代数学：数、矩阵、群、环、域、模、代数（第二版）

邓月，电子科技大学，基础与前沿研究院，941951631@qq.com

2022 年 10 月 29 日

核心内容总结自《近世代数》、《矩阵理论》、《最优化理论》等课程。若无特别说明，向量默认为列向量。《分析学：数学中的“空间感”》建立起了用算子理论等代数思维看待数学问题的意识，主要分为线性和非线性问题的分析。《代数学：矩阵、群、环、域、模、代数》进一步探讨其中的线性部分，将矩阵视为线性算子进行研究。“特殊的矩阵算子”中例如对称阵、Hermite 阵、正交阵、酉阵、单纯阵、正规阵、幂等阵等方阵算子，其自身良好的性质能够为问题的分析提供极大便利；“算子范数”研究矩阵算子的有界性，探究它们在 Banach 不动点理论等实际应用中的先决条件；“特征值估计、谱分解”也是算子谱理论中老生常谈的问题了，这里集中将谱理论反映在矩阵算子上；“广义逆”就像是自反性在矩阵算子的体现。此外，矩阵算子还延伸出其他的研究内容，如“矩阵算子的分解”、“矩阵算子级数”和“矩阵算子函数”等。如何利用矩阵算子的相关理论来研究优化问题 (如近似估计等) 是一大主题，这不仅是线性部分的用武之地，同时也是非线性部分 (例如嵌入定理、变分法等) 的用武之地。切记，始终用算子理论等代数的思维来理解这一篇章，且有意识地回归到《分析学：数学中的“空间感”》的相应内容中去。群、环、域等抽象代数能够帮助我们将对矩阵的理解更上一个台阶。为了更好地促成这一点，这里的关于抽象代数的例题都被尽量地联系到矩阵。如果说分析学是“鸟与青蛙”中的青蛙，那么我偏向于将代数学形象化为那只“鸟”。

“等价”（如：模运算、陪集、同构、同态）、“生成”这些化繁为简的思想真的特别棒，在科研中我们可以留意去探究如何运用这些思想来辅助我们解决难题。对于研究代数系统的结构，“子群（环或域等）”以及“生成元”起到了很关键的作用。通过同构等“等价”联系后，我们可以通过一个更容易被摸清的代数系统的结构来洞察另一个较为复杂的代数系统的结构。

主要参考资料：

【1】黄廷祝, 钟守铭，李正良. (2003). 矩阵理论. 高等教育出版社.

【2】胡冠章，王殿军. (2006). 应用近世代数. 清华大学出版社有限公司.

【3】张晓伟. 最优化理论及应用课件. 电子科技大学.

目录

1 基本概念

1.1 实数

实数分为有理数和无理数。有理数包括整数和分数，无理数是无限不循环小数。

理解：

由上面的分类可以看出：循环小数是有理数哟！因为它是分数。

1.2 幂集

设 A 是一个集合，由 A 的所有子集构成的集合称为 A 的幂集，记作 2^A。当 $|A|<\infty$ 时，2^A 的元素的个数正好是 $|2^A|=2^{|A|}$【1-8 的 25 题证明】。

拓展：

设 A,B 为两个非空集合，$\mathrm{map}\{A,B\}$ 表示 “A 到 B 的所有映射”，记作 B^A，且有 $|B^A|=|B|^{|A|}$。

1.3 二元运算、代数系统、二元关系

(1) 设 S 是一个非空集合，若有一个对应规则 f，对 S 中每一对元素 a 和 b 都规定了一个惟一的元素 $c\in S$ 与之对应，即 f 是 $S\times S\to S$ 的一个映射，则此对应规则就称为 S 中的一个**二元运算**；

(2) 设 S 是一个非空集合，若在 S 中定义了一种运算 $\cdot$（或若干种运算 $+,\cdot,\times$ 等），则称 S 是一个**代数系统**，简称**代数系**；

(3) 设 A,B 是两个集合，若规定一种规则 R，使对任何 $a\in A$ 和对任何 $b\in B$ 均可确定 a 和 b 是否适合这个规则，若适合这个规则，就说 a 和 b 有**二元关系** R，记作 aRb，否则记作 $aR'b$。

理解：

(1) 由定义可见，一个二元运算是基于特定的集合而言的，且必须满足 “封闭性” 和 “惟一性”。例如，在整数集合中，普通的加法和乘法都是二元运算。实数域上的全体可逆方阵集合中，矩阵乘法是一个二元运算，而矩阵加法不是二元运算；

