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 (ED) 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 $\mathbb{Z}[\sqrt{-1}] = \{a + bi \mid a, b \in \mathbb{Z}\}$ 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*

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

其中对于 $R = \mathbb{Z}$, min 指按整数的大小关系比较所得的最小非负整数; 对于 $R = \mathbb{F}[x]$, min 指按多项式的次数比较所得的次数最小的首一多项式.

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

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

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 $\phi(r) < \phi([a, b])$. $\square$

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

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

up to a unit (an invertible element).

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 $k(a, b) \mid (a, b)$. It immediately follows that k is a unit. $\square$

2.3 整除关系序与最大公约/最小公倍数/式

对于 $R = \mathbb{Z}$ 或 $\mathbb{F}[x]$ 而言, 不难验证整除关系满足反身性和对称性, 即整除关系给出了 R 上的一个预序 (preorder)

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

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, 故而在相差至多一个单位的意义下 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). 需要强调的一点是在预序中一个集合的上/下界不一定有最小/大元, 而上述定义实际上暗含了如下两个非平凡的事实:

Proposition 2.3.1. *对于 $R = \mathbb{Z}$ 或 $\mathbb{F}[x]$, 两个元素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/式一定能整除任何公共倍数/式. (lattices as posets)*

2.4 主理想与最大公约/最小公倍数/式

为叙述方便, 仅考虑 R 为整环的情形. 称子环 $I \subseteq R$ 为 R 的一个理想子环, 简称理想 (ideal), 若对任意 $r \in R$, $rI = \{rx \mid x \in I\} \subseteq I$. 例如偶数集可看作整数环 $\mathbb{Z}$ 的一个理想. 特别地, 若 I 可由一个元素生成, 即存在 $a \in R$ 使得

$$I = (a) := aR := \{ar \mid r \in R\},$$

则称 I 为一个主理想 (principal ideal).

事实上教材中关于最大公约数/式及上文中关于最小公倍数/式的叙述给出了如下关系.

Proposition 2.4.1. *For $a, b \in R = \mathbb{Z}$ or $\mathbb{F}[x]$, we have*

- $(a) + (b) := \{ua + vb \mid u, v \in R\} = ((a, b))$;
- $(a) \cap (b) = ([a, b])$.

3 典型例题

Problem 3.1. 设 $\mathbb{F}$ 为数域. $A \in \mathbb{F}^{n\times n}$ 的特征多项式为

$$\det(\lambda I - A) = (\lambda - \lambda_1)^{l_1}(\lambda - \lambda_2)^{l_2} \cdots (\lambda - \lambda_s)^{l_s},$$

其中 $\lambda_1, \lambda_2, \cdots, \lambda_s$ 互不相同, 那么 A^m 的特征多项式为

$$\det(\lambda I - A^m) = (\lambda - \lambda_1^m)^{l_1}(\lambda - \lambda_2^m)^{l_2} \cdots (\lambda - \lambda_s^m)^{l_s}.$$

证明. 由 $\mathbb{F}$ 是数域可设 $\lambda = r\mathrm{e}^{\mathrm{i}\theta}$, 其中 $r = |\lambda|$ 为其模长. 考虑多项式 $g(x) = \lambda - x^m$ 在 $\mathbb{C}$ 上的分解

$$g(x) = -(x^m - \lambda) = -\prod_{q=0}^{m-1}\left(x - r^{1/m}\mathrm{e}^{\mathrm{i}(\theta+2\pi q)/m}\right) = (-1)^{m-1}\prod_{q=0}^{m-1}\left(r^{1/m}\mathrm{e}^{\mathrm{i}(\theta+2\pi q)/m} - x\right),$$

那么

$$\begin{aligned}
\det(\lambda I - A^m) &= (-1)^{n(m-1)}\prod_{q=0}^{m-1}\det\left(r^{1/m}\mathrm{e}^{\mathrm{i}(\theta+2\pi q)/m}I - A\right) \\
&= (-1)^{n(m-1)}\prod_{q=0}^{m-1}\prod_{k=1}^{s}\left(r^{1/m}\mathrm{e}^{\mathrm{i}(\theta+2\pi q)/m} - \lambda_k\right)^{l_k} \\
&= (-1)^{n(m-1)}\prod_{k=1}^{s}\prod_{q=0}^{m-1}\left(r^{1/m}\mathrm{e}^{\mathrm{i}(\theta+2\pi q)/m} - \lambda_k\right)^{l_k} \\
&= (-1)^{n(m-1)}\prod_{k=1}^{s}\left((-1)^{m-1}g(\lambda_k)\right)^{l_k} = (-1)^{(m-1)\left(n+\sum_k \lambda_k\right)}\prod_{k=1}^{s}g(\lambda - \lambda_k^m)^{l_k}.
\end{aligned}$$

比较特征多项式的定义中等式两边关于 λ 的次数可知 $n = \sum_k \lambda_k$, 故而上式最后一项中 (-1) 对应的指数为偶数, 得最终结论成立. □

