第五节　因式分解定理

主要内容

- 引入
- 不可约多项式
- 因式分解及唯一性定理

一、引入☜

$$x^4-4=(x^2-2)(x^2+2) \qquad on\ Q$$

$$=(x-\sqrt{2})(x+\sqrt{2})(x^2+2) \qquad on\ \ R$$

$$=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}i)(x+\sqrt{2}i) \qquad on\ \ C$$

二、不可约多项式

在下面的讨论中，仍然选定一个数域 P 作为系数域，我们考虑数域 P 上的多项式环 $P[x]$ 中多项式的因式分解.

1. 定义

定义 8 数域 P 上次数 ≥ 1 的多项式 $p(x)$ 称为域 P 上的**不可约多项式**，如果它不能表成数域 P 上两个次数比 $p(x)$ 的次数低的多项式的乘积.

按照定义，一次多项式总是不可约多项式.

多项式是否可约和所选的数域有关。如(x^2-2)在有理数域上不可约，但在$Q(\sqrt{2})$和实数域可约。

又如，x^2+2是实数域上的不可约多项式，但是它在复数域上可以分解成两个一次多项式的乘积，因而不是不可约的. 这就说明了，一个多项式是否不可约是依赖于系数域的.

显然，不可约多项式$p(x)$的因式只有非零常数与它自身的非零常数倍$cp(x)$ $(c\neq 0)$这两种，此

外就没有了．反过来，具有这个性质的次数 ≥ 1 的多项式一定是不可约的．由此可知，不可约多项式 $p(x)$ 与任一多项式 $f(x)$ 之间只可能有两种关系，或者 $p(x) \mid f(x)$ 或者 $(p(x), f(x)) = 1$．事实上，如果 $(p(x), f(x)) = d(x)$，那么 $d(x)$ 或者是 1 或者是 $cp(x)\ (c \neq 0)$．当 $d(x) = cp(x)$ 时，就有 $p(x) \mid f(x)$．

不可约多项式有下述的重要性质.

定理 4 如果 $(f(x), g(x)) = 1$，且 $f(x) \mid g(x)h(x)$，那么 $f(x) \mid h(x)$.

2. 性质

定理 5 如果 $p(x)$ 是不可约多项式，那么对于任意的两个多项式 $f(x), g(x)$，由 $p(x) \mid f(x)g(x)$ 一定推出 $p(x) \mid f(x)$ 或者 $p(x) \mid g(x)$.

证明 如果 $p(x) \mid f(x)$，那么结论已经成立.

如果 $p(x) \nmid f(x)$，那么由以上的说明可知

$$(p(x), f(x)) = 1 .$$

于是由 **定理 4** 即得 $p(x) \mid g(x)$.

证毕

利用数学归纳法，这个定理可以推广为：如果不可约多项式 $p(x)$ 整除一些多项式 $f_1(x)$, $f_2(x)$, … , $f_s(x)$ 的乘积 $f_1(x)\,f_2(x)\ldots f_s(x)$ ，那么 $p(x)$ 一定整除这些多项式之中的一个.

下面来证明这一章的主要定理.

三、因式分解及唯一性定理

因式分解及唯一性定理 数域 P 上每一个次数 ≥ 1 的多项式 $f(x)$ 都可以唯一地分解成数域 P 上一些不可约多项式的乘积. 所谓唯一性是说，如果有两个分解式

$$f(x) = p_1(x)\, p_2(x) \dots p_s(x) = q_1(x)\, q_2(x) \dots q_t(x),$$

那么必有 $s = t$，并且适当排列因式的次序后有

$$p_i(x) = c_i\, q_i(x),\quad i = 1, 2, \dots, s,$$

其中 c_i $(i = 1, 2, \dots, s)$ 是一些非零常数.

证明 先证分解式的存在性. 我们对 $f(x)$ 的次数作归纳法.

因为一次多项式都是不可约的，所以 $n = 1$ 时结论成立.

设 $\partial(f(x)) = n$, 并设结论对于次数低于 n 的多项式已经成立.

如果 $f(x)$ 是不可约多项式，结论是显然的, 不妨设 $f(x)$ 不是不可约的，即有

$$f(x) = f_1(x)\, f_2(x) ,$$

其中 $f_1(x)$， $f_2(x)$ 的次数都低于 n . 由归纳法假设 $f_1(x)$ 和 $f_2(x)$ 都可以分解成数域 P 上一些不可约多项式的乘积. 把 $f_1(x)$， $f_2(x)$ 的分解式合起来就得到 $f(x)$ 的一个分解式.

由归纳法原理，结论普遍成立.

再证唯一性. 设 $f(x)$ 可以分解成不可约多项式的乘积

$$f(x) = p_1(x)\, p_2(x) \ldots p_s(x)\ .$$

如果 $f(x)$ 还有另一个分解式

$$f(x) = q_1(x)\, q_2(x) \,\ldots\, q_t(x)\,,$$

其中 $q_i(x)$ ($i = 1, 2, \ldots, t$) 都是不可约多项式, 于是

$$f(x) = p_1(x)\, p_2(x) \,\ldots\, p_s(x) = q_1(x)\, q_2(x) \,\ldots\, q_t(x)\,. \quad (1)$$

我们对 s 作归纳法. 当 $s = 1$， $f(x)$ 是不可约多项式，由定义必有

$$s = t = 1\,,$$

且

$$f(x) = p_1(x) = q_1(x)\,.$$

现在设不可约因式的个数为 $s-1$ 时唯一性已证.

