线性代数复习

李忠华——线性代数讲义

时间：9/25/2022

版本：1.0

ElegantLaTeX Program

重学根基，日学日新

目录

第 1 章 多项式

1.1 数域

定义 1.1 (数域)

我们规定,$\mathbb{C}$ 是复数域, 若称子集 $\mathbb{F} \subset \mathbb{C}$ 是数域, 那么就要满足:

(1)$0, 1 \in \mathbb{F}$

(2)$\mathbb{F}$ 对数的加减乘除是封闭的, 即 $\forall a, b \in \mathbb{F}$

$$a+b, a-b, a \cdot b, \frac{a}{b}(b \neq 0) \in \mathbb{F}$$

♣

注 整数集合 $\mathbb{Z}$ 不是数域, 因为对除法不封闭.

注 我们定义记号 $\mathbb{F}^{\times}$ 为数域 F 中非零数构成的集合, 即

$$\mathbb{F}^{\times} = \mathbb{F} - \{0\} = \{c \in \mathbb{F} | c \neq 0\}$$

为了后续相关内容的叙述方便, 我们在这里先引入代数学中群环域的定义.

定义 1.2 (群与交换群 (Abel 群))

设 G 是非空集合, 在 G 上有一个二元运算. 对于任意的 $a, b, \in G$, 存在唯一的 $ab = a{\cdot}b \in G$ 与之对应, 且满足下面公理:

(G1)(结合律) 对任意 $a, b, c \in G$, 有 $(ab)c = a(bc)$;

(G2)(存在单位元) 存在 $e \in G$, 对于任意 $a \in G$, 有 $ae = ea = a$;

(G3)(存在逆元) 对于任意 $a \in G$, 存在 $b \in G$, 有 $ab = ba = e$ 那么我们称之为一个群.

若还满足:

(G4)(交换律) 对于任意 $a, b \in G$, 有 $ab = ba$. 则称 G 为交换群, 也称为 Abel 群.

♣

定义 1.3 (环、交换环、含幺环)

设非空集合 R 上配有两个二元运算, 一个记为加法, 一个记为乘法, 满足:

(R1)$(R, +)$ 是交换群;

(R2)(乘法结合律) 对任意的 $a, b, c \in R$, 有 $(ab)c = a(bc)$;

(R3)(分配律) 对任意的 a, b, c, 有

$$a(b+c) = ab + ac \quad (a+b)c = ac + bc$$

满足如上条件, 我们称 R 是一个环.

(R4)(乘法交换律) 对任意 $a, b \in R$, 有 $ab = ba$. 我们则称 R 是交换环.

(R5) 存在 $1_R \in R$, 使得对任意 $a \in R$, 有

$$1_R a = a 1_R = a$$

我们则称 R 是含幺环. ♣

定义 1.4 (除环和域)

设 D 是含幺环, 若 $1_D \neq 0$, 且 D 的任意非零元都是可逆元, 则称 D 是除环, 交换除环称作域. ♣

注 我们亦可以总结 (根据数学分析讲义第一节). 域就是一个非空集合上配有两种运算, 且两种运算均满足交换律, 结合律, 逆元, 单位元, 且乘法运算满足分配律.

1.2 一元多项式

定义 1.5 (一元多项式)

称形式表达式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

为 $\mathbb{F}$ 上的一个关于未定元 x 的一元多项式, 也称为一个 $\mathbb{F}$-系数一元多项式. ♣

注 之所以称 x 是未定元而不是未知数, 是因为 x 可能带入的不仅仅是数, 可以是其他合适的对象, 例如矩阵.

注 当 $a_n \neq 0$ 时, 我们把 $a_n x_n$ 称为首项, 把 a_n 称为首项系数, 把 a_0 称为常数项. 首项系数为 1 的多项式, 我们称之为首一多项式.

