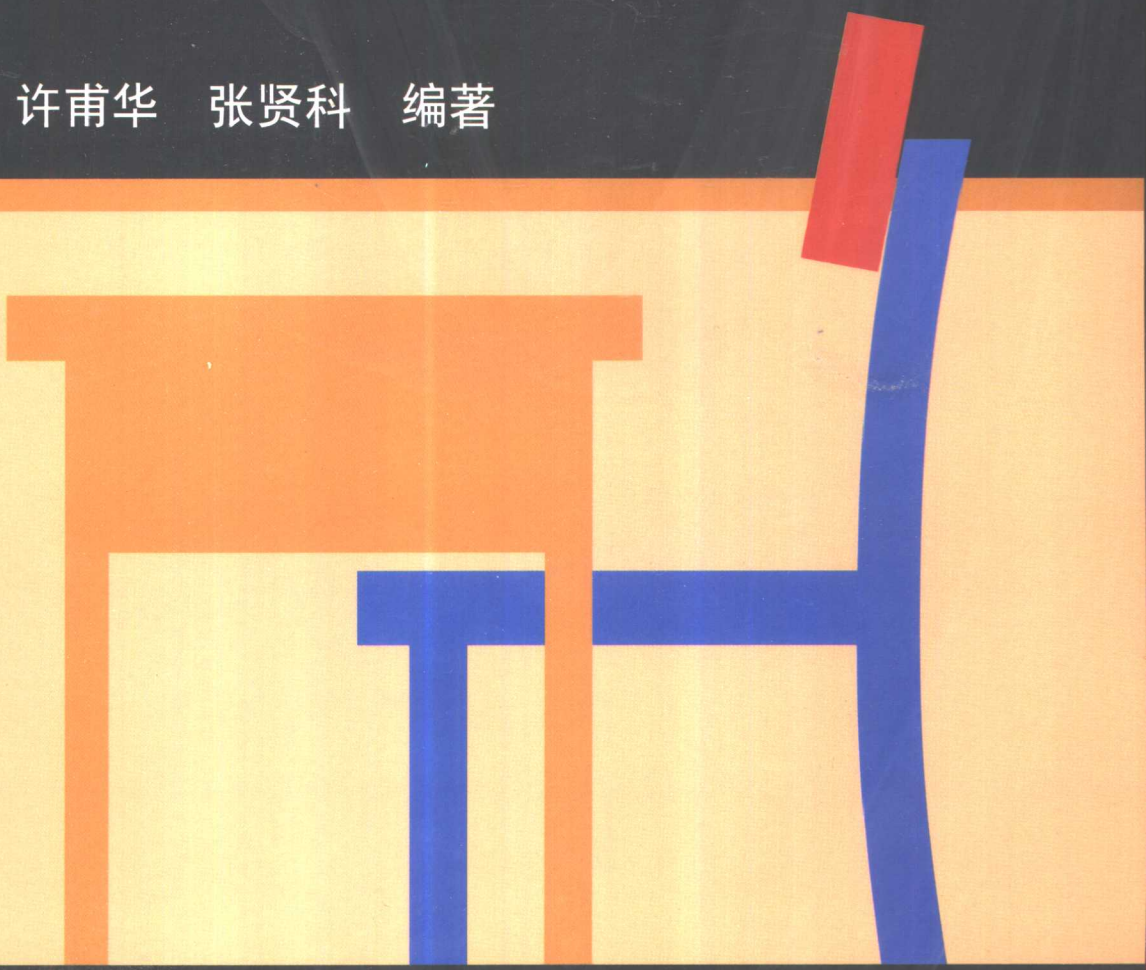
高等代数解题方法

许甫华　张贤科　编著



清华大学出版社
http://www.tup.tsinghua.edu.cn

高等代数解题方法　许甫华　张贤科　编著　清华大学出版社

高等代数解题方法

许甫华　张贤科　编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书是学习高等代数和线性代数的辅导参考书，内容系统深入. 按本社出版的《高等代数学》(张贤科、许甫华编著，1998 年)章节为顺序，内容有：系统的线性代数学，数与多项式理论，近世代数介绍，变换族(群)，张量积和外积等，共 11 章. 每章包括：概念和定理介绍；解题方法思路的分析总结；《高等代数学》书中全部习题的详细分析解答. 本书的补充题与解答，融入了作者在中国科大和清华大学的数学系和非数学系的长期教学经验和科研心得. 本书适用于各类高校学生学习和复习时参考，还适合于各类考试(例如研究生考试)前的复习以及应用代数的科学技术人员学习参考.

书　名：高等代数解题方法
作　者：许甫华　张贤科　编著
出版者：清华大学出版社(北京清华大学学研大厦，邮编 100084)
http:// www. tup. tsinghua. edu. cn
印刷者：世界知识印刷厂
发行者：新华书店总店北京发行所
开　本：787×1092 1/16　印张：26.5　字数：613 千字
版　次：2001 年 9 月第 1 版　2001 年 9 月第 1 次印刷
书　号：ISBN 7-302-04533-X/O・257
印　数：0001～4000
定　价：29.80 元

引　言

本书是学习和使用高等代数和线性代数的辅导参考书，内容系统深入. 本书适用于各类高校学生学习和复习时参考；并适合各类考试（例如研究生考试）前的复习以及应用代数的科学技术人员学习参考.

