

多项式环的算术性质^{*}

王航平

(中国计量学院数学系, 浙江 杭州 310018)

摘要: 通过对整系数多项式环的由二次首一整系数不可约多项式生成的理想的研究, 找出系数的关系使得相应的剩余类环为惟一分解环, 或者是主理想整环, 或者是欧氏整环的条件. 由此可得到一些是主理想整环但不是欧氏整环的例子.

关键词: 惟一分解环; 主理想整环; 欧氏整环

中图分类号: O153.3 **文献标识码:** A **文章编号:** 0529-6579 (2005) 01-0025-04

固定 $m, n \in \mathbb{Z}$, 并满足 $\Delta = m^2 - 4n < 0$, 设 $(x^2 + mx + n)$ 表示由不可约多项式 $x^2 + mx + n$ 生成的理想. 设 α_1, α_2 为 $x^2 + mx + n$ 的两个共轭复根, 则

$$Z[\alpha_i] = \{a + b\alpha_i \in \mid a, b \in \mathbb{Z}\}, i = 1, 2$$

且环 $\frac{Z[x]}{x^2 + mx + n}$ 是含么交换诺特整环. 同时环 $R = \frac{Z[x]}{x^2 + mx + n}$, 同构于 $Z[\pm\alpha_i], i = 1, 2$.

引理 1 设环 $R = \frac{Z[x]}{x^2 + mx + n}$

(1) 如 m 为偶数, 则环 R 同构于

$$\frac{Z[x]}{x^2 + (m/2)x + n}$$

$$\frac{Z[x]}{x^2 + x + n - (m-1)^2/4 - (m-1)/2}$$

由 $m^2 - 4n < 0$, 则 $n - (m/2)^2$ 和 $n - (m-1)^2/4 - (m-1)/2$ 均大于 0. 由引理 1, 只须研究型如

$$\frac{Z[x]}{x^2 + q} \text{ 与 } \frac{Z[x]}{x^2 + x + q}, q \in \mathbb{N} \text{ 的环. 而它们分别同构}$$

于 $Z[\sqrt{qi}]$ 和 $Z\left[\frac{1 + \sqrt{4q-1}i}{2}\right]$. 本文中设 $\alpha_1 = \sqrt{qi}, \alpha_2 = \frac{1 + \sqrt{4q-1}i}{2}, R = Z[\alpha_1] \text{ 或 } Z[\alpha_2]$.

引理 2 设 $r, r', s_1, s_2 \in R, r$ 为 R 中不可约元. 如果 $rr' = s_1 s_2$ 且 $s_1/r, s_2/r \notin R$, 则 R 不是惟一分解环.

定义 1 设 $\alpha \in C, a, b \in \mathbb{Z}$, 定义 α 的范数为

$$N(\alpha) = \alpha\bar{\alpha} = |a + b\alpha|^2$$

显然 $\alpha = 0 \Leftrightarrow N(\alpha) = 0$;

$$N(\alpha\beta) = N(\alpha)N(\beta), \forall \alpha, \beta \in C$$

且

$$N(a + b\alpha_1) = a^2 + qb^2 \quad (1)$$

$$N(a + b\alpha_2) = a^2 + ab + qb^2 =$$

$$\begin{cases} (a-b)^2 + 3ab + qb^2 & \text{当 } ab \geq 0 \text{ 时} \\ (a+b)^2 - ab + qb^2 & \text{当 } ab < 0 \text{ 时} \end{cases} \quad (2)$$

引理 3 设 $\alpha \in R$,

(1) α 为 R 的可逆元 $\Leftrightarrow N(\alpha) = 1$;

(2) $q > 1$ 如, 则 α 为 R 的可逆元 $\Leftrightarrow \alpha = \pm 1$;

(3) 如 $q = 1$, 则 $Z[\alpha_1]$ 中可逆元为 $\pm 1, \pm\alpha_1 = \pm i$; $Z[\alpha_2]$ 中可逆元为 $\pm 1, \pm\alpha_2 = \pm \frac{1 + \sqrt{3}i}{2}$.

引理 4 设 $q > 2, p$ 为一小于 q 的素数, 则 p 为 R 中的不可约元.

