第17卷第3期 数学研究与评论 Vol. 17 No. 3
1997年8月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Aug. 1997

关于NF-环的构造*

杨子胥 郝秀梅
(山东财政学院数学系, 济南250014)

摘 要 研究了无限的NF-环及有限的NF-环, 并且给出了有限NF-环的构造

关键词 NF-环, 循环环
分类号 AMS(1991) 16A45/CCL O153.3

本文所说的环R均指结合环; 所说环中元素a的阶, 均指a在R的加群$(R, +)$中的阶, 并用$|a|$表示. 又常用Z_n表示以正整数n为模的剩余类环.

定义1 设R是一个环. 如果R无非平凡子环, 或者R的所有非平凡子环都是域, 则称R是一个NF-环.

R的非平凡子环有时也称为R的真子环.

显然, 一阶环和素阶环均为NF-环; 又任何有限域都是NF-环, 因为它如果有非平凡子环, 则其非平凡子环便是无零因子的有限环, 从而必为域.

§1 关于无限NF-环

定理1 设R是一个NF-环. 如果R有零因子, 则R必为有限环.

证明 若不然, 设R为无限环, 则由[3]知, R必有真子环. 但因R是NF-环, 故其任何真子环都是域, 从而R必含有素域.

如果R中有素域F的特征数为∞, 则F与有理数域Q同构. 但Q有整数环Z为其非域真子环, 从而R有与Z同构的非域真子环, 这与R是NF-环矛盾. 因此, R中每个素域的特征数都必为素数.

由于R有零因子, 故在R中存在元素$a \neq 0, b \neq 0$而$ab = 0$. 令

$$S_i = \{na^i \mid n \in Z\}, \quad i = 1, 2, 3, \cdots,$$

则显然$S = \sum_{i=1}^{\infty} S_i$是$R$的一个非零子环. 又$b \notin S$, 因若$b \in S$, 则令

$$b = \sum_{i=1}^{k} n_i a^i, \quad n_i \in Z.$$

右乘以b, 得$b^2 = 0$. 于是零乘环

* 1994年11月14日收到

$$\langle b\rangle = \{nb \mid n \in Z\}$$

是 R 的一个非域真子环(因为 R 含有素域, 故 $\langle b\rangle \neq R$), 这与 R 是NF-环矛盾. 因此 $b \notin S$, 即 S 是NF-环 R 的一个真子环, 从而 S 为域. 于是 S 含有素域 F_1, 设其特征数为素数 p, 且

$$F_1 = \{0, e_1, 2e_1, \cdots, (p-1)e_1\},$$

其中 e_1 是 F_1 的单位元, 当然也是域 S 的单位元. 又因 $a \in S$, 故在域 S 中有

$$aa^{-1} = a^{-1}a = e_1.$$

同理, 令

$$S_i' = \{nb^i \mid n \in Z\}, \quad i = 1, 2, 3, \cdots,$$

则 $S' = \sum_{i=1}^{\infty} S_i'$ 也是NF-环 R 的真子环, 从而也是域. 设 S' 含有的素域为

$$F_2 = \{0, e_2, 2e_2, \cdots, (q-1)e_2\},$$

其中 q 为素数, e_2 是 F_2 与 S' 的单位元, 且在 S' 中有

$$bb^{-1} = b^{-1}b = e_2.$$

由上可得 $e_1e_2 = a^{-1}abb^{-1} = 0$, 从而可知直和 $F_1 \oplus F_2$ 是 R 的一个 pq 阶非域真子环(因为假设 R 是无限环), 这与 R 是NF-环矛盾. 因此, R 必为有限环.

§2 有限NF-环的构造

为了进一步讨论有限NF-环, 本节先介绍和证明四个引理.

定义 2 一个环称为循环环, 如果其加群是一个循环群.

引理 1[1] 循环环的子加群是(循环)子环, 也是理想.

引理 2[1] n 阶循环环 $R = \langle a\rangle$ 有且仅有 $T(n)$ 个子环, 并且其中有 $2^{\psi(n)-\psi(k,n)}$ 个是有单位元的. 其中 $T(n)$ 为正整数 n 的正因数个数, $a^2 = ka$, $\psi(n)$ 是 n 的不同素因子的个数, $\psi(k, n)$ 是 k 与 n 的最大公因数的不同素因子的个数.