内容顺序按《高等代数学》（张贤科，许甫华编著. 清华大学出版社. 1998 年），包括：系统的线性代数学，数与多项式理论，近世代数介绍，酉空间和内积空间，变换族（群），张量积和外积等，共 11 章. 每章首先介绍概念和定理，然后是解题方法思路分析（绝大部分章均有），接下来逐一详细分析解答《高等代数学》一书收入的大量习题，最后是此次补充的习题和解答. 本书对大量各类问题，包括一些难题，作了深入分析，给出详尽解答，并总结了解题方法. 许多解题方法简洁巧妙，切入理论本质的理解，是作者多年教学的积累，期望能引导启发读者掌握解决问题的思路和方法，帮助读者克服在高等代数的学习、复习、迎考和应用中遇到的困难，培养学习代数的兴趣，增进对代数理论的深入理解.

第一作者有长期教授“非数学系线性代数”课程的经验（也有数学系高等代数教学经验），包括理论课和习题课（在中国科技大学和清华大学），有许多教学心得和解题方法技巧方面的总结，大多融入了本书. 第二作者有长期从事数学系高等代数和其他代数、数论课程的教学及科研经验，使得本书收入了一些综合性强的习题. 此次特别在第 10、11 章的补充题中，较系统介绍了线性空间的“变换族”（变换群）、空间的特征分解、对称平方等群表示论的基础问题，这是许多数学和应用领域常常需要的.

《高等代数学》一书有一些特点，也影响到本书，现将该书前言简述如下：内容较深厚，基础训练得到加强；包含了一些进一步的内容，采用了较新的理论观点. 一方面，坐标和矩阵方法使用较多，因为有简洁直接性，可算性，也有助于对抽象概念的理解领悟；另一方面，映射和变换等概念和方法论述也很充分，这是进一步学习和阅读现代文献的基础. 为了适应理论和应用两方面的新需求，采用了较新的理论角度，也写进了一些书中不常有的内容，一些地方试探了新的、可能更自然的发展脉路和证法.《高等代数学》一书适于高等学校作高等代数或者线性代数的教材. 可以讲授两学期，每周四学时. 也可以只讲授一学期，每周四或三学时，只讲第 2—6 章及若干介绍（若当形、二次型和欧氏空间，即 7.7～7.9，8.1～8.4，9.1～9.3）. 带星号的内容一般不作要求.

《高等代数学》一书出版以来，收到全国各地一些读者来信，反映此书对他们学习帮助很大，其中也有自学、考研究生的同学询问书上习题的解答. 这也促使我们下决心编写目前这样一本解题方法方面的书.

本书中分析讨论的问题，数量很大，有各种层次. 一方面有许多基础性问题，从多个角度帮助理解理论和概念，锤炼基本方法. 另一方面，也有许多层次较高的问题，有助于进一步的学习和应用. 不少问题的解答有独特思路和方法，有的是吸收了较新的成果，有些则

是作者的心得积累.创新能力和创新意识的提高,人人向往,它需要我们主动地、深入系统地学习和理解现代理论,在实践中不断培养分析和解决问题的能力.我们希望本书在这方面对读者能有所帮助,帮您实现跨越.

不足之处,请批评指正.

作　者

2000 年初夏于清华园

目　录

第1章

数与多项式

1.1 定义与定理

定义 1.1 设 G 是一个非空集合，在 G 中定义了一个二元运算 $*$（即对 G 中任意 a,b 在 G 中有唯一元素（记为 $a*b$）与之对应），且满足如下规律：

(1) **封闭性** 对任意 $a,b\in G$，总有 $a*b\in G$；

(2) **结合律** $a*(b*c)=(a*b)*c$（对任意 $a,b,c\in G$）；

(3) 恒元 存在 $e\in G$，使 $e*a=a$ 对所有 $a\in G$ 成立；

(4) 逆元 对任意 $a\in G$，总存在 $b\in G$，使 $b*a=e$.

则称 $(G,*)$ 为**群**，(4)中的 b 称为 a 的逆元，记为 a^{-1}，(3)中恒元也称为单位元.

如果还有对任意 $a,b\in G$，$a*b=b*a$，则称 $(G,*)$ 为 **Abel 群**或**交换群**. Abel 群的运算常记为加法(+)，恒元常记为 0 称为**零元**，a 的逆元常记为 $-a$ 称为 a 的负元.

定义 1.2 设 R 是一个集合，在 R 上定义了两个二元运算，分别记为加法(+)和乘法(*)，且满足：

(1) $(R,+)$ 是 Abel 群；

(2) $(R,*)$ 是半群，即满足封闭性和结合律；

(3) **分配律** $a*(b+c)=a*b+a*c$，$(a+b)*c=a*c+b*c$，对任意 $a,b,c\in R$ 成立. 则称 $(R,+,*)$ 为**环**. 如果环 R 对乘法有恒元 e，则称 R 为**含幺环**. 若乘法满足交换律，则称 R 为**交换环**. 在含幺环 R 中，对 $c\in R$，若 $\exists x\in R$ 使得 $xc=cx=e$，则称 x 为 c 的**逆元**，称 c 为**可逆元**.