注 我们把所有系数都为零的多项式称为零多项式, 记为 0, 约定零多项式的次数为 $-\infty$, 即

$$\deg 0 = -\infty$$

定义 1.6

我们可以规定数域 $\mathbb{F}$ 上所有一元多项式做成的集合为 $\mathbb{F}[x]$, 即

$$\mathbb{F}[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 : n \in \mathbb{Z}_{\geqslant 0}, a_0, \cdots, a_n \in \mathbb{F}\}$$ ♣

接下来, 我们可以对多项式规定其加减乘法的运算, 可以发现,$\mathbb{F}[x]$ 在多项式的加法和乘法下成为有单位元的交换环, 称其为一元多项式环.

1.3 带余除法

我们首先介绍整数的带余除法, 这样就可以自然而然的过渡到多项式的带余除法.

定理 1.1 (整数的带余除法)

对于任意 $a, b \in \mathbb{Z}$, 其中 $b > 0$, 存在唯一的 $q, r \in \mathbb{Z}$, 使得

$$a = qb + r, 0 \leqslant r < b$$

称 q 是 b 除 a 的商,r 是余数.

♡

定理 1.2 (多项式的带余除法)

设 $f(x), g(x) \in \mathbb{F}[x]$, 其中 $g(x) \neq 0$, 存在唯一的 $q(x), r(x) \in \mathbb{F}[x]$, 使得

$$f(x) = q(x)g(x) + r(x), 0 \leqslant \deg(r(x)) < \deg(g(x))$$

我们称 $g(x)$ 除 $f(x)$ 的商是 $q(x)$, 而余式是 $r(x)$.

♡

证明 我们粗略写下证明的概要, 我们需要证明的是存在性和唯一性. 当 $\deg(f(x)) < \deg(g(x))$, 结果是显然的. 只需讨论 $\deg(f(x)) \geqslant \deg(g(x))$, 其中会运用到数学归纳法.

对于证明唯一性, 运用到反证法. 在整个多项式一章, 运用的最广泛的两个方法即是数学归纳法和反证法.

运用带余除法化简式子的例子繁多, 不再赘述. 当除式为首一多项式时, 还可以运用综合除法简化运算. 我们下面一个例子是介绍利用带余除法降低运算的次数.

例题 1.1 设多项式 $f(x) = x^5 - 4x^4 + 3x^3 - 2x^2 + x - 1$, 计算 $f(1+\sqrt{3})$.

解 记 $\alpha = 1 + \sqrt{3}$, 则有 $(\alpha - 1)^2 = 3$, 即 $\alpha^2 - 2\alpha - 2 = 0$, 令 $g(x) = x^2 - 2x - 2$, 有 $g(\alpha) = 0$. 通过带余除法可得

$$f(x) = (x^3 - 2x^2 + x - 4)g(x) + (-5x - 9)$$

从而 $f(\alpha) = -14 - 5\sqrt{3}$.

1.4 整除性

定义 1.7 (整除)

设 $f(x), g(x) \in \mathbb{F}[x]$.

如果存在 $q(x) \in \mathbb{F}[x]$, 使得 $f(x) = q(x)g(x)$, 则称 $g(x)$ 在 $\mathbb{F}[x]$ 中整除 $f(x)$, 记作 $g(x)|f(x)$.

当 $g(x)$ 整除 $f(x)$ 时, 称 $g(x)$ 是 $f(x)$ 的一个因式, 而 $f(x)$ 是 $g(x)$ 的一个倍式. ♣

多项式的整除满足如下的性质:

命题 1.1

设 $f(x), g(x), h(x), f_1(x), \cdots, f_r(x) \in \mathbb{F}[x]$, 其中 $r \in \mathbb{N}$. 有

(1)$g(x)|g(x), g(x)|0, a|g(x)(\forall a \in \mathbb{F}^{\times})$;

(2)$g(x)|f(x)$ 且 $f(x) \neq 0 \Rightarrow \deg(g(x)) \leq \deg(f(x))$;

(3)$f(x)|g(x), g(x)|f(x) \Leftrightarrow \exists c \in \mathbb{F}^{\times}$, 使得 $f(x) = cg(x)$. 我们称此时 $f(x), g(x)$ 相伴, 记作 $f(x) \sim g(x)$;

(4)$f(x)|g(x), g(x)|h(x) \Rightarrow f(x)|h(x)$;