证明 如果 $p = \alpha\beta$, 其中 $\alpha, \beta \in R$ 都不是可逆元, 则

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$$

但 $N(\alpha), N(\beta) \neq 1$, 故 $N(\alpha) = p$. 设 $\alpha = a + b\alpha_i, i = 1, 2$, 由公式(1)知, 如果 $b > 0$, 则 $N(\alpha) \geq q > p$, 于是 $b = 0$, 有 $N(\alpha) = a^2 = p$, 矛盾.

1 环 $R = Z[\sqrt{qi}]$ 和

$R = Z[(1 + \sqrt{4q-1}i)/2]$ 的性质

定理 1 当 $q > 2$ 时 $R = Z[\sqrt{qi}] (q \in \mathbb{N})$ 不是惟一分解环.

证明 由引理 4 知 2 是不可约元, 我们只须证明 2 不是 R 中的素元即可. 应用引理 2: 如果 q 是奇数, 则

* 收稿日期: 2004-08-30

基金项目: 浙江省教育厅科研基金资助项目 (20040365)

作者简介: 王航平 (1959年生), 男, 副教授; E-mail: wanghp@cjl.edu.cn

$$(1 + \sqrt{qi})(1 - \sqrt{qi}) = 1 + q = 2d$$

其中, $d \in N$, 但 $(1 + \sqrt{qi})/2, (1 - \sqrt{qi})/2 \notin R$, 故 2 不是素元, 如果 q 是偶数, 则 $\sqrt{qi}(1 - \sqrt{qi}) = q = 2d$, 其中 $d \in N$, 但 $\sqrt{qi}/2, -\sqrt{qi}/2 \notin R$, 故 2 也不是素元。

定理 2 当 $q = 1, 2$ 时, 环 $R = Z[\sqrt{qi}]$ 为欧氏整环。

证明 将证明范函数 $N: R^* \rightarrow N$ 是 R 的一个欧氏函数。如 $r, r' \in R$, 使得 $r \mid r'$, 则存在 $s \in R$ 使得 $r' = rs$, 我们有 $N(r') = N(r)N(s)$ 。于是 $N(r') \geq N(r)$, 设 $r, r' \in R$, 令 $r'/r = u + v\sqrt{qi} \in C$, 其中 $u, v \in R$, 我们总能取 $u', v' \in Z$, 使得,

$$|u - u'| \leq 1/2, |v - v'| \leq 1/2$$

令 $s = u' + v'\sqrt{qi}, t = r' - rs$, 显然 $s, t \in R$, 且

$$N(t) = N(r)N((u - u') + (v - v')\sqrt{qi}) =$$

$$N(r)((u - u')^2 + q(v - v')^2) \leq$$

$$N(r)(1/4 + q/4) \leq 3/4N(r) < N(r)$$

所以结论正确。

定理 3 如果 q 是合数, 则

$$R = Z[(1 + \sqrt{4q-1}i)/2] \quad (q > 0)$$

不是惟一分解整环。

定理 4 当 $q = 1, 2, 3$ 时, 环

$$R = Z[(1 + \sqrt{4q-1}i)/2] \quad (q > 0)$$

为欧氏整环。

证明 证明方法与定理 2 的相似。

设 A 是一个非零含么交换整环, S 是 A^* 的一个子集, 定义 S' 为集合

$$S' = \{\alpha \in S \mid \text{存在 } \beta \in A^* \text{ 使得 } \beta + \alpha A \subset S\}$$

对于任意自然数 i , 递归地定义

$$S^1 = S, S^{i+1} = (S^i)'$$

易知如 T 是 A^* 的另一子集且 $S \subset T$, 则 $S' \subset T'$ 。

设 A 是欧氏整环, ϕ 是 A 的一个欧氏函数。对于任意自然数 i , 定义,

$$P_i = \{\alpha \in A^* \mid \phi(\alpha) \geq i\}$$

据欧氏整环和欧氏函数的定义, 如果 $\alpha \in A^*, \beta \in P_i$, 则 $\alpha\beta \in P_i$ 。序列 (S^i) 和 (P^i) 都随 i 的递增而递减, 且 $\bigcap_{i=1}^\infty P_i = \Phi$ 。记 $(P_i)' = P_i'$ 。

引理 5

(1) 如 A 是欧氏整环, 则 $P_i' \subset P_{i+1}, (A^*)^i \subset P_i$;

