m^{(2)}$ 都不成立. 从而 $\theta_m^{(1)}$，$\rho_m^{(1)}$，$\rho_m^{(2)}$ 也都不成立.

证. 1) 先证 m 为奇数的情况. $m = 1$ 时，显然. 以下设 $m > 1$.

1.1) 首先，在 I 中取一正奇素数 p，使 $(m, \phi(p^2)) = 1$. 并且为便于 2)中使用，可取 $p > 5$ 且为 $4k + 3$ 形状. p 的存在可如下看出：由 m 为奇数知存在 x_1，使 $mx_1 \equiv 1 \pmod 4$，设 $mx_1 = 4k_1 + 1$，考虑等差数列 $S:(4m)y + (mx_1 + 2)$ $(y = 0, 1, 2, \cdots\cdots)$. 显见，$S$ 中的数均为 $4k + 3$ 形状. 设 $d = (4m, mx_1 + 2)$，则由 m 为奇数可知 m 的因子均非 d 的因子，又由 $d = (4m, 4k_1 + 3)$ 知 $2 \nmid d$，所以 $d = 1$. 于是由 I 中的 Dirichlet 定理知，在 S 中存在无限多素数，任取其中一个大于 5 的作为 p，则由 S 中诸项的形状可知 m 与 $p(p-1)$ 互素. 设 $p = p_j$.

1.2) 考虑 I 中的数以 p^2 为模时与 p^2 互素的 $\phi(p^2)$ 个剩余类组成的乘法群 U. U 为循环群（因 p^2 有原根，例如见文献[5] p. 53）. 设 u 为 U 的一个生成元.

由 $(m, \phi(p^2)) = 1$ 知 u^m 也是 U 的生成元，由此可知 U 的每个元都能表为 $x^m (x \in U)$ 形状. 特别地，对于 $2 \in U$，存在 $v \in U$，使 $2 = v^m$.

在 I 中看，由以上讨论可得

$$1^m + 1^m \equiv v^m \pmod{p_j^2} \quad (p_j \nmid v).$$

从而，当 $n \geqslant j$ 时，令 $x_n = y_n = p_1 \cdots p_{j-1} p_{j+1} \cdots p_n$，$z_n = v p_1 \cdots p_{j-1} p_{j+1} \cdots p_n$，则有

$$x_n^m + y_n^m \equiv z_n^m \pmod{p_1^2 \cdots p_j^2 \cdots p_n^2} \quad (p_j \nmid x_n, y_n, z_n).$$

在 $K_n (n \geqslant j)$ 中看：$x_n^m + y_n^m = z_n^m$ 且 $x_n y_n z_n$ 均非幂零元，

1.3) 在 R 中，令 $\bar{x} = (0, \cdots, 0, x_j, x_{j+1}, x_{j+2}, \cdots\cdots)_D$，其中每个 x_{j+i} 依 1.2)在 K_{j+i} 中选取. 仿此取 $\bar{y}, \bar{z}$. 则有 $\bar{x}^m + \bar{y}^m = \bar{z}^m$. 假若 $\bar{x}\bar{y}\bar{z}$ 是 R 中的幂零元，则存在正整数 r，使 $(\bar{x}\bar{y}\bar{z})^r = 0$. 由此及超积定义易知 $\sigma = \{i : (x_{j+i} y_{j+i} z_{j+i})^r = 0\} \in D$，所以 σ 不空. 从而，对任何 $i \in \sigma$，$x_{j+i} y_{j+i} z_{j+i}$ 应为 K_{j+i} 中的幂零元，与 1.2) 不符合，所以 $\bar{x}\bar{y}\bar{z}$ 不是幂零元. 同理 $\bar{y}, \bar{z}$ 也都不是幂零元.

所以当 m 为奇数时，$\theta_m^{(2)}$ 在 R 中不成立.

2) 当 m 为偶数时. 设 $m = 2^s m_1$（m_1 奇，$s \geqslant 1$）.

为便于引用 1) 中论证，以下将 m 改记为 m'，将 m_1 改记为 m.