(5) 若 $g(x)|f_i(x), i = 1, 2, \cdots, r$, 则对任意 $u_1(x), u_2(x), u_r(x) \in \mathbb{F}[x]$, 有

$$g(x)|(u_1(x)f_1(x) + \cdots u_r(x)f_r(x))$$

♠

定理 1.3 (整除不随域扩张而改变)

设 $\mathbb{F}_1, \mathbb{F}_2$ 都是数域, 且 $\mathbb{F}_1 \subset \mathbb{F}_2$. 设 $f(x), g(x) \in \mathbb{F}_1[x](\subset \mathbb{F}_2[x])$, 则

$$g(x)|f(x) \in \mathbb{F}_1[x] \Leftrightarrow g(x)|f(x) \in \mathbb{F}_2[x]$$

♡

1.5 最大公因式

我们依旧从整数理论出发, 然后延伸到多项式中. 我们记任意两个未定元 a, b 的最大公因式的记号为 (a, b).

定义 1.8 (整数的最大公因子)

设 a, b 是两个不全为 0 的整数,$d \in \mathbb{N}$, 则 $d = (a, b)$ 的充分必要条件是:

(i)$d|a, d|b$;

(ii)$\forall d_1 \in \mathbb{Z}, d_1|a, d_1|b \longrightarrow d_1|d$. ♣

也就是说, 所有的公因子都是最大公因子的因子. 我们用整数举个例子, 不妨设 $a = 8, b =$

12, 则他们的公因子为

$$\pm 1, \pm 2, \pm 4$$

这样我们就可以发现当 4 是最大公因子. 我们依葫芦画瓢, 也可以得到多项式的最大公因式.

定义 1.9 (多项式的最大公因式)

不妨设 $f(x), g(x) \in \mathbb{F}[x]$, 我们令 $d(x) = (f(x), g(x))$. 则有

(i)$d(x)|f(x), d(x)|g(x)$;

(ii)$\forall d_1(x) \in \mathbb{F}[x], d_1(x)|f(x), d_1(x)|g(x), d_1(x)|d(x)$.

♣

引理 1.1

设 $f(x), g(x) \in \mathbb{F}$ 不全为零,$d(x) \in \mathbb{F}[x]$.

(1) 如果 $d(x)$ 是 $f(x), g(x)$ 的最大公因式,$d_1(x) \in \mathbb{F}[x]$, 则

$$d_1(x)\text{也是最大公因式} \iff d_1(x) \sim d(x)$$

(2)$f(x), g(x)$ 有最大公因式, 则 $d(x)$ 为最大公因式的充分必要条件为

(i)$d(x)|f(x), d(x)|g(x)$;

(ii)$\forall d_1(x) \in \mathbb{F}[x], d_1(x)|f(x), d_1(x)|g(x) \longrightarrow \deg(d_1(x)) \geqslant \deg(d(x))$.

♡

定理 1.4 (Euclid 辗转相除法)

设 $f(x), g(x) \in \mathbb{F}[x]$, 则存在 $d(x) = (f(x), g(x)) \in \mathbb{F}[x]$, 且存在 $u(x), v(x) \in \mathbb{F}[x]$, 使得

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

我们也将上面的等式称作 Bezout 等式.

♡

证明 待补.

定理 1.5 (最大公因式不随域扩张而改变)

多项式的最大公因式不随系数域的扩大而改变.

♡

1.6 多项式互素

定义 1.10 (互素)

设 $f(x), g(x) \in \mathbb{F}[x]$, 若 $(f(x), g(x)) = 1$, 则称 $f(x)$ 与 $g(x)$ 互素.

♣

通过上一节的 Bezout 等式, 我们也能得到互素的一个充分必要条件.

定理 1.6

设 $f(x),g(x)\in\mathbb{F}[x]$, 则 $f(x),g(x)$ 互素的充分必要条件是存在 $u(x),v(x)\in\mathbb{F}[x]$, 使得

$$u(x)f(x)+v(x)g(x)=1$$

我们这里举出一个互素和最大公因式综合运用的例子, 看看它们在分母有理化上所发挥的作用.