(2) $(A^*)' \neq \Phi$ 且 $(A^*)' = (A^*)^2$, 则 A 不是欧氏整环。

引理 6 设

$$R = Z[(1 + \sqrt{4q-1}i)/2] \quad (q > 3)$$

当 $q > 3$ 时,

$$(R^*)' = R \setminus \{-1, 0, 1\} \neq \Phi, (R^*)' = (R^*)^2$$

现在考虑 q 是大于 3 的素数情形。定义函数

$$T(q) = \begin{cases} \sqrt{(16q-4)/3} & \text{如果 } q > 5 \\ q-1 & \text{如果 } q = 5 \end{cases}$$

注意到当 $q \geq 7$ 时 $\sqrt{(16q-4)/3} < q$ 于是对所有大于 3 的素数 q 满足 $T(q) < q$ 。

定义 2 设 q 为大于 3 的素数, 称 q 是衍素数, 如果对 Z 中的任意元 a, b , 使得 $(a, b) = 1$, 且 $0 < a, b \leq T(q)$, 所有

$$N\left[a + b \frac{1 + \sqrt{4q-1}i}{2}\right] = a^2 + ab + qb^2$$

的素因子都大于等于 q 。

例 5 是一个衍素数。

引理 7 如果 q 是一个衍素数, $a, b, c \in Z$ 满足

$$(a, b, c) = 1, 1 < |c| \leq T(q)$$

那么在 Z 中 c 不整除 $a^2 + ab + qb^2$ 。

证明 首先令 $a', b' \in Z$ 为惟一一对满足

$$a' \equiv a \pmod{c},$$

$$b' \equiv b \pmod{c}, 0 < a', b' \leq |c|$$

的整数。显然 $(a', b', c) = 1$, 且 $c \mid a'^2 + a'b' + qb'^2$, 当且仅当 $c \mid a^2 + ab + qb^2$, 于是可以简单地只对引理证明 $0 < a, b \leq |c| \leq T(q)$ 的情形。令 $\theta = (a, b) = 1$, 则 $(a/\theta, b/\theta) = 1$ 且 $0 < a/\theta, b/\theta \leq T(q)$ 。令

$$\alpha = \frac{a}{\theta} + \frac{b}{\theta} \frac{1 + \sqrt{4q-1}i}{2} \in R$$

据衍素数的定义,

$$N(\alpha) = \frac{a^2 + ab + qb^2}{\theta^2}$$

没有小于 q 的素因子。令 q 为 c 的一个素因子, 有 $p \leq |c| \leq T(q) < q$ 。如果 $c \mid a^2 + ab + qb^2$ 则

$$p \mid a^2 + ab + qb^2 = N(\alpha)\theta^2$$

由于 $N(\alpha)$ 没有小于 q 的素因子, p 不整除 $N(\alpha)$ 。所以 $p \mid \theta^2$, 故 $p \mid \theta$ 。于是 p 也是 a, b 的公因子, 这与 $(a, b, c) = 1$ 矛盾。

引理 8 设环 R 满足以下条件: 对任意 $r, r' \in R^*$ 使得 $N(r) \leq N(r')$, 或者 $r \mid r'$, 或者存在 $s, t \in R$, 使得 $0 < N(r's - rt) < N(r)$, 则 R 是主理想整环。

证明 设 I 是 R 的理想, 记 $I^* = I \setminus \{0\}$ 。固定 I^* 中元素 r 满足条件 $N(r)$ 极小。设 $r' \in I^*$, 那么如果 r 不整除 r' , 由假设知存在 $s, t \in R$, 使得 $u = r's - rt$ 满足 $0 < N(u) < N(r)$ 。但这与 $N(r)$ 的极小的假定矛盾, 因为 $u \in I^*$ 。于是 $r \mid r'$, I 由 r 生成。

下面我们给出本文二个主要定理:

