Notes of "Polynomials"

Jinxin Wang

1 一元多项式

Definition 1 (数域 P 上的一元多项式)**.**

Definition 2 (一元多项式相等及零多项式)**.**

Definition 3 (数域 P 上的一元多项式环)**.**

2 整除的概念

Proposition 1 (带余除法的成立)**.**

$$f(x) = q(x)g(x) + r(x) \tag{1}$$

$q(x)$ and $r(x)$ are uniquely determined. $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

Remark 1 (综合除法)**.**

Definition 4 (整除)**.**

Properties of Divisors:

- 对偶等价于相差常数倍
- 传递性
- 整除组合

3 最大公因式

Definition 5 (Common Divisor and Greatest Common Divisor)**.** *If $\phi(x)$ is a divisor of both $f(x)$ and $g(x)$, we say it is a common divisor of $f(x)$ and $g(x)$.*

Suppose $f(x) \in P[x]$ and $g(x) \in P[x]$. A polynomial $d(x) \in P[x]$ is the greatest common divisor of $f(x)$ and $g(x)$ if the following conditions are true:

- *$d(x)$ is a common divisor of $f(x)$ and $g(x)$.*
- *Every common divisor of $f(x)$ and $g(x)$ is a divisor of $d(x)$.*

Remark 2. *Since $\forall f(x) \in P[x]$ is a divisor of the zero polynomial, in other words $0 = 0 \cdot f(x)$, the greatest common divisor of $f(x)$ and 0 is 0. Especially, the greatest common divisor of 0 and 0 is 0, which is in accordance with the definition of GCD.*

Lemma 1 (Common Divisors in Euclidean Division)**.** *If it holds that* $f(x) = q(x)g(x) + r(x)$ *for* $f(x) \in P[x]$ *and* $g(x) \in P[x]$*, then the two pairs of polynomials* $(f(x), g(x))$ *and* $(g(x), r(x))$ *have the same common divisors.*

证明. □

Theorem 1 (Theorem of Polynomial Greatest Common Divisor)**.** $\forall f(x) \in P[x]$ *and* $\forall g(x) \in P[x]$*, there exists* $d(x) \in P[x]$ *that is the greatest common divisor of* $f(x)$ *and* $g(x)$*, and* $d(x)$ *can be expressed as a combination of* $f(x)$ *and* $g(x)$*, which is* $\exists u(x) \in P[x], v(x) \in P[x]$ *such that*

$$d(x) = u(x)f(x) + v(x)g(x)$$

证明. (TODO) □

Remark 3 (Euclid's Algorithm)**.**