特别, 有单位元的 n 阶循环环的每个子环都有单位元 $\Leftrightarrow$ 对任意素数 p, 都有 $p^2 \nmid n$.

引理 3 n 阶循环环 R 是域的充分与必要条件是, n 为素数且 R 不是零乘环.

证明 设 $R = \langle a\rangle = \{0, a, 2a, \cdots, (n-1)a\}$, 且

$$|a| = n, \quad a^2 = ka, \quad 0 \leq k < n.$$

如果 R 是域, 则 R 当然不能是零乘环; 又若 n 为合数, 令

$$n = n_1n_2, \quad 1 \leq n_i < n, \quad i = 1, 2$$

则 $n_1a \neq 0$, $n_2a \neq 0$, 但是 $n_1a \cdot n_2a = na^2 = 0$, 这同 R 是域矛盾, 故 n 必为素数.

反之, 如果 R 不是零乘环且 $n = p$ 是素数, 则 $k \neq 0$. 这样, 若

$$sa \cdot ta = sta^2 = stka = 0,$$

则 $p \mid stk$. 但 $(p, k) = 1$, 故 $p \mid st$. 从而 $p \mid s$ 或 $p \mid t$, 亦即 $sa = 0$ 或 $ta = 0$. 即 R 无零因子, 因此 R 是域.

引理 4 设 R 是一个阶大于 1 的环. 则 R 只有平凡子环的充分与必要条件是 $|R|$ 为素数.

证明 充分性显然, 下证必要性.

设 R 只有平凡子环, 则由[3]知, R 必为有限环. 设 $|R| = n > 1$, p 是 n 的任意一个素因数.

且 $n = pn'$, 则

$$S = \{x \mid x \in R, px = 0\}$$

是 R 的一个非零子环, 从而 $S = R$.

若 $n' > 1$, 且 n' 有异于 p 的素因数 q, 则由 sylow 定理知, R (即 S) 中有阶为 q 的元素, 但这是不可能的. 因此, n' 只能有素因数 p. 于是可设

$$n = p^k, \text{ 其中 } k > 1.$$

1) 若 R 无零因子, 则 R 为 p^k 阶域. 设 e 为其单位元, 则素域

$$S_1 = \{0, e, 2e, \cdots, (p-1)e\}$$

是 R 的非平凡子环, 这与 R 只有平凡子环矛盾.

2) 若 R 有零因子, 则在 R 中有元素 $a \neq 0, b \neq 0$, 而 $ab = 0$. 于是

$$S_2 = \{x \mid x \in R, ax = 0\}$$

是 R 的一个非零子环, 故 $S_2 = R$. 于是 $a^2 = 0$. 这样

$$S_3 = \{0, a, 2a, \cdots, (p-1)a\}$$

便是 R 的一个 p 阶零乘环, 它是 R 的一个非平凡子环, 这与 R 只有平凡子环矛盾.

因此 $n' = 1$, 即 $|R| = n = p$ 为素数.

定理 2 设 R 是阶大于 1 的有限NF-环, 则 R 为域或 $|R| = p$ 与 $|R| = p_1p_2$, 其中 p, p_1 与 p_2 均为素数.

证明 1) 若 $|R| = p_1^{k_1}p_2^{k_2}p_3^{k_3}m$, 其中 p_1, p_2, p_3 为互异素数, $k_i \geq 1$, $i = 1, 2, 3$. 则易知

$$S_1 = \{x \mid x \in R, p_1x = 0\}, \quad S_2 = \{x \mid x \in R, p_2x = 0\}$$

是 R 的两个子环且 $S_1 \cap S_2 = \{0\}$, 故有直和 $S = S_1 \oplus S_2$.

由于 R 中有阶为 p_1 和 p_2 的元素, 故 $|S| \geq p_1p_2$, 从而 $S \neq \{0\}$.

又若 $S = R$, 则在 S 中将有阶为 p_3 的元素 b, 令

$$b = b_1 + b_2, \quad b_i \in S_i, \quad i = 1, 2$$

于是

$$p_1p_2b = p_1p_2b_1 + p_1p_2b_2 = 0, \quad p_3 \mid p_1p_2.$$

这与 p_1, p_2, p_3 是互异的素数矛盾, 故 $S \neq R$.