定义 1.3 设 F 是有两个二元运算(+)和(·)的集合，且满足：

(1) $(F,+)$ 是 Abel 群；

(2) $(F^*,\cdot)$ 是 Abel 群，F^* 指 F 的非 0 元全体；

(3) 分配律；

则称 $(F,+,\cdot)$ 为域.

定义 1.4 若域 F 的子集合 K 对于 F 中的原运算仍是一个域，则称 K 是 F 的**子域**，F 是 K 的扩域，类似有**子群**，**子环**的定义.

定义 1.5 若整数 a 与 b 除以 m 的余数相同，则称 a 与 b 对模 m 同余，记为 $a\equiv b(\mathrm{mod}\ m)$.

弃九法：记正整数 a 的十进位表示的各位数字之和除以 9 的余数为 $\bar{a}$，则“弃九法”断言，若 $a\times b=c$，则 $\overline{\bar{a}\times\bar{b}}=\bar{c}$；若 $a+b=c$，则 $\overline{\bar{a}+\bar{b}}=\bar{c}$.

定理 1.1 整数对模 m 的 m 个同余类构成的集合记为

$$\mathbf{Z}/m\mathbf{Z} = \{l + m\mathbf{Z} \mid l = 0,1,\cdots,m-1\} = \{\bar{0},\bar{1},\cdots,\overline{m-1}\},$$

它对如下定义的加法和乘法是一个交换环：

$$\bar{l_1} + \bar{l_2} = \overline{l_1 + l_2}, \qquad \bar{l_1} \cdot \bar{l_2} = \overline{l_1 l_2}.$$

定理 1.2 (1) 当 $m = p$ 为素数时，$\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ 是域.

(2) 当 m 不是素数时，$\mathbf{Z}/m\mathbf{Z}$ 不是域. 此时 $\bar{l}$ 可逆，当且仅当 l 与 m 互素.

定义 1.6 $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} = \{\bar{0},\bar{1},\cdots,\overline{p-1}\}$，称为 **$p$ 元(有限)域**(其中 p 为素数，这样的域称为**特征是 p** 的域.

定理 1.3 (Fermat) $\mathbf{F}_p$ 的元素 x 均满足

$$x^p = x.$$

定理 1.4 域 F 上 X 的多项式形式全体 $F[X]$ 按如下运算成为交换环(称为多项式形式环)

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i,$$

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} \left(\sum_{i+j=k} a_i b_j\right) x^k.$$

其中 a_i, b_i 只有有限个非零.

系 多项式形式环 $F[X]$ 中**消去律**成立，即若 $fg = fh$，且 $f \neq 0$，，则 $g = h$(对任意 $f, g, h \in F[X]$).

定义 1.7 有消去律的含幺交换环称为整环.

定理 1.5(带余除法) 对域 F 上任两多项式形式 $f, g \in F[X]$，若 $g \neq 0$，则总存在多项式形式 $q, r \in F[X]$ 使

$$f = gq + r, \quad \deg r < \deg g \text{ 或 } r = 0,$$

且 q 和 r 由 f, g 唯一地决定.

定义 1.8 有带余除法的环称为 **Euclid 环**.

定理 1.6 记 f 与 g 的首一最大公因子为 (f, g)，若 $f = gq + r$，则 $(f, g) = (r, g)$. (其中 $f, g, q, r \in F[X]$).

定理 1.7 域 F 上任两不全为 0 的多项式形式 $f, g \in F[X]$ 的最大公因子 d 存在且唯一(不计常数倍)；且存在 $u, v \in F[X]$ 使

$$uf + vg = d. \qquad \textbf{(Bezout 等式)}$$

系 1 f 与 $g (\in F[X])$ 互素当且仅当存在 $u, v \in F[X]$ 使得

$$uf + vg = 1.$$

系 2 若 $h \mid fg$，$(h, g) = 1$，则 $h \mid f$.

系 3 若 $(f, g) = 1$，$(f, h) = 1$，则 $(f, gh) = 1$.

系 4 若 $f \mid h$，$g \mid h$，$(f, g) = 1$，则 $fg \mid h$.

系 5 设 $f_1, \cdots, f_n \in F[X]$，则其首一最大公因子 $(f_1, \cdots, f_n)$ 存在且唯一，且存在 $u_1, \cdots, u_n \in F[X]$ 使得

$$u_1 f_1 + \cdots + u_n f_n = (f_1, \cdots, f_n) \qquad \text{(Bezout 等式)}.$$

定义 1.9 若域 F 上的非常数多项式形式 $f \in F[X]$ 可表为

$$f = gh \qquad (g,h \in F[X] \text{ 均非常数}),$$

则称 f 在 F 上是**可约的**；否则称 f 是不可约的.

定理 1.8 域 F 上的多项式形式环 $F[X]$ 是**唯一析因整环**. 即对任一非常数多项式 $f \in F[X]$ 均有

$$f = p_1 p_2 \cdots p_s,$$

其中 $p_1,\cdots,p_s$ 是不可约多项式，且不计常数倍及 p_i 的次序，此分解是唯一的.