定理5 设 $q > 3$, 则

$$R = Z[(1 + \sqrt{4q-1}i)/2]$$

不是欧氏整环。

证明 由引理5、6即得。

定理6 设 q 为大于3的素数,

$$R = Z[(1 + \sqrt{4q-1}i)/2]$$

(1) 如果 q 不是衍素数, 那么 R 不是惟一分解整环。

(2) 如果 q 是衍素数, 那么 R 是主理想环。

证明

(1) 由 q 不是衍素数, 那么存在一对整数 a, b , 满足 $(a, b) = 1, 0 < a, b \leq T(q)$, 使得 $a^2 + ab + qb^2 = pp'$ 其中 p 是一个小于 q 的素数。据引理4, 在 R 中 p 是不可约元。我们将证明它不是素元。令

$$\alpha = a + b \frac{\sqrt{4q-1}i}{2} \in R$$

则

$$\bar{\alpha} = a + b + (-b) \frac{1 + \sqrt{4q-1}i}{2} \in R$$

且

$$N(\alpha) = \alpha\bar{\alpha} = a^2 + ab + qb^2 = pp'$$

但

$$\frac{a}{p} = \frac{a}{p} + \frac{b}{p} \frac{1 + \sqrt{4q-1}i}{2} \in R$$

当且仅当同时整除 a 和 b , 这与 $(a, b) = 1$ 矛盾。同样的结论对于 $\bar{\alpha}/p$ 也成立。据引理2, p 不是素元。所以, R 不是惟一分解环。

(2) p 是衍素数。设 $r, r' \in R$, 且 $N(r) \leq N(r')$, r 不整除 r' 。据引理8, 只须找到 $s, t \in R$ 使得 $0 < N(r's - rt) < N(r)$, 亦即 $0 < N(r's/r - t) < 1$, 易知 r'/r 总可以被写作

$$\frac{r'}{r} = \frac{d + e \sqrt{4q-1}i}{c} \quad (3)$$

(总可设 $c > 0$ 的形式, 其中 $c, d, e \in Z, (c, d, e) = 1$ 。)

令 $u, v, w \in Z$ 为满足 $cu + dv + ew = 1$ 的整数。

分两种情况考虑: $|c| > T(q)$ 和 $|c| \leq T(q)$:

(a) 设 $|c| > T(q)$ 。先不考虑 $q = 5$ 且 $c = 5$ 的情况, 易知此时 $4q - 1 < 3c^2/4$ 。设

$$dw + ev(4q - 1) = kc + \epsilon \quad (4)$$

其中 $k, \epsilon \in Z, |\epsilon| \leq c/2$ 。取

$$s = w + v \sqrt{4q-1}i =$$

$$(w - v) + (2v) \frac{1 + \sqrt{4q-1}i}{2} \in R$$

$$\frac{r's}{r} = (k - u \sqrt{4q-1}i) + \frac{\epsilon + \sqrt{4q-1}i}{c}$$

取 $t = k - u \sqrt{4q-1}i$

$$\frac{r's}{r} - t = \frac{\epsilon + \sqrt{4q-1}i}{c} =$$

$$(k + u) + (-2u) \frac{1 + \sqrt{4q-1}i}{2} \in R,$$

$$N\left(\frac{r's}{r} - t\right) = N\left(\frac{\epsilon + \sqrt{4q-1}i}{c}\right) = \frac{4q - 1 + \epsilon^2}{c^2}$$

有

$$0 < \frac{4q - 1 + \epsilon^2}{c^2} < \frac{3c^2/4 + c^2/4}{c^2} = 1 \quad (5)$$

再考虑 $q = 5$ 且 $c = 5$ 的情形。所有的步骤都和上面的一样。只是在(4)中 ϵ 可取 $|\epsilon| \leq 2$ (而非(4)中较为粗糙的 $|\epsilon| \leq c/2$)。于是(5)中估计为

$$0 < \frac{4q - 1 + \epsilon^2}{c^2} \leq \frac{23}{25} < 1$$

(b) 设 $|c| \leq T(q)$ 。我们把公式(3)改写一下。令

$$\begin{aligned} d' &= d - e, e' = 2e \\ \frac{r'}{r} &= \frac{d' + e'(1 + \sqrt{4q-1}i)/2}{c} \end{aligned}$$