2.1) 依 1.1)取 $p = p_j$，使 $(m, \phi(p^2)) = 1$，$p > 5$，且为 $4k + 3$ 形状.

2.2) 依 1.2)取 u 为 U 的任一生成元. u^2 生成 U 的子群 V，元数为 $\frac{1}{2}\phi(p^2) = \frac{1}{2} p(p-1)$. u^4 生成 V 的子群 V_1. 由 p 为 $4k + 3$ 形知 $(4, p(p-1)) = 2$，从而 V_1 的元数为 $\frac{1}{2} p(p-1)$ $V_1 = V$. 由此可知，V 中每元都能表为 $x_2^4 (x_2 \in U)$ 形状. 再仿此讨论可知，V 中每个元都能表为 $x_3^8, x_4^{16}, \cdots\cdots (x_3, x_4, \cdots\cdots \in U)$ 的形状.

由 $p>5$ 知，$p\nmid 3,4,5$，从而 $3,4,5\in U$，$3^2,4^2,5^2\in V$. 由上段知存在 $x,y,z\in U$，使 $x^{2^s}=3^2$，$y^{2^s}=4^2$，$z^{2^s}=5^2$. 又由 1.2)知存在 $x_1,y_1,z_1\in U$，使 $x_1^m=x$，$y_1^m=y$，$z_1^m=z$.

在 I 中看，由 $3^2+4^2=5^2$ 及以上讨论可知，有(注意 $m'=2^sm$) $x_1^{m'}+y_1^{m'}\equiv z_1^{m'}\pmod{p_j^2}$ $(p_j\nmid x_1,y_1,z_1)$. 从而，当 $n\geqslant j$ 时，令 $u_n=x_1p_1\cdots p_{j-1}p_{j+1}\cdots p_n$，$v_n=y_1p_1\cdots p_{j-1}p_{j+1}\cdots p_n$，$w_n=z_1p_1\cdots p_{j-1}p_{j+1}\cdots p_n$，则有

$$u_n^{m'}+v_n^{m'}\equiv w_n^{m'}(\bmod p_1^2\cdots p_j^2\cdots p_n^2)\quad (p_j\nmid u_n,v_n,w_n).$$

在 $K_n(n\geqslant j)$ 中看：$u_n^{m'}+v_n^{m'}=w_n^{m'}$ 且 $u_nv_nw_n$ 均非幂零元.

2.3) 仿 1.3) 可知，$\theta_{m'}^{(2)}$ 在 R 中不成立. 定理 3.2 证毕.

四、平方和问题

由整数环 I 中关于正整数的 4 平方和定理，易见 K_n 及 R 中每一元素都是 4 个平方元的和. 以下作进一步的考查.

定理 4.1. R 中每一元素都是 3 个平方元之和.

证.

任取 I 中正整数 a.

i) 若 $a\equiv 1,2,3,5,6(\bmod 8)$，则 a 在 I 中能表为 3 个平方元之和(参看文献[6]p.175)，因而在 K_n 中也如此.

ii) 若 $a\equiv 7(\bmod 8)$，令 $a_1=a+p_1^2p_2^2\cdots p_n^2$，则易见 $a_1\equiv 3(\bmod 8)$，因而由i)知在 K_n 中 $a=a_1$ 为 3 个平方元之和.

iii) 若 $a\equiv 0,4(\bmod 8)$，把 a 表示为 $4^t(8k+l)$ 形状 $(t>0;l=1,2,3,5,6,7)$. 由 i)，ii) 知，在 K_n 中 $8k+l$ 为 3 个平方元之和，从而易见 a 也如此.

由上可知，对每一 n，K_n 中每一元素都是 3 个平方元之和. 因而 R 中也如此.

引理 4.1. 对每一 $n\geqslant 1$，K_n 中的元素 a 能表示为两个平方元之和的充分必要条件是：a 不为 $4k+3$ 形状并且对于 $p_1,\cdots,p_n$ 中每一个 $4k+3$ 形的 p_i，或 $p_i\nmid a$ 或 $p_i^2\mid a$.

证. 任取整数环 I 中一非负整数 a，看它在 K_n 中是否两个平方元之和(以下令 $\mu=p_1^2p_2^2\cdots p_n^2$).