因此, S 是 R 的一个非平凡子环.

又由于 S 有零因子, 从而 S 是 R 的一个非域真子环. 这与 R 是NF-环矛盾. 因此, R 的阶不能有三个和三个以上互异的素因数.

2) 设 $|R| = p_1^{k_1}p_2^{k_2}$, 其中 p_1 与 p_2 为互异素数, 且 $k_1 \geq 2, k_2 \geq 1$.

令 S_1, S_2 如上, 则此时同样有 $S_1 \cap S_2 = \{0\}$. 又易知 S_1 是 R 的一个非平凡子环, 从而为域. 令 F 是它的素域, 则由于 $k_1 \geq 2$ 且易知 $|S_2| \leq p_2^{k_2}$, 故

$$|F \oplus S_2| \leq p_1p_2^{k_2} < p_1^{k_1}p_2^{k_2} = |R|,$$

从而直和 $F \oplus S_2$ 是 R 的一个非域真子环. 这也与 R 是NF-环矛盾.

3) 设 $|R| = p^k$, 其中 p 是素数, 且 $k \geq 3$.

若 R 不是域, 则 R 必含有零因子, 从而在 R 中存在元素 $a \neq 0, b \neq 0$, 而 $ab = 0$. 令

$$S_i = \{na^i \mid n \in Z\}, \quad i = 1, 2, 3, \cdots,$$

则类似于定理1中的证明, 可知$S = \sum_{i=1}^{\infty} S_i$是$R$ 的一个非平凡子环, 从而为域 令F_1为它的素域, 则 $|F_1| = p$.

同理, 令$S_i' = \{nb^i \mid n \in Z\}$, $i = 1, 2, 3, \cdots$, 则$S' = \sum_{i=1}^{\infty} S_i'$也是$R$ 的一个非平凡子环, 从而也是域 令F_2为其素域, 则 $|F_2| = p$.

由于$S \cap S' = \{0\}$, 从而$F_1 \cap F_2 = \{0\}$. 由于 $|R| = p^k$, 而$k \geq 3$, 故$F_1 \oplus F_2$是R 的一个阶为p^2 的非域真子环. 这与R 是NF-环矛盾. 因此, R 必为域

综上所述, 阶大于 1 的有限NF-环只能是域, 或 $|R| = p$ 与 $|R| = p_1 p_2$. □

本文开头已指出, 凡有限域必为NF-环; 又一阶和素阶环也是NF-环, 而且由引理4知, 这是仅有的无真子环的NF-环. 下面将进一步考虑, 阶为二素数之积的环是NF-环的条件:

定理3 设R 是环, 且 $|R| = n = p_1 p_2$, 其中p_1与p_2是互异素数 则R 是NF-环的充分与必要条件是R 有单位元

证明 由于 $|R| = p_1 p_2$, 故由 sylow 定理知, R 中有阶为p_1和p_2的元素; 又由于p_1与p_2是互异素数, 故R 中有阶为$p_1 p_2$的元素 设a 是这样的一个元素, 则由[1]知, $R = \langle a \rangle$是由a生成的$p_1 p_2$阶循环环.

1) 若R 有单位元, 则由引理 1 与引理 2 知, R 有$T(p_1 p_2) = 4$个子环, 且这 4 个子环都是有单位元的循环环, 其阶分别为 $1, p_1, p_2$和$p_1 p_2$. 除去平凡子环外, 其两个非平凡子环设为

$$S_i = \{0, e_i, 2e_i, \cdots, (p_i - 1)e_i\}, \quad i = 1, 2$$

其中e_i为S_i的单位元 由引理3知, S_1与S_2都是域, 从而$S_i \cong Z_{p_i}$, $i = 1, 2$ 因此, R 是NF-环.