(2) 初等代数、高等代数和线性代数都称为经典代数，它的研究对象主要是代数方程和线性方程组，近世代数又称为抽象代数，它的研究对象是代数系；

(3) 二元关系例如 “实数集合的小于等于”，“整数集合的整除关系” 都是二元关系。因为集合（可看成两个）中的元素之前都能够被确定是否适合这个规则。

1.4 等价关系、等价类、代表元、商集

(1) 设 $\sim$ 是集合 A 上的一个二元关系，满足以下条件：(a) 对任何 $a\in A$ 有 $a\sim a$；(b) 对任何 $a,b\in A$ 有 $a\sim b\Rightarrow b\sim a$；(c) 对任何 $a,b,c\in A$ 有 $a\sim b$ 和 $b\sim c\Rightarrow a\sim c$。则称 $\sim$ 为 A 中的一个**等价关系**。A 的子集 $\overline{a}=\{x|x\in A,x\sim a\}$ 是所有与 a 等价的元素的集合，称为 a 所在的一个**等价类**。a 称为这个等价类的**代表元**；

(2) 集合 A 对某个等价关系 $\sim$ 的所有等价类构成的集合，称为 A 关于 $\sim$ 的**商集**，记作 $A/\sim$，即 $A/\sim=\{\overline{a}|a\in A\}$【《应用近世代数》P21 的例题 1.3.7，求定义在全体 2 阶实矩阵集合商的二元关系 $A\sim B\Leftrightarrow \det A=\det B$ 的商集】。

理解：

(1) 别把等价关系理解的那么死板，不要下意识就认为是针对两个元素之间而言的，实际上应该理解成用一种规则把集合中的元素进行了 “聚类”，比如矩阵的 “相似关系”、“合同关系” 都是等价关系。等价关系的目的是用于分类，比如 $R^{3\times3}$ 的矩阵集合可按 $=0,1,2,3$ 分成 4 类；

(2) 商集可理解为 “压缩” 后的结果。

1.5 模 n 的同余关系、同余类、正则代表元

设 n 是一个取定的正整数，在 Z 中定义一个二元关系 $\equiv \pmod n$ 如下：$a \equiv b \pmod n \Leftrightarrow n|(a-b)$，这个二元关系称为模 n 的**同余关系**，a 与 b 模 n 同余是指 a 和 b 分别用 n 来除所得的余数相同。同余关系是一个等价关系，每一个等价类 $\overline{a} = \{x|x \in z, x \equiv a \pmod n\}$ 称为一个**同余类或剩余类**。例如，对同余关系 $\equiv \pmod 6$，有同余类 $\overline{0}, \overline{1}, ..., \overline{5}$，每一类的代表元不是惟一的，将其中每一类中最小非负整数的代表元命名为**正则代表元**。

理解：

同余关系有许多实际背景，例如，如果两个人的生肖相同，则它们的年龄模 12 同余；如果两个人都是星期一出生的，则他们活到今天的天数模 7 同余，等等。

1.6 划分

设 A 为非空集合，$A_\alpha(\alpha \in I)$ 为 A 的一些非空子集，其中 I 为子集 A_α 的脚标 α 构成的集合，若有 (1) $\bigcup_{\alpha \in I} A_\alpha = A$，(2) 当 $\alpha, \beta \in I$ 且 $\alpha \neq \beta$，有 $A_\alpha \bigcap A_\beta = \emptyset$，则称 $\{A_\alpha|\alpha \in I\}$ 为 A 的一个**划分或分类**。

理解：

(1) 直观上理解划分，就是把集合分得不重不漏。

(2) 等价关系与划分的联系：设 $\sim$ 为非空集合 A 中的一个等价关系，则等价类集合 $\{\overline{a}|a \in A\}$ 是 A 的一个划分；反之，A 的任何一个划分 $\{A_\alpha|\alpha \in I\}$ 决定了 A 中的一个等价关系【《应用近世代数》P21 证明】。

1.7 偏序、偏序集、全序、全序集、Hesse 图、覆盖、极大 (小) 元、上 (下) 界、最小上界、最大下界

(1) 设 S 是一个集合，$\leq$ 是 S 中一个二元关系满足：(a) 对任何 $x \in S$ 有 $x \leq x$，(b) 对任何 $x, y \in S$ 若有 $x \leq y$ 且 $y \leq x$ 则 $x = y$，(c) 对任何 $x, y, z, \in S$ 若有 $x \leq y$ 且 $y \leq z$ 则 $x \leq z$，则称 $\leq$ 是 S 中的一个**偏序**，S 称为**偏序集**，记作 $(S, \leq)$。(d) 若对任何 $x, y \in S$ 均有 $x \leq y$ 或 $y \leq x$，则称 $\leq$ 为 S 中的一个**全序**，$(S, \leq)$ 称为一个**全序集**；