Problem 3.2. 证明对于正整数 m, n, 在 $\mathbb{F}[x]$ 中有

$$(x^m - 1, x^n - 1) = x^{(m,n)} - 1.$$

证明. 法一 (数学归纳法): 对 $\max(m,n)$ 进行归纳. (i) 当 $\max(m,n)=1$ 时结论显然成立. (ii) 假设命题对 $\max(m,n)<k$ 均成立, 当 $\max(m,n)=k$ 时不妨令 $m\leq n=k$. 若 $m=n$,

$$(x^m-1,x^n-1)=(x^m-1,x^m-1)=x^m-1=x^{(m,n)}-1;$$

若 $m<n$,

$$(x^m-1,x^n-1)=(x^m-1,x^n-1-x^{n-m}(x^m-1))=(x^m-1,x^{n-m}-1).$$

注意到此时 $\max(m,n-m)<k$, 于是根据归纳假设

$$(x^m-1,x^n-1)=(x^m-1,x^{n-m}-1)=(x^{(m,n-m)}-1)=x^{(m,n)}-1.$$

综上所述, 由归纳原理可知原命题成立.

法二 (唯一分解): 取 (x^m-1) 和 (x^n-1) 在 $\mathbb{C}$ 上的标准分解

$$x^m-1=\prod_{p=0}^{m-1}(x-\mathrm{e}^{2\pi\mathrm{i}p/m}),\ x^n-1=\prod_{q=0}^{n-1}(x-\mathrm{e}^{2\pi\mathrm{i}q/n}).$$

易知上述分解各自均不存在重复的一次因式, 故而只需要确定两个标准分解中公共的一次因式即可. 令

$$\mathrm{e}^{2\pi\mathrm{i}p/m}=\mathrm{e}^{2\pi\mathrm{i}q/n},$$

结合 p 和 q 的取值范围得 $p/m=q/n$, 即 $np=mq$. 下面确定所有满足条件的 p 和 q.

$$p=\frac{mq}{n}\in\mathbb{Z}\Leftrightarrow n\mid mq\Leftrightarrow\frac{n}{(m,n)}\mid\frac{m}{(m,n)}q\Leftrightarrow\frac{n}{(m,n)}\mid q,$$

其中最后一个等价性依赖于 $n/(m,n)$ 和 $m/(m,n)$ 互素. 结合 p 和 q 的取值范围可知满足条件的 p 和 q 有且仅有

$$q=sn/(m,n),\ s=0,1,\cdots,(m,n)-1;$$
$$p=tm/(m,n),\ t=0,1,\cdots,(m,n)-1.$$

最终可得

$$(x^m-1,x^n-1)=\prod_{s=0}^{(m,n)-1}(x-\mathrm{e}^{2\pi\mathrm{i}s/(m,n)})=x^{(m,n)}-1.$$

□

Problem 3.3. *求 $f(x)$ 除以 $g(x)$ 所得的商式与余式.*

1. $f(x)=x^4+2x^3-5x+7$, $g(x)=x^2-3x+1$;
2. $f(x)=x^4-x^3+4x^2+ax+b$, $g(x)=x^2+2x-3$.

证明.

$$\begin{aligned}x^4+2x^3-5x+7&=x^2(x^2-3x+1)+5x^3-x^2-5x+7\\&=(x^2+5x)(x^2-3x+1)+14x^2-10x+7\\&=(x^2+5x+14)(x^2-3x+1)+32x-7;\\x^4-x^3+4x^2+ax+b&=x^2(x^2+2x-3)-3x^3+7x^2+ax+b\\&=(x^2-3x)(x^2+2x-3)+13x^2+(a-9)x+b\\&=(x^2-3x+13)(x^2+2x-3)+(a-35)x+(b+39).\end{aligned}$$

验算技巧: 若除式 $g(x)$ 有简单的因式分解 (例如本题第二个例子中 $g(x)=x^2+2x-3=(x+3)(x-1)$), 可尝试将其零点代入被除式, 验证

$$f(x_0)=p(x_0)g(x_0)+r(x_0)=r(x_0).$$

对于本题第二个例子,

$$\begin{aligned}f(-3)&=81-(-27)+36-3a+b=144-4a+b=-3(a-35)+(b+39),\\ f(1)&=1-1+4+a+b=4+a+b=(a-35)+(b+39).\end{aligned}$$

□

Problem 3.4. *称整环 R 为主理想整环 (principal ideal domain, PID), 若 R 中的理想均为主理想. 试证明数域 $\mathbb{F}$ 上的多项式环 $\mathbb{F}[x]$ 为主理想整环.*

证明. 设 I 为 $\mathbb{F}[x]$ 的一个理想. 若 $I=\{0\}$, 那么 $I=(0)$ 为主理想. 否则可取 I 中次数最低的首一非零多项式 $m(x)$. 任取 $f(x)\in I$, 做如下带余除法

$$f(x)=q(x)m(x)+r(x), \deg r(x)<\deg m(x).$$

于是有

$$r(x)=f(x)-q(x)m(x)\in I+q(x)I\subseteq I+I\subseteq I.$$

由 $m(x)$ 的定义可知在 I 中不存在次数比 $m(x)$ 小的非零多项式, 故而 $r(x)=0$, $m(x)\mid f(x)$. 结合 $f(x)\in I$ 的任意性有 $I\subseteq(m(x))\subseteq I$, 即 $I=(m(x))$ 为主理想. □

事实上, 使用这一思路可证明 Euclid 整环一定是主理想整环 (ED $\Rightarrow$ PID).