例题 1.2 试将下面分数的分子分母乘适当的根式将分母有理化.

$$\frac{1}{\sqrt[3]{4}+2\sqrt[3]{2}+3}$$

解 我们令 $\alpha=\sqrt[3]{2}$, 那么可以将分母表示为 $f(\alpha)=\alpha^2+2\alpha+3$. 我们又知 $\alpha^3=2$, 所以令 $g(\alpha)=\alpha^3-2$. 这样我们就得到了两个多项式 $f(x)=x^2+2x+3, g(x)=x^3-2$. 我们对两个多项式进行辗转相除, 可以发现其最大公因式为 11. 我们通过回溯辗转相除法, 可以得到 $u(x),v(x)$. 于是可以表示为

$$11=(x^2-4x+5)f(x)+(-x+2)g(x)$$

我们将 α 带入就可以知道, 应该对分母乘上 $\sqrt[3]{4}-4\sqrt[3]{2}+5$, 便可以使得分母有理化, 为 11.

1.7 唯一分解定理

定义 1.11 (素数)

对于 $p\in\mathbb{N}$, 若 $p\neq 1$, 且 p 的因子只有 $\pm1.\pm p$, 则称 p 是素数.

定理 1.7 (算术基本定理)

对任意的 $n\in\mathbb{N}, n>1, n$ 可以唯一地写成素数的乘积.

定义 1.12 (不可约多项式)

设 $p(x)\in\mathbb{F}[x]$ 且 $\deg(p(x))\geqslant 1$. 如果 $p(x)$ 满足下面的等价条件之一:

(i)$p(x)$ 不能写成 $\mathbb{F}$ 上两个次数比 $p(x)$ 小的多项式的乘积;

(ii)$p(x)$ 的因式只有

$$c\in\mathbb{F}^{\times}\quad and\quad cp(x),c\in\mathbb{F}^{\times}$$

则称 $p(x)$ 是 $\mathbb{F}$ 上的不可约多项式.

命题 1.2

设 $p(x)\in\mathbb{F}[x]$ 为不可约多项式.

(1) 对任意 $f(x)\in\mathbb{F}[x]$, 有

$$(p(x),f(x))=1 \quad or \quad p(x)|f(x)$$

(2) 设 $f(x),g(x)\in\mathbb{F}[x]$, 若 $p(x)|f(x)g(x)$, 则 $p(x)|f(x)$ or $p(x)|g(x)$. 进而, 如果

$$p(x)|f_1(x)f_2(x)\cdots f_s(x)(f_1(x),\cdots,f_s(x)\in\mathbb{F}[x])$$

则存在 $i(1\leqslant i\leqslant s)$, 使得 $p(x)|f_i(x)$.

定理 1.8 (因式分解的唯一性定理)

设 $f(x)\in\mathbb{F}[x]$ 且 $\deg(f(x))\geqslant 1$, 则 $f(x)$ 可以唯一分解为 $\mathbb{F}$ 上有限个不可约多项式的乘积. 这里的唯一性是指: 如果有两个分解式

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

其中 $p_1(x)p_2(x)\cdots p_s(x)$ 与 $q_1(x)q_2(x)\cdots q_t(x)$ 都是 $\mathbb{F}$ 上的不可约多项式. 则 $s=t$, 且将两个不可约多项式组进行重排后, 有 $p_i(x)\sim q_i(x), i=1,2,\cdots,s$.

命题 1.3

设 $0\neq f(x),g(x)\in\mathbb{F}[x]$ 有分解式

$$f(x)=cp_1^{(a_1)}(x)p_2^{(a_2)}(x)\cdots p_t^{(a_t)}(x),\quad g(x)=dp_1^{(b_1)}(x)p_2^{(b_2)}(x)\cdots p_t^{(b_t)}(x)$$

则

$$(f(x),g(x))=p_1^{(r_1)}(x)p_2^{(r_2)}(x)\cdots p_t^{(r_t)}(x)$$

其中

$$r_i=\min\{a_i,b_i\}(i=1,2,\cdots,t)$$

特别地,$(f(x),g(x))=1$ 的充分必要条件是它们无相同的不可约多项式.