定理 1.9(算术基本定理) 整数环 $\mathbf{Z}$ 是唯一析因环. 即任一整数 n($0,\pm1$ 除外)均可表为素数的乘积 $n=p_1\cdots p_s$，若不计正负号和素数的次序，则此表示是唯一的.

定理 1.10 设 $f(X)\in F[X], c\in F$，则有

(1) (**余数定理**)$f(X)$除以 $X-c$ 的余式为 $f(c)$.

(2) (**零点一因子定理**)$X-c$ 整除 $f(X)$的充分必要条件为 $f(c)=0$.

定理 1.11 域 F 上的 $n(\geqslant 0)$次多项式 $f(X)\in F[X]$在 F 中最多有 n 个根(重根按重数计入).

定理 1.12 若次数小于 n 的两个多项式形式 $f(X), g(X)\in F[X]$，在 n 个不同点 $c_1,\cdots,c_n\in F$ 的值均相同，即

$$f(c_i) = g(c_i) \qquad (1 \leqslant i \leqslant n),$$

则 $f(X)=g(X)$.

定理 1.13 设 $f(X)\in F[X]$, $c\in F$.

(1) c 为 $f(X)$的重根$\rightleftharpoons f(c)=f'(c)=0$,

$\rightleftharpoons c$ 为$(f(X),f'(X))$的根；

(2) 若$(f,f')=1$，则 $f(X)$无重根(在 F 或其任意扩域中)；

(3) 若 $f(X)$在 F 上不可约且 $f'(X)\neq 0$，则 $f(X)$无重根(在 F 或其任意扩域中)，特别，数域上不可约多项式在 $\mathbf{C}$ 中无重根.

定理 1.14 设 $f(X), p(X)\in F[X], p(X)$不可约.

(1) $p(X)$为 $f(X)$的重因子$\Leftrightarrow p(X)$为 $f(X)$与 $f'(X)$的公因子.

(2) $(f,f')=1\rightleftharpoons f(X)$无重因子.

古典代数学基本定理 任一非常数复系数多项式在复数域中总有一根.

定理 1.15 n 次复系数多项式$(n\geqslant 1) f(X)$在复数域 $\mathbf{C}$ 中恰有 n 个根，且总可以唯一分解为一次因子的乘积

$$f(X) = c(X-z_1)^{n_1}(X-z_2)^{n_2}\cdots(X-z_s)^{n_s}. \qquad (c,z_i \in \mathbf{C})$$

定理 1.16 实系数多项式(次数$\geqslant 1$) $f(X)$在实数域上总可以唯一分解为一次和二次不可约因子之积

$$f(X) = a(X-a_1)^{n_1}\cdots(X-a_s)^{n_s}(X^2-b_1X+c_1)^{e_1}\cdots(X^2-b_tX+c_t)^{e_t}.$$

定义 1.10 若 $f(X)\in\mathbf{Q}[X]$且其系数为互素的整数，则称 $f(X)$为本原多项式.

定理 1.17 设 $f(X)\in\mathbf{Z}[X]$，则 $f(X)$可分解为 $\mathbf{Q}[X]$中 $r,s(\neq 0)$次多项式的乘积当且仅当 $f(X)$可分解为 $\mathbf{Z}[X]$中 r,s 次多项式之积.

定理 1.18 $\mathbf{Z}[X]$是唯一析因整环，即任一 $f(X)\in\mathbf{Z}[X]$可唯一表为若干素数和不可约的本原多项式之积.

定理 1.19 若整系数多项式 $f(X)=a_nX^n+\cdots+a_1X+a_0\in\mathbf{Z}[X]$有有理根$\frac{b}{a}\in\mathbf{Q}$，$(a,b)=1$，则 $a|a_n,b|a_0$.

定理 1.20(Eisenstein 判别法) 设

$$f(X)=a_nX^n+\cdots+a_1X+a_0\in\mathbf{Z}[X],$$

若有素数 p 使 $p\nmid a_n,p|a_i(i=0,\cdots,n-1),p^2\nmid a_0$，则 $f(X)$在$\mathbf{Q}[X]$中不可约.

定理 1.21 设 $f(X)\in\mathbf{Z}[X]$为首一多项式且 $f(X)$在 $\mathbf{F}_p[X]$中不可约，则 $f(X)$在$\mathbf{Z}[X]$中不可约.

定理 1.22 对称多项式总可唯一地表为初等对称多项式的多项式. 即对任意 n 元对称多项式 $f(X_1,\cdots,X_n)$总存在唯一的 n 元多项式 $\varphi(Y_1,\cdots,Y_n)$使得 $f(X_1,\cdots,X_n)=\varphi(\sigma_1,\cdots,\sigma_n)$.

1.2 解题方法介绍

1.2.1 表对称多项式 $f(X_1,\cdots,X_n)$为初等对称多项式的多项式 $\varphi(\sigma_1,\cdots,\sigma_n)$的方法

(1) 表 f 为齐次对称多项式之和：$f=f_n+f_{n-1}+\cdots+f_0$，先对每个 m 次齐次多项式 f_m 按下述步骤表出，再合而得 f 的表示.