由

$$f(x) = p_1(x)\, p_2(x) \ldots p_s(x) = q_1(x)\, q_2(x) \ldots q_t(x)$$

得

$$p_1(x) \mid q_1(x)\, q_2(x) \ldots q_t(x),$$

因此，$p_1(x)$ 必能除尽其中的一个，无妨设

$$p_1(x) \mid q_1(x).$$

因为 $q_1(x)$ 也是不可约多项式，所以有

$$p_1(x) = c_1 q_1(x), \tag{2}$$

由 $p_1(x)\,p_2(x)\,\ldots\,p_s(x) = q_1(x)\,q_2(x)\,\ldots\,q_t(x)$ 得

$$p_1(x) = c_1 q_1(x)$$

$$p_2(x)\,\ldots\,p_s(x) = c_1^{-1} q_2(x)\,\ldots\,q_t(x)\,.$$

由归纳法假定，有

$$s - 1 = t - 1\,,\ \text{即}\ s = t\,, \tag{3}$$

并且适当排列次序之后有

$$p_2(x) = c_2' c_1^{-1} q_2(x)\,,\ \text{即}\ p_2(x) = c_2 q_2(x)\,,$$

$$p_i(x) = c_i q_i(x)\ \ (\,i = 3, \ldots, s\,)\,. \tag{4}$$

(2) , (3) , (4) 合起来就是所要证的结论. 证毕

应该指出，因式分解定理虽然在理论上有其基本重要性，但是它并没有给出一个具体的分解多项式的方法．实际上，对于一般的情形，普遍可行的分解多项式的方法是不存在的．

在多项式 $f(x)$ 的分解中，可以把每一个不可约因式的首项系数提出来，使它们成为首项系数为 1 的多项式，再把相同的不可约因式合并．于是 $f(x)$ 的分解式为

$$f(x)=cp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x),$$

其中 c 是 $f(x)$ 的首项系数， $p_1(x), p_2(x), \ldots, p_s(x)$ 是不同的首项系数为 1 的不可约多项式，而 $r_1, r_2, \ldots, r_s$ 是正整数. 这种分解式称为**标准分解式**.

如果已经有了两个多项式的标准分解式，我们就可以直接写出两个多项式的最大公因式. 多项式 $f(x)$ 与 $g(x)$ 的最大公因式 $d(x)$ 就是那些同时在 $f(x)$ 与 $g(x)$ 的标准分解式中出现的不可约多项式方幂

的乘积，所带的方幂的指数等于它在 $f(x)$ 与 $g(x)$ 中所带的方幂中的较小的一个.

推论 设 $p_1(x), p_2(x), \cdots, p_s(x)$ 是数域 P 上的首项系数为 1 的不可约多项式。$f(x)$ 和 $g(x)$ 有标准分解式

$$f(x) = ap_1^{\lambda_1}(x)p_2^{\lambda_2}(x)\cdots p_s^{\lambda_s}(x)$$

$$g(x) = bp_1^{\mu_1}(x)p_2^{\mu_2}(x)\cdots p_s^{\mu_s}(x)$$

其中 a, b 是 P 中的数，$\lambda_i \geq 0, \mu_i \geq 0\ (i = 1, 2, \cdots, s)$，则有

$$(f(x), g(x)) = p_1^{\min(\lambda_1, \mu_1)}(x)p_2^{\min(\lambda_2, \mu_2)}(x)\cdots p_s^{\min(\lambda_s, \mu_s)}(x)$$

$$[f(x), g(x)] = p_1^{\max(\lambda_1, \mu_1)}(x)p_2^{\max(\lambda_2, \mu_2)}(x)\cdots p_s^{\max(\lambda_s, \mu_s)}(x)$$

例 设

$$f(x)=x^2+3x+2,\ \ g(x)=x^2+4x+3$$

求$(f(x),g(x))$和$[f(x),g(x)]$。

解 求得

$$f(x)=(x+1)(x+2),\ \ g(x)=(x+1)(x+3)$$

所以

$$(f(x),g(x))=x+1$$

$$[f(x),g(x)]=(x+1)(x+2)(x+3)$$

练习 设

$$f(x)=x^3-x,\ \ g(x)=x^4+2x^3+x^2$$

求$(f(x),g(x))$和$[f(x),g(x)]$。

解 求得

$$f(x)=x(x+1)(x-1),\ \ g(x)=x^2(x+1)^2$$

所以

$$(f(x),g(x))=x(x+1)$$

$$[f(x),g(x)]=x^2(x+1)^2(x-1).$$

由以上讨论可以看出，带余除法是一元多项式因式分解理论的基础．我们知道，整数也有带余除法，即

对于任意整数 a , b, $b \neq 0$, 都存在唯一的整数 q , r , 使

$$a = qb + r ,$$

其中 $0 \leq r < | b |$.