1.8 多项式的根

定义 1.13 (根)

设 $f(x)\in\mathbb{F}[x], c\in\mathbb{F}$. 若 $f(c)=0$, 则称 c 为 $f(x)$(在 $\mathbb{F}$ 上) 的一个根.

命题 1.4 (因式定理)

设 $f(x) \in \mathbb{F}[x], c \in \mathbb{F}$, 则

$$c\text{为}f(x)\text{的根} \iff x-c|f(x)$$

定理 1.9

设 $0 \neq f(x) \in \mathbb{F}[x], \deg(f(x)) = n \in \mathbb{Z}$, 则 $f(x)$ 在 $\mathbb{F}$ 中最多有 n 个根.

推论 1.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 满足

$$\deg(f(x)), \deg(g(x)) \leqslant n \in \mathbb{N}$$

又设 $a_1, a_2, \cdots, a_{n+1} \in \mathbb{F}$ 两两互不相同, 满足

$$f(a_i) = g(a_i), i = 1, 2, \cdots, n+1$$

则有 $f(x) = g(x)$

1.9 重因式

定义 1.14 (重因式)

设 $p(x) \in \mathbb{F}[x]$ 是首一不可约多项式,$k \in \mathbb{Z}$, 称 $p(x)$ 是 $f(x)$ 的 k 重因式, 如果

$$p^k(x)|f(x),\ p^{k+1}(x) \nmid f(x)$$

当 $k=0$ 时,$p(x)$ 不是 $f(x)$ 的因式;$k=1$ 时,$p(x)$ 是 $f(x)$ 的单因式; 当 $k>1$ 时, 称 $p(x)$ 是 $f(x)$ 的重因式.

定理 1.10

设 $p(x), f(x) \in \mathbb{F}[x]$, 其中 $p(x)$ 是 $f(x)$ 首一不可约多项式, 设 $k \in \mathbb{N}$, 则

$$p(x)\text{为}f(x)\text{的}k\text{重因式} \iff p(x)\text{为}f'(x)\text{的}k-1\text{重因式}$$

推论 1.2

设 $k \in \mathbb{N}, p(x), f(x) \in \mathbb{F}[x]$, 其中 $p(x)$ 是首一不可约多项式.

(1) 若 $p(x)$ 是 $f(x)$ 的 k 重因式, 则 $p(x)$ 分别是 $f'(x), f''(x), \cdots, f^{k-1}(x)$ 的 $k-1, k-2, \cdots, 1$ 重因式, 而不是 $f^(k)(x)$ 的因式;

(2)$p(x)$ 是 $f(x)$ 的 k 重因式当且仅当

$$p(x)|f(x), f'(x), \cdots, f^{(k-1)}(x), \quad however\ p(x) \nmid p^{(k)}(x);$$

(3)$p(x)$ 为 $f(x)$ 的重因式当且仅当 $p(x)|(f(x),f'(x))$.

(4)$f(x)$ 无重因式当且仅当 $(f(x),f'(x))=1$.

推论 1.3

(1)c 是 $f(x)$ 的重根 $\iff f(c)=f'(c)=0$;

(2)c 是 $f(x)$ 的 k 重根 $\iff f(c)=f'(c)=\cdots=f^{k-1}=0$, 而 $f^k(c)\neq 0$;

(3)$f(x)$ 在 $\mathbb{F}$ 中有重根 $\iff (f(x),f'(x))$ 在 $\mathbb{F}[x]$ 中有一次因式;

(4) 如果 $f(x)$ 在 $\mathbb{F}$ 中有重根, 那么 $f(x)$ 在 $\mathbb{F}[x]$ 中有重因式.

1.10 复系数多项式的因式分解

定理 1.11 (代数基本定理)

设 $f(x)\in\mathbb{C}[x]$ 且 $\deg(f(x))\geq 1$, 则 $f(x)$ 在 $\mathbb{C}$ 中至少有一个根.