(2) 设 f_m 首项为 $aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$，写出满足以下三条件的所有可能数组$(l_1,l_2,\cdots,l_n)$：

① $(i_1,i_2,\cdots,i_n)\geqslant(l_1,l_2,\cdots,l_n)$，

② $l_1\geqslant l_2\geqslant\cdots\geqslant l_n$，

③ $l_1+l_2+\cdots+l_n=m$.

(3) 令 $f_m(X_1,\cdots,X_m)=\sum\limits_{(i_1,\cdots,i_n)}A(l_1,\cdots,l_n)\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\cdots\sigma_n^{l_n}$，其中$(l_1,\cdots,l_n)$ 是满足(2) 中三个条件的数组，$A_{(l_1,\cdots,l_n)}$ 为待定系数.

(4) 取$(X_1,\cdots,X_n)$的若干特殊值(例如$(1,1,\cdots,1,0,0,\cdots,0)$)代入上式定出各系数 $A_{(l_1,\cdots,l_n)}$，即得出 f_m.

1.2.2 求 f,g 的首一最大公因式(f,g)及 Bezout 等式$(uf+vg=(f,g))$中 u,v 的方法

(1) 辗转相除求(f,g). 由带余除法可设

$f=q_1g+r_1$　　$\deg r_1<\deg g$

$g=q_2r_1+r_2$　　$\deg r_2<\deg r_1$

$r_1=q_3r_2+r_3$　　$\deg r_3<\deg r_2$

……　　……

$r_{s-2}=q_sr_{s-1}+r_3$　　$\deg r_s<\deg r_{s-1}$

$r_{s-1}=q_{s+1}r_s$

由定理 1.6 知有

$$(f,g)=(g,r_1)=\cdots=(r_{s-2},r_{s-1})=cr_s,$$

这里要特别注意 r_s 与(f,g)的关系，当 r_s 不是首一多项式时，它们相差一个倍数.

(2) 先找公式，再代入 q_i 算 u,v. 应该说求 u,v 使 $uf+vg=(f,g)$的思路大部分人是知道的，但许多人往往得不到正确的结果，其原因主要是从反解(或称回代)上述公式找 f,g 的关系中，一开始就用具体的多项式参加运算，结果越算越繁，眼花缭乱. 我们认为要分两步走：① 写出公式；② 再代具体的多项式. 下面以辗转相除三次得到最大公因式为例说明方法. 由

$$\begin{aligned}(f,g) &= c(r_3) = c(r_1 - q_3 r_2) = c[(f - q_1 g) - q_3(g - q_2 r_1)],\\ &= c[f - q_1 g - q_3(g - q_2(f - q_1 g))],\\ &= c(1 + q_2 q_3) f - c(q_1 + q_1 q_2 q_3 + q_3) g,\end{aligned}$$

所以 $$u = c(1 + q_2 q_3), \qquad v = -c(q_1 + q_1 q_2 q_3 + q_3).$$

再把辗转相除中的各 q_i 的表达式代入，即可求出 u,v.

1.3 习题与解答

1. 自然数全体 **N** 对加法是否成群？对乘法呢？

解 对加法不成群，因为无恒元，无逆元. 对乘法也不成群，因为有恒元为 1，但无逆元.

2. $(\mathbf{Z},+,\cdot)$是否为域？含 **Z** 的最小域是什么？为什么？

解 $(\mathbf{Z},+,\cdot)$不是域. 因为$(\mathbf{Z},+)$是 Abel 群，但$(\mathbf{Z},\cdot)$是半群(对乘法有恒元 1，但无逆元). 要有逆元必须有分数，所以含 **Z** 的最小域为 **Q**，这时$(\mathbf{Q},+)$为 Abel 群，$(\mathbf{Q}^*,\cdot)$为 Abel 群，且满足乘法对加法的分配律.

3. 举出$(\mathbf{Z},+)$中三个子群例子.

解 $\{2K \mid K\in\mathbf{Z}\}$，$\{3K \mid K\in\mathbf{Z}\}$；$\{4K \mid K\in\mathbf{Z}\}$.

4. 在 $\mathbf{F}_2$ 中计算：$(a+b)^2$，$(a-b)^4$，$(a+b)^{32}$ $(a,b\in\mathbf{F}_2)$.

解 因为在 $\mathbf{F}_2$ 中，任 $x\in\mathbf{F}_2$ 均有 $x^2=x$，$2x=0$.

所以 $$(a+b)^2 = (a+b),$$

$$(a-b)^4 = [(a-b)^2]^2 = (a-b)^2 = (a-b) = a+b,$$

$$(a+b)^{32} = (a+b)^{4\times4\times2} = (a+b).$$

这里用到$-\bar{1}=\bar{1}$.

注意 在一般的特征为 p 的域中，仅有 $px=0$，未必有 $x^p=x$(x 为域中任一元素)，只在 F_p 中有 $x^p=x$，因为 $\mathbf{F}_p^*$ 是乘法循环群.

5. 举出一些群，环，域的例子.