2) 设R 为NF-环, 且$a^2 = ka$, $1 \leq k < p_1 p_2$(由于R 是NF-环, 故$k \neq 0$), 则R 必有单位元, 由[1]知, 亦即必有$(k, p_1 p_2) = 1$. 因若不然, 不妨设$k = p_1$, 则$\psi(n) = 2$, $\psi(k, n) = 1$, 于是由引理 2 知, R 有

$$2^{\psi(n) - \psi(k, n)} = 2^{2-1} = 2$$

个子环有单位元 但R 共有4个子环, 从而R 有非平凡子环无单位元, 当然就不是域 这与R 是NF-环矛盾, 因此R 必有单位元 □

由此定理的证明, 易得

推论 若R 是$p_1 p_2$阶NF-环, 其中p_1与p_2是互异素数, 则R 为二子域S_1与S_2的直和, 且

$$R = S_1 \oplus S_2 \cong Z_{p_1} \oplus Z_{p_2} \cong Z_{p_1 p_2}.$$

定理4 设R 是一个p^2阶环, p 是一个素数 则R 为NF-环的充分与必要条件是, R 为域或$R \cong Z_p \oplus Z_p$.

证明 充分性是显然的, 下证必要性.

设R 为NF-环, 则首先R 中不能有p^2阶元素 因若不然, 设$a \in R$ 且 $|a| = p^2$, 则

$$\langle pa \rangle = \{0, pa, 2pa, \cdots, (p - 1)pa\}$$

是R 的一个p 阶子环, 而且是一个零乘环. 这与R 是NF-环矛盾. 因此, R 中所有非零元素的阶均为p.

如果R 不是域, 则R 必有零因子. 因此在R 中存在元素$a \neq 0, b \neq 0$ 使$ab = 0$. 于是 $|a|$

$= |b| = p$. 令

$$S_1 = \langle a \rangle = \{0, a, 2a, \cdots, (p-1)a\},\ S_2 = \langle b \rangle = \{0, b, 2b, \cdots, (p-1)b\}.$$

若 $a^2 = 0$, 则 S_1 是 p 阶零乘环, 从而是 R 的一个非域真子环, 这与 R 是NF-环矛盾, 故 $a^2 \neq 0$. 从而 $|a^2| = p$. 这样, 若 $x \in S_1 \cap S_2$, 令

$$x = sa = tb, \quad 0 \leq s < p, 0 \leq t < p,$$

则

$$a(sa) = a(tb),\ sa^2 = t(ab) = 0.$$

于是 $p \mid s, s = 0$. 从而 $x = 0, S_1 \cap S_2 = \{0\}$. 这样一来, R 与 S_1 和 S_2, 作为加群和子加群, 有

$$R = S_1 \oplus S_2.$$

由于 $a^2 \in R$, 故可令

$$a^2 = k_1 a + k_2 b, \quad 0 \leq k_i < p,$$

于是 $a^2 b = k_1 ab + k_2 b^2, k_2 b^2 = 0$. 同上理, $b^2 \neq 0$, 从而 $|b^2| = p$. 于是 $p \mid k_2, k_2 = 0$. 因此

$$a^2 = k_1 a \in S_1, \quad 1 \leq k_1 < p.$$

这就是说, S_1 是 R 的一个子环, 而且是一个 p 阶子环. 但由于 R 是NF-环, 故 S_1 为 p 阶域且 $S_1 \cong Z_p$.

同理, S_2 也是 R 的 p 阶子域且 $S_2 \cong Z_p$. 于是, 作为环, 有

$$R = S_1 \oplus S_2 \cong Z_p \oplus Z_p.$$

这样, 定理 2, 3, 4 就完全弄清楚了有限NF-环的构造. 至于无限NF-环, 需要进一步研究的是, 不知道是否存在这样的环. 当然, 由定理 1 知, 这种环如果存在的话, 必须是不含零因子的.

参 考 文 献

[1] 杨子胥, 关于循环环及其幂等元, 数学的实践与认识, 3(1985), 73-76.

[2] 杨子胥, 循环环的幂零根, 数学季刊, 2(1988),

[3] R. Gilmer, *A note on rings with only finitely many subrings*, Scripte Math., 29(1973), 37-38.

[4] N. Jacobson, *Structure of Rings*, AMS, 1956.

On the Structure of NF-Rings

Yang Zixu *Hao Xiumei*

(Dept. of Math., Shandong Finance Institute, Jinan 250014)

Abstract

An associative ring R is called a NF-Ring, if R has no non-trivial subring or all the non-trivial subrings are fields. In this paper, we discuss the properties of NF-Rings, and then the structure of finite NF-Rings.

Keywords NF-ring, cyclic ring.