由 $cu + dv + ew = 1$ 知

$$c(2u) + d'(2v) + e'(w + v) = 2$$

于是 (c, d', e') 至多为2。如 $(c, d', e') = 1$, 那么 $c > 1$, 否则这意味着 $r \mid r'$ 。记

$$\alpha = d + e \sqrt{4q-1}i =$$

$$d' + e' \frac{1 + \sqrt{4q-1}i}{2} \in R$$

由引理7知 c 不整除

$$N(\alpha) = d'^2 + d'e' + qe'^2 = d^2 + (4q - 1)e^2$$

于是令

$$N(\alpha) = d^2 + (4q - 1)e^2 = kc + \epsilon$$

其中 $k, \epsilon \in Z, 0 < \epsilon < c$ 。我们取

$$s = \bar{\alpha} \in R, t = k \in R, r's/r - t = \epsilon/c。$$

$$0 < N(\epsilon/c) = \epsilon^2/c^2 < 1$$

如 $(c, d', e') = 2$, 进一步令 $d'' = d'/2, e'' = e'/2$ 。我们有

$$(c, d'', e'') = 1,$$

$$r'/r = [d'' + e''(1 + \sqrt{4q-1}i)/2]/c'$$

于是 $c' > 1$, 否则这意味着 $r \mid r'$ 。记

$$\alpha = d'' + e''(1 + \sqrt{4q-1}i)/2 \in R$$

由引理 7 知, c 不整除

$$N(\alpha) = d''^2 + d''e'' + qe''^2$$

于是令 $N(\alpha) = kc' + \epsilon$, 其中 $k, \epsilon \in \mathbb{Z}, 0 < \epsilon < c'$.

我们取

$$s = \bar{\alpha} \in R, t = k \in R,$$

$$r's/r - t = \epsilon/c',$$

$$0 < N(\epsilon/c')(\epsilon^2/c'^2) < 1$$

由引理 8 知, 定理得证。

注 一个很自然的问题是: 衍素数到底有多少? 我们用计算机对一百万以内的素数进行验算, 发现只有 5, 11, 17, 41 共 4 个衍素数 (猜想这 4 个素数也就是所有的衍素数)。所以, $\mathbb{Z}[(1 + \sqrt{19}i)/2], \mathbb{Z}[(1 + \sqrt{43}i)/2], \mathbb{Z}[(1 + \sqrt{67}i)/2], \mathbb{Z}[(1 + \sqrt{63}i)/2]$ 都是主理想整环, 但不是欧氏整环的例子。

2 结 论

总结引理 1 及定理 1, 2, 3, 4, 5, 6, 有

定理 7 令 $m, n \in \mathbb{Z}$ 满足 $\Delta = m^2 - 4n < 0$, 令环

$$R = \frac{\mathbb{Z}[x]}{x^2 + mx + n}$$

(1) 如为偶数, 令 $q = n - (m/2)^2$, 则

- (a) 当 $q=1, 2$ 时环 R 为欧氏整环;
- (b) 当 $q>2$ 时, 环 R 不是惟一分解整环。
- (2) 如 m 为奇数, 令 $q = n - (m-1)^2/4$ 则
 - (a) 当 $q=1, 2, 3$ 时, 环 R 是欧氏整环;
 - (b) 当 q 不是衍素数或 q 是合数时, 则 R 不是惟一分解整环;
 - (c) 当 q 是衍素数时, 环 R 是主理想整环但不是欧氏整环。

参考文献:

[1] KAC G I. Certain arithmetic properties of ring groups[J] . Funkcional Anal i Prilo V zen, 1972, 6(2): 88—90.
[2] KLAZAR MARTIN, LUCA FLORIAN. On Some arithmetic properties of polynomial expressions involving striting numbers of the second kind[J] . Acta Arith, 2003, 107(4): 357—372.
[3] 王芳贵. 环与环上的模[J] . 四川大学学报, 2002, 25(6): 557—562.
[4] 刘卫江. 多项式代数与半群代数中的 Groebner-基的关系[J] . 数学杂志, 2002, 22(4): 464—468.
[5] NATHAN J. Basic algebra[M] . San Francisco: W H Freeman and Company, 1974.
[6] HUGERFORD T W. Algebra[M] . New York: Springer, 1980.

The Arithmetic Property of Polynomial Rings

WANG Hang ping

(Department of Mathematics, China Jiliang University, Hangzhou 310018, China)

Abstract: Based on the ideal research on integral coefficient polynomial rings generated by irreducible quadratic with first coefficient one integral coefficient polynomials, the coefficient relationship is determined so that the corresponding surplus ring becomes the condition for the unique factorization domain, the Euclidean ring. Hence, examples of principal ideal domain not Euclidean domain are obtained.

Key words: unique factorization domain; euclidean domain; principal ideal domain