解 $(\mathbf{Z},+)$Abel 群；$(\mathbf{Z},+,\cdot)$是环；**Q**，**R**，**C** 等均是域.

$\mathbf{Z}/8\mathbf{Z}$ 中子集$\cup=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$是个群(乘法群)；

$\mathbf{Z}/5\mathbf{Z}$ 中子集$\{\bar{1},\bar{2},\bar{3},\bar{4}\}$是乘法群.

6. 分别找出 3，9，4，5，8，7，11，13 整除一个整数 n 的判则，并证明之.

解 **用 3 整除判则**：因为 $10\equiv1 \pmod 3$，所以设 $n=a_0+a_1\times10+\cdots+a_k\times10^k$，则

$$n \equiv a_0 + a_1 + \cdots + a_k \pmod 3,$$

所以 $$3 \mid n \rightleftharpoons 3 \mid \sum_{i=1}^{k} a_i .$$

用 9 整除判则：

因为 $$9 \mid n \rightleftharpoons n \equiv 0 \pmod 9$$

又因为 $$n = \sum_{i=0}^{k} a_i \times 10^i \equiv \sum_{i=0}^{k} a_i \pmod 9$$

所以 $$9 \mid n \rightleftharpoons 9 \mid \sum_{i=0}^{n} a_i .$$

用 4 整除判则：因为 $100 \equiv 0 \pmod 4$

所以 $$n \equiv a_0 + a_1 \times 10 \pmod 4,$$

故只要看末两位数字能否被 4 整除即可.

用 5 整除判则：因为 $10 \equiv 0 \pmod 5$，所以 $n \equiv a_0 \pmod 5$所以只要看个位数字能否被 5 整除.

用 8 整除判则：因为 $1000 \equiv 0 \pmod 8$

所以 $$n \equiv a_0 + a_1 \times 10 + a_2 \times 10^2 \pmod 8,$$

故只要看末三位数字能否被 8 整除.

用 7 整除判则：因为 $11 \times 7 \times 13 = 1001$，

所以 $$1000 \equiv -1 \pmod 7,$$

故 $$n = \sum_{i=1}^{k} a_i \times 10^i = \sum_{i=0}^{[k/3]} b_i \times 10^{3i} \equiv \sum_{i=0} b_i (-1)^i$$

$$= b_0 - b_1 + b_2 - b_3 - \cdots \pmod 7$$

即只要看把 n 从个位开始三位一组分组后得到的数字的代数和能否被 7 整除.

用 11 整除判则：因为 $10 \equiv -1 \pmod{11}$

所以 $$n = \sum_{i=0}^{k} a_i \times 10^i \equiv \sum_{i=0}^{k} a_i \times (-1)^i$$

$$= a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \pmod{11}$$

故只要看(从个位数)n 的奇数位数字的和与偶数位数字和的差能否被 11 整除.

用 13 整除判则：同 7，即对任整数 n，看 13 是否能整除 $b_0 - b_1 + b_2 - b_3 + \cdots$，其中 $b_i (i = 0, 1, 2, \cdots)$是把 n 从个位开始三位一组分组后得到的数字.

例 $n = 87654320$，则因为

$$n \equiv b_0 - b_1 + b_2 = 320 - 654 + 87 = -297 \pmod{13}$$

而 $13 \mid -247$，故 $13 \mid n$.

7. 证明 $641 \mid 2^{32} + 1$.

证明 方法 1. 因为 $641 = 2^6 \times 10 + 1 = 2^7 \times 5 + 1$

所以 $$-1 \equiv 2^7 \times 5 \pmod{641},$$

故 $$1 \equiv (2^7)^4 \times 5^4 = (2^7)^4 \times 625$$

$$\equiv (2^7)^4 (-2^4) = -2^{32} \pmod{641}$$

即 $$2^{32} + 1 \equiv 0 \pmod{641}$$

方法 2.　　$641=2^6\times10+1=2^7\times5+1$,

$$\begin{aligned}2^{32}+1&=2^4\times2^{28}+1=(15+1)(2^7)^4+1\\&=3\times(2^7)^3[5\times2^7+1]+(2^7)^4-3(2^7)^3+1\\&=3\times(2^7)^3[5\times2^7+1]+125(2^7)^3+1\\&=(5\times2^7+1)[3\times(2^7)^3+(5\times2^7)^2-5\times2^7+1],\end{aligned}$$

所以　　$641\mid 2^{32}+1$.

8. 域 $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$ 的特征是多少？计算 $(a+b)^{p^k}$ $(a,b\in\mathbf{F}_p)$.

解　因为　　$\mathbf{F}_p=\{\bar0,\bar1,\cdots,\overline{p-1}\}$,

$$\overbrace{\bar1+\bar1+\cdots+\bar1}^{p\text{个}}=\bar p=\bar0,$$

所以 $\mathbf{F}_p$ 的特征是 p；

又因为在 $\mathbf{F}_p$ 中，任 $x\in\mathbf{F}_p$，有 $x^p=x$，

所以　　$(a+b)^{p^k}=(a+b)^{p^{k-1}}=\cdots=a+b$.

9. 列出 $\mathbf{Z}/7\mathbf{Z}$ 和 $\mathbf{Z}/8\mathbf{Z}$ 的乘法表.