定理 1.12

(1) 设 $p(x)\in\mathbb{C}[x]$, 则

$$p(x)\text{不可约}\iff p(x)\text{是一次的}.$$

(2) 任意次数大于等于 1 的复系数多项式, 在 $\mathbb{C}$ 中可以唯一分解为一次因式的乘积.

(3) 任意 n 次复系数多项式有 n 个复根.

1.11 实系数多项式的因式分解

定理 1.13

(1) 设 $0\neq p(x)\in\mathbb{R}[x]$ 是首一多项式, 则

$$p(x)\text{不可约}\iff p(x)=x-c(\exists c\in\mathbb{R})\ or\ p(x)=x^2+px+q(\exists p,q\in\mathbb{R},p^2-4q<0).$$

1.12 有理数系数多项式的因式分解

命题 1.5

设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x], n \in \mathbb{N}, a_n = 0$, 设 $\alpha = \dfrac{r}{s} \in \mathbb{Q}$ 为 $f(x)$ 的根, 其中 $r, s \in \mathbb{Z}, (r, s) = 1$, 则有

$$s|a_n, \quad r|a_0$$

特别地, 若 $a_n = 1$, 则 $\alpha \in \mathbb{Z}$ 且 $\alpha|a_0$.

定义 1.15 (本原多项式)

设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x], n \geq 1$, 若系数 $a_0, a_1, \cdots, a_n$ 互素, 则称 $f(x)$ 为本原多项式.

引理 1.2

设 $f(x) \in \mathbb{Q}[x], \deg(f(x)) \geq 1$.

(1) 存在 $r \in \mathbb{Q}$, 存在本原多项式 $g(x) \in \mathbb{Z}[x]$, 使得 $f(x) = rg(x)$. 若 $f(x) \in \mathbb{Z}[x]$, 则可取 $r \in \mathbb{Z}$.

(2) 如果 $f(x) = r_1 g_1(x) = r_2 g_2(x)$, 其中 $r_1, r_2 \in \mathbb{Q}, g_1(x), g_2(x) \in \mathbb{Z}[x]$ 是本原多项式, 则

$$r_1 = r_2.g_1(x) = g_2(x)\text{或者}r_1 = -r_2, g_1(x) = -g_2(x).$$

引理 1.3 (Gauss 引理)

两个本原多项式的乘积仍本原.

根据上面的所有的引理, 我们可以得到如下的结论.

定理 1.14

设 $f(x) \in \mathbb{Z}[x], \deg(f(x)) \geq 1$, 则

$$f(x)\text{在}\mathbb{Z}[x]\text{中可约} \iff f(x)\text{在}\mathbb{Q}[x]\text{中可约}$$

定理 1.15 (Eisenstein 判别法)

设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x], n \geq 1$. 如果存在素数 p, 满足

(i) $p \nmid a_n$,

(ii) $p|a_i, i = 0, 1, \cdots, n-1$,

(iii) $p^2 \nmid a_0$,

则 $f(x) \in \mathbb{Q}[x]$ 中不可约.

例题 1.3 设 $f(x) = x^n + 2(n \in \mathbb{N})$, 当取 $p = 2$ 时, 由 Eisenstein 判别法就可知其在 $\mathbb{Q}$ 上不可约.

例题 1.4 证明:$f(x) = x^6 + x^3 + 1$ 在 $\mathbb{Q}$ 上不可约.

证明 本题直接使用判别法无法算出, 所以需要做出适当的变换. 令 $y = x + 1$ 然后带入, 求得 $f(y)$ 的结果后, 很容易发现其满足 Eisenstein 判别法. 然后通过反证 $f(x)$ 可约, 通过 $g(x)$ 不可约, 可知 $f(x)$ 不可约.

例题 1.5 判别多项式 $f(x) = x^4 + 3x + 1$ 在 $\mathbb{Q}$ 上的可约性.

证明 本题无法通过 Eisenstein 判别法进行求解, 所以给出一种判别的新方法. 先计算出其所有的有理根, 发现其没有一次因式, 若其可约, 只有可能是两个因式的乘积. 通过待定系数, 得出方程组, 若方程组有解, 说明其是可约的; 若方程组无解, 那就说明其是不可约的.