高等代数 (II) 第一次习题课

李卓远　　数学科学学院

zy.li@stu.pku.edu.cn

1　内容概要

- 使用带余除法求得多项式的最大公因子 (系数可能不确定);
- 补充最小公倍式的定义.

2　补充知识

2.1　带余除法

在本章的学习中我们了解到类比整数集 $\mathbb{Z}$ 上的带余除法, 数域上的多项式 $\mathbb{F}[x]$ 也可以定义带余除法. 思考: 带余除法所需要的运算包括哪些? 是否只要一个集合上存在这样的运算就一定有某种 "带余除法"?

事实上, 带余除法所需的加法和乘法对应于 "环 (ring)" 的结构, 而满足某种 "带余除法" 的环一般称为 Euclid 整环, 定义如下.

Definition 2.1.1. *An integral domain R is defined as a Euclidean domain if there exists a function $\phi : R^* \to \{0, 1, \cdots\}$ such that for any $a, b \in R^*$, there exist $q, r \in R$ satisfying*

$$a = bq + r,$$

where $r = 0$ or $\phi(r) < \phi(b)$.

ϕ 衡量了 R 中元素某种意义下的大小, 使得带余除法要么恰好整除，要么满足余数 "小于" 除数.

- $\mathbb{Z}$ 为 Euclid 整环, 可取 $\phi : n \mapsto |n|$.
- $\mathbb{F}[x]$ 为 Euclid 整环, 可取 $\phi : h(x) \mapsto \deg h$.

Exercise 2.1.2. *尝试构造合适的 ϕ, 使得 $\mathbb{Z}[\sqrt{-1}] = \{a + bi | a, b \in \mathbb{Z}\}$ 满足带余除法.*

思考: 对于 $\mathbb{Z}[x]$, $\mathbb{Z}[\sqrt{-5}]$, 或是矩阵环 (全体 n 阶矩阵构成的集合), 是否也存在合适的 ϕ 使得它 (们) 满足带余除法? 在构造的过程中注意体会它们与前文 Euclid 整环结构上的差别.

2.2　最小公倍数/式的基本性质

在本小节中, 我们始终假定 $R = \mathbb{Z}$ 或 $\mathbb{F}[x]$, 可自行思考对于一般的 Euclid 整环相应结论是否成立.

Definition 2.2.1. *For $a, b \in R$, the least common multiple of a and b is given as*

$$[a, b] := \min\{c \in R | a|c, \, b|c\}.$$

Proposition 2.2.2. *For $a, b, c \in R$,*

$$a|c,\ b|c \Rightarrow [a,b]|c.$$

证明. Otherwise let $c = q[a,b] + r$ for $r \neq 0$ and $\phi(r) < \phi([a,b])$. Since both c and $[a,b]$ are common multiples of a and b, r should be common multiples of a and b, which means $r \geq [a,b]$ by the definition of $[a,b]$, and thus contradicts $\phi(r) < [a,b]$. □

Proposition 2.2.3. *The least common multiple of $a, b \in R$ satisfies*

$$[a,b](a,b) = ab.$$

证明. Since

$$\frac{ab}{(a,b)} = a\frac{b}{(a,b)} = \frac{a}{(a,b)}b,$$

$ab/(a,b)$ is a common multiple of a, b. By the previous proposition, we may assume that $k[a,b] = ab/(a,b)$ for some $k \in R$, which indicates

$$k\frac{[a,b]}{a}(a,b) = b,\ k\frac{[a,b]}{b}(a,b) = a.$$

Note that both $[a,b]/a$ and $[a,b]/b \in R$, so $k(a,b)$ is a common divisor of a and b, which implies $k(a,b)|(a,b)$. It immediately follows that $k = 1$ and $[a,b](a,b) = ab$. □

2.3 整除关系与最大公约/最小公倍数/式

不难验证整除关系都满足反身性和对称性, 即整除关系实际为 R 上的一个预序 (preorder)

- reflexivity: $a|a$ for all $a \in R$;
- transitivity: $a|b$ and $b|c$ imply $a|c$ for all $a, b, c \in R$.

对于 $R = \mathbb{Z}$ 或 $\mathbb{F}[x]$ 而言, 从序的角度看, 对任意 $a \in R$, a 的因子全体构成了 $\{a\}$ 的下界, 而 a 的倍数/式全体则构成了 $\{a\}$ 的上界. 故而 a 和 b 的最大公约数/式 $(a,b) := \inf\{a,b\}$(公共下界的最大值), 类似地可以定义 a 和 b 的最小公倍数/式 $[a,b] := \sup\{a,b\}$(公共上界的最小值). 需要强调的一点是一个集合的上/下界不一定有最小/大元, 上述定义实际上暗含了两个非平凡的事实: 最大的公共因子一定会被任何公共因子整除, 而最小的公共倍数/式一定会被整除任何公共倍数/式.

3 典型例题

Problem 3.1. *111*