解

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

10. 把多项式形式 $f(X)\in\mathbf{F}_7[X]$ 化为降幂排列形式：

(1) $f(X)=(4X^3+2X+6)(3X^3-4X^2-3)$

$$\begin{aligned}&=12X^6-16X^5+6X^4-2X^3-24X^2-6X-18\\&=5X^6+5X^5+6X^4+5X^3+4X^2+X+3.\end{aligned}$$

(2) $f(X)=(3X^5+5X^3-2)(4X^4+6X+5)$

$$=5X^9+6X^7+4X^6+X^5+X^4+4X^3+2X+4.$$

11. $\frac{1}{3}+\frac{1}{5}X^{\frac12}+4X^5+\frac{1}{2}X^7$ 是否是 $\mathbf{Q}$ 上多项式？

解　因为不定元 X 的次数非全是自然数，所以不是 Q 上多项式.

12. 作 $f(X)$ 除以 $g(X)$ 的带余除法：

(1) $f(X)=X^5+4X^4+X^2+2X+3$，$g(X)=X-2$.

解

$$\begin{array}{c|cccccc} 2 & 1 & 4 & 0 & 1 & 2 & 3 \\ & & \frac{2}{6} & \frac{12}{12} & \frac{24}{25} & \frac{50}{52} & \frac{104}{107} \end{array}$$

所以　　$f(X)=g(X)(X^4+6X^3+12X^2+25X+52)+107.$

(2) $f(X)=X^n-1$, $g(X)=X-a.$

解　因为

$$\begin{aligned} f(X)&=X^n-a^n+a^n-1=g\cdot q+r \\ &=(X-a)(X^{n-1}+aX^{n-2}+\cdots+a^{n-1})+a^n-1. \end{aligned}$$

或直接做带余除法有

$$\begin{array}{c|cccccc} a & 1 & 0X^{n-1} & \cdots & \cdots & 0X & -1 \\ & & \frac{a}{a} & \frac{a^2}{a^2} & \cdots & \frac{a^{n-1}}{a^{n-1}} & \frac{a^n}{a^n-1} \end{array}$$

所以　　$f(X)=(X-a)(X^{n-1}+aX^{n-2}+\cdots+a^{n-1})+a^n-1.$

(3) $f(X)=X^6-1$, $g(X)=X^3+X+1.$

$$\begin{array}{r|l} X^3+X+1 & \begin{array}{cccccccc} X^6 & 0 & 0 & 0 & 0 & 0 & -1 \\ \hline X^6 & & X^4 & X^3 & & & & \\ \hline & & -X^4 & -X^3 & & & & -1 \\ & & -X^4 & & -X^2 & -X & & \\ \hline & & & -X^3 & +X^2 & +X & -1 & \\ & & & -X^3 & & -X & -1 & \\ \hline & & & & & X^2 & +2X & \end{array} \end{array} \quad X^3-X-1$$

所以　　$f(X)=(X^3+X+1)(X^3-X-1)+X^2+2X.$

或直接由因式分解式得

$$\begin{aligned} X^6-1=&(X^3+X+1)(X^3-X-1) \\ &+(X+1)^2-1 \end{aligned}$$

13. 求下列各对多项式的最大公因子及 Bezout 等式：

(1) $f(X)=X^5+X^4-5X^3-5X^2+4X+4$, $g(X)=X^4+X^3-17X^2-21X+36$

解　定理 1.6 提供了求最大公因子(f,g)的方法——**辗转相除**(见 1.2.2)，我们将在(3)题写出详细的除法竖式，这里只给出公式和各步答案.

$$\begin{aligned} f&=gq_1+r_1, \\ g&=r_1q_2+r_2, \\ r_1&=r_2q_3+r_3, \\ r_2&=r_3q_4. \end{aligned}$$

其中　　$q_1=X,\quad q_2=\frac{1}{12}X-\frac{1}{36},\quad q_3=-\frac{9\times12}{125}X+\frac{9\times16}{125\times5},$

$$q_4=-\frac{25}{9}\cdot\frac{25}{108}(5X+13),\ r_3=\frac{108}{25}(X-1).$$

所以　　$(f,g)=(X-1)=\frac{25}{108}r_3=\frac{25}{108}(r_1-(g-r_1q_2)q_3)$

$$=\frac{25}{108}[(f-gq_1)(1+q_2q_3)-gq_3]$$
$$=u(X)f(X)+v(X)g(X).$$

$$u(X)=\frac{25}{108}(1+q_2q_3)=-\frac{X^2}{60}+\frac{X}{100}+\frac{23}{100};$$

$$v(X)=-\frac{25}{108}(q_1(1+q_2q_3)+q_3)=\frac{X^3}{60}-\frac{X^2}{100}-\frac{3X}{100}-\frac{4}{75}$$

注意 这里在求 Bezout 等式时，是先导出 $u(X)$，$v(X)$的计算公式，然后代入 q_i 计算，这样较简单，不易错.

(2) $f(X)=3X^4-8X^2-3$，$g(X)=X^3-2X^2-3X+6$.