1) 若 $a\equiv 3(\bmod 4)$，则对任何 $x,y\in I$ 都有 $x^2+y^2\not\equiv a(\bmod 4)$，从而 $x^2+y^2\not\equiv a(\bmod \mu)$. 所以此时 a 在 K_n 中不是平方和.

2) 若 a 有一个 $4k+3$ 形的素因子 $p_i(i\leqslant n)$ 其指数为 1. 假若在 K_n 中有 $a=x^2+y^2$，则在 I 中有 $a\equiv x^2+y^2=a_1(\bmod \mu)$. 由 μ 的形状可知该 p_i 在 a_1 中指数也是 1，从而由整数环 I 中结果知 a_1 不能表为平方和(参看文献 [5] p.126)，与 $a_1=x^2+y^2$ 产生矛盾. 所以此时 a 在 K_n 中不是平方和.

3) 当 a 不为 1)，2) 的情况时.

3.1) 若 a 为奇数，则 a 为 $4k+1$ 形.

令 $(a,\mu)=d(>0)$，则由 μ 的形状知 d 为 $p_1^{r_1}\cdots p_n^{r_n}$ 形，且每 $r_i\leqslant 2$. 对于每个 $4k+3$ 形的 $p_i(1\leqslant i\leqslant n)$，由于 a 不为 2) 中情况，易见 p_i 在 d 中指数或为零或为 2 (特知 d 为 $4k+1$ 形状).

令 $a=a'd$，$\mu=\mu'd$，则 $(a',\mu')=1$. 考虑等差数列 $S:a'+\mu'x(x=0,1,2,\cdots\cdots)$. 由

a 为奇数知 d 为奇数，故知 $4|\mu'$. 又由 a 为 $4k+1$ 形状及上段可知 a' 也如此. 所以 S 中各项都是 $4k+1$ 形状. 又由 I 中 Dirichlet 定理知在 S 中有素数存在，任取其一为 r. 设 $r=a'+\mu' x_1$，则 $dr=a+\mu x_1\equiv a(\mathrm{mod}\,\mu)$. 并且由上段及 I 中结果可知 dr 在 I 中能表为平方和，从而 a 在 K_n 中能表为平方和.

3.2) 若 a 为偶数. 设 $a=2^s a_1$ (a_1 为奇数，$s\geqslant 1$).

3.2.1) 若 a_1 为 $4k+1$ 形状. 由 a 不为 2) 的情况显见 a_1 也不为 2) 的情况. 所以 a_1 是 3.1)的情况，从而 a_1 在 K_n 中是平方和. 由此及 $2=1^2+1^2$ 反复利用可换环中恒等式 $(x_1^2+y_1^2)\cdot(x_2^2+y_2^2)=(x_1x_2+y_1y_2)^2+(x_1y_2-x_2y_1)^2$ 即知 a 在 K_n 中也是平方和.

3.2.2) 若 a_1 为 $4k+3$ 形状. 令

$$a_2=a_1+\frac{1}{2}\mu,$$

则由 μ 的形状可知 a_2 为 $4k+1$ 形. 并且 $2a_1\equiv 2a_2(\mathrm{mod}\,\mu)$，从而有 $a\equiv 2^s a_2=a^*(\mathrm{mod}\mu)$. 现在考虑 a^*.

a^*显然不是 1) 的情况 (因 $s\geqslant 1$). 由 $a^*=2^s a_2=a+2^{s-1}\mu$ 及 a 不是 2)的情况可知 a^* 也不是. 再由上段即知 a^* 是 3.2.1) 的情况. 所以 a^* (从而 a)在 K_n 中是平方和. 引理 4.1 证毕.

K_n 中的这一充分必要条件，不是一个与 n 无关的 1 阶命题，所以不能由它简单地转移到 R 中而得出相应的充分必要条件. 我们利用它只得到了一些较弱的结果.

