

习题 2.2.7

叶卢庆*

杭州师范大学理学院, 浙江 杭州 310036

习题 (2.2.7). 证明 $x^d - 1$ 整除 $x^n - 1$ 当且仅当 d 整除 n .

证明. \Leftarrow : 此时, 不妨设 $n = kd$, 此时, 易得

$$x^n - 1 = (x^d)^k - 1^k = (x^d - 1)\Delta.$$

其中 Δ 是一个多项式. 因此 $x^d - 1 | x^n - 1$.

\Rightarrow : $x^d - 1 | x^n - 1$ 说明 $n \geq d$. 假若 $d \nmid n$, 则根据带余除法, 存在唯一的 q, r , 使得

$$n = qd + r,$$

其中 $0 < r < d$. 则

$$x^n - 1 = x^{qd+r} - 1.$$

而

$$x^{qd+r} - 1 = x^{qd}x^r - x^r + x^r - 1 = x^r(x^{qd} - 1) + (x^r - 1) = (x^d - 1)x^r\Delta' + (x^r - 1).$$

易得 $x^d - 1 \nmid x^r - 1$, 因此, $x^d - 1 \nmid x^n - 1$, 矛盾. 因此 $d | n$. ■

注 1. 这个结论建立了 $d | n$ 和 $x^d - 1 | x^n - 1$ 的对应关系, 个人认为会有大用.

*叶卢庆 (1992—), 男, 杭州师范大学理学院数学与应用数学专业本科在读, E-mail: h5411167@gmail.com