解 由辗转相除知

$$f=gq_1+r_1$$
$$g=r_1q_2$$

其中 $q_1=3X+6$；$q_2=\frac{1}{13}X-\frac{2}{13}$；$r_1=13(X^2-3)$. 于是得$(f,g)=(X^2-3)$，且有

$$(f,g)=(X^2-3)=\frac{1}{13}r_1=\frac{1}{13}f-\frac{1}{13}q_1g,$$

所以 $$u(X)=\frac{1}{13},\quad v(X)=-\frac{1}{13}(3X+6).$$

(3) $f(X)=X^4-2X^3-2X^2-2X-3$，$g(X)=X^3+6X^2+6X+1$.

	g	f	
$q_2=\frac{X}{40}+\frac{39}{40\times8}$	X^3+6X^2+6X+1	$X^4-2X^3-2X^2-2X-3$	$q_1=X-8$
	$X^3+\frac{9}{8}X^2+\frac{1}{8}X$	$X^4+6X^3+6X^2+X$	
	$\frac{39}{8}X^2+\frac{47}{8}X+1$	$-8X^3-8X^2-3X-3$	
	$\frac{39}{8}X^2+\frac{39\times9}{8\times8}X+\frac{39}{8\times8}$	$-8X^3-48X^2-48X-8$	
	$r_2=\frac{25}{64}X+\frac{25}{64}$	$r_1=40X^2+45X+5$ $=5(8X+1)(X+1)$	

所以 $$(f,g)=(X+1)=\frac{64}{25}r_2=\frac{64}{25}(-q_2f+(1+q_1q_2)g)$$
$$=\left(-\frac{8}{125}X-\frac{39}{125}\right)f+\frac{8}{125}\left(X^2-\frac{25}{8}X+1\right)g$$
$$=uf+vg.$$

14. (1) 求第 13 题中前 4 个多项式的最大公因子及 Bezout 等式.

解 记 13 题中前 4 个多项式分别为 f_1,g_1,f_2,g_2. 并记 13 题(1)，(2)的 Bezout 等式分别为

$$d_1(X)=(f_1,g_1)=(X-1)=w_1f_1+w_2g_1,$$

$$d_2(X)=(f_2,g_2)=(X^2-3)=w_3f_2+w_4g_2.$$

则由

$$d_2(X)=d_1(X)(X+1)-2=d_1q_1+r_1,$$

得

$$(d_1,d_2)=1=-\frac{1}{2}r_1=-\frac{1}{2}(d_2-d_1q_1)=\frac{1}{2}d_1q_1-\frac{1}{2}d_2,$$

把上述两个 Bezout 等式代入,得

$$\frac{1}{2}(w_1f_1+w_2g_1)q_1-\frac{1}{2}(w_3f_2+w_4g_2)=1.$$

所以

$$(f_1,g_1,f_2,g_2)=1,$$

且有 u_1,u_2,u_3,u_4 使

$$u_1f_1+u_2g_1+u_3f_2+u_4g_2=1$$

其中

$$u_1=\frac{1}{2}w_1q_1=-\frac{1}{120}X^3-\frac{1}{300}X^2+\frac{3}{25}X+\frac{23}{200},$$

$$u_2=\frac{1}{2}w_2q_1=\frac{1}{120}X^4+\frac{1}{300}X^3-\frac{1}{50}X^2-\frac{1}{24}X-\frac{2}{75},$$

$$u_3=-\frac{1}{2}w_3=-\frac{1}{26},$$

$$u_4=-\frac{1}{2}w_4=\frac{3}{26}(X+2).$$

(2) 求第 13 题中后 4 个多项式的最大公因子及 Bezout 等式.

解 记 13 题中后 4 个多项式分别为 f_1,g_1,f_2,g_2. 并记 13(1),(2)的 Bezout 等式分别为

$$d_1(X)=(f_1,g_1)=X^2-3=w_1f_1+w_2g_1, \tag{1}$$

$$d_2(X)=(f_2,g_2)=X+1=w_3f_1+w_4g_2, \tag{2}$$

则

因为

$$X^3-3=(X+1)(X-1)-2\longrightarrow d_1=(X-1)d_2+r_1$$

所以

$$(d_1,d_2)=1=-\frac{1}{2}d_1+\frac{1}{2}(x-1)d_2 \tag{3}$$

把(1),(2)代入(3)中,即得

$$-\frac{1}{2}\left(\frac{1}{13}f_1-\frac{3}{13}(X+2)g_1\right)$$

$$+\frac{1}{2}(X-1)\left[\left(-\frac{8}{125}X-\frac{39}{125}\right)f_2+\left(\frac{8}{125}X^2-\frac{1}{5}X+\frac{8}{125}\right)g_2\right]=1,$$

故

$$u_1=-\frac{1}{26};\quad u_2=\frac{3}{26}(X+2);\quad u_3=-\frac{4}{125}X^2-\frac{31}{250}X+\frac{39}{250};$$

$$u_4=\frac{4}{125}X^3-\frac{33}{250}X^2+\frac{33}{250}X-\frac{4}{125},\quad d(X)=1.$$

15. 试求 a 与 b 使 $X^2-2aX+2$ 整除 X^4+3X^2+aX+b.