定理 4.2. 1) 如果 R 中一元素 a 能表示为两个平方元之和，则 a 不是 $4k+3$ 形状，并且 I 中每一 $4k+3$ 形状的正素数 p 在 a 中的指数不是 1. 2) 如果 R 中一元素 a 不是 $4k+3$ 形状，并且 a 没有指数为 1 的 $4k+3$ 的素因子，则 a 能表示为两个平方元之和.

证. 1) 设 R 中的元素 $a=(a_1,a_2,a_3,\cdots\cdots)_D$ 能表示为两个平方元之和. 则由超积性质可知 $\sigma=\{i:a_i$ 在 K_i 中能表为二平方之和$\}\in D$. 又令 $\tau=\{i:$ 在 K_i 中 a_i 不为 $4k+3$ 形状$\}$, $\rho=\{i:$在 K_i 中对于 $p_1,\cdots,p_i$ 中每一 $4k+3$ 形的 p_j，或 $p_j\nmid a_i$ 或 $p_j^2|a_i\}$，则由引理 4.1 可知 $\sigma=\tau\cap\rho$，从而也有 $\tau,\rho\in D$.

由 $\tau\in D$ 可知，在 R 中 a 不为 $4k+3$ 形状.

任取 I 中一个 $4k+3$ 形的正素数 p_r. 假若在 R 中 $p_r|a$ 而 $p_r^2\nmid a$. 则由超积性质易见有 $\lambda=\{i:i\geqslant r$ 且 $p_r|a_i$ 且 $p_r^2\nmid a_i\}\in D$. 从而有 $\lambda\cap\rho\in D$，$\lambda\cap\rho$ 不空. 对任何$i\in\lambda\cap\rho$，由 $i\geqslant r$ 及 $i\in\rho$ 可知或 $p_r\nmid a_i$ 或 $p_r^2|a_i$，从而与 $i\in\lambda$ 产生矛盾. 所以，在 R 中或 $p_r\nmid a$或$p_r^2|a$.

所以，定理中的 1) 成立.

2) 设 R 中的元素 $a=(a_1,a_2,a_3,\cdots\cdots)_D$ 不能表示为两个平方元之和. 则由超积性质可知 $\sigma_1=\{i:a_i$ 在 K_i 中不能表为二平方之和$\}\in D$. 又令 $\tau_1=\{i:$ 在 K_i 中，或 a_i 为 $4k+3$ 形，或 a_i 有指数为 1 的 $4k+3$形状的素因子$\}$，则由引理 4.1 可知 $\sigma_1\subseteq\tau_1$，从而有 $\tau_1\in D$. 由于 τ_1 中的定义条件是 1 阶命题，故由超积性质可知，在 R 中或 a 为 $4k+3$ 形状或 a 有指数为 1 的 $4k+3$ 形状素因子.

所以，定理中的 2) 成立. 定理 4.2 证毕.

注意：上述的 σ_1,τ_1 未必相等. 所以，若有 $\tau_1\in D$ 尚不知必有 $\sigma_1\in D$. 即 2) 中的充分条件尚不知是否必要条件. $\sigma_1\neq\tau_1$ 的例子如下可见：在 K_3 中 ($\mu=2^2\cdot 3^2\cdot 5^2=900$)，70 有

$4k+3$ 形的素因子 35，且指数为 1．但在 K_3 中 $70=3^2+31^2$.

定理 4.3. 如果 $a\in I$，则 a 在 R 中能表示为两个平方元之和的充分必要条件是：a 在 I 中不为 $4k+3$ 形状，并且 I 中每一 $4k+3$ 形的正素数 p 在 a 中的指数不是 1.

证明与上定理类似，略去.

参 考 文 献

[1] 王世强，北京师范大学学报，**1**(1982)，17—22.
[2] 王世强、武涛，同上，**3**(1982)，21—25.
[3] 王世强，中国科学A辑 1984，1：16—23.
[4] Chang, C. C. & Keisler, H. J., *Model Theory*, North-Holland Publishing Company. 1973.
[5] LeVeque, W. J., *Topics in Number Theory*, Vol. 1, Addison-Wesley Publishing Company, 1956.
[6] Mordell, L. J., *Diophantine Equations*, Academic Press Inc., 1969.