(2) 可以用 **Hesse 图**来表示一个偏序集。例如 $S = \{1, 2, 3, 4, 5, 6\}$，$\leq$ 为整除关系。S 中每一个元素对应图中的一个点。若 $x < y$ 且不存在 $u \in S$ 使 $x < u < y$，则称 y **覆盖** x。当 y 覆盖 x 时，在图中点 y 与点 x 之间有一条边相连，且点 y 在点 x 的上方。我们可以从任何一点开始按照规则画出所有的点和边。这样得到的图就是偏序集的 Hesse 图。全序集的 Hesse 图是一条竖链；

(3) (a) 设 $a \in S$，若对任何 $x \in S$ 均有 $x \leq a(x \geq a)$，则称 a 是 S 的**最大 (小) 元**。(b) 设 $a \in S$，若 $x \geq a(x \leq a) \Rightarrow x = a$，则称 a 是 S 中的一个**极大 (小) 元**。(c) 设 T 是 S 的一个子集，$a \in S$，若对任何 $x \in T$ 均有 $x \leq a(x \geq a)$，就称 a 是 T 的一个**上 (下) 界**，注意子集的上（下）界未必在此子集中。(d) 设 $T \subseteq S$，a 是 T 的一个上界，若对 T 的任意一个上界 a' 均有 $a \leq a'$，则称 a 是 T 的**最小上界**。类似有**最大下界**的概念。

理解：

(1) $\leq$ 可定义为 “大 (小) 于等于”、“(被) 包含于”、“整除” 等关系。要会判断一个代数系是不是偏序集或全序集，如 $(2^A, \subseteq)$ 是偏序集但不是全序集，$(Z^+, |)$ 是偏序集但不是全序集 (其中 | 表示整除关系)，$(Z^+, \leq)$ 是全序集。偏序集与全序集的区别只是在于，在全序集中任何两个元素均有序的关系，而在偏序集中则不一定；

(2) 区分 “最大 (小) 元” 和 “上（下）界”，前者是对于整个集合而言的，后者是对于集合中的子集而言的。并且这里的 “极大” 与函数值的极大是不一样的，“极小” 也是哟。

1.8 良序集

设 A 为全序集，若 A 的任何非空子集都有最小元，则称 A 为**良序集**。

理解：

（1）对于一个集合，它是否是良序集取决于是否可以定义，以及怎么去定义二元关系 $\leq$。例如，正整数集 Z^+ 是良序集，可将二元关系定义为小于或等于【《应用近世代数》P23 证明】。而整数集合 Z 对普通的数的大小不是良序的，但可以对 Z 重新规定序使其成为良序集。

（2）良序集的概念非常重要，由它可以引出数学归纳法原理和超限归纳法原理，具体见“应用”章节。

（3）深化对“区间”的理解：集合按照某种偏序的关系进行排序，所形成的集合就是**半区间**。将**紧凑的**（不紧凑的意思是说我们能在一个按照偏序排序的集合的两个元素之间找到另一个不属于该集合的元素，比如整数集之于实数集，整数集就是不紧凑的。由此可见，全集必然是一个紧凑集）半区间称为**区间**。

1.9 最大公因子、最小公倍数

设 $a,b\in Z$，不全为 0，它们的正最大公因子记作 (a,b)，正最小公倍数记作 $[a,b]$。

性质：

$ab=(a,b)\cdot[a,b]$【《应用近世代数 P25-26 证明》，用“存在表示定理”把 $(a,b),[a,b]$ 表示出来】。

拓展：

多项式的最大公因子 (gcd)，$\forall f(x),g(x)\in R(x),\exists d(x)$，且首项系数为 1，使得(a)$d(x)|f(x),d(x)|g(x)$;(b)$\overline{d(x)}|f(x),\overline{d(x)}|g(x)\Rightarrow\overline{d(x)}|d(x)$。

1.10 互素、Euler 函数

若 $a,b\in Z$ 满足 $(a,b)=1$，则称 a 与 b **互素**。

性质：

（1）$(a,b)=1\Leftrightarrow\exists p,q\in Z$ 使 $pa+qb=1$；

（2）$a|bc$ 且 $(a,b)=1\Rightarrow a|c$；

（3）设 $a,b\in Z$，p 为素数，则有 $p|ab\Rightarrow p|a$ 或 $p|b$；

（4）$(a,b)=1,(a,c)=1\Rightarrow(a,bc)=1$；

（5）$a|c,b|c$ 且 $(a,b)=1\Rightarrow ab|c$；

（6）**Euler 函数：**设 n 为正整数，$\varphi(n)$ 为小于 n 并与 n 互素的正整数的个数。若 n 的标准分解式为 $n=p_1^{\varepsilon_1}p_2^{\varepsilon_2}...p_s^{\varepsilon_S}$，则 $\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_S})$。【1-8 的 26 题证明】

（上述性质中，1,3,6 最为重要，尤其是 6）

性质：

$\varphi(mn)=(mn)\cdot\varphi([m,n])$。它的功能是：当 m,n 互素，即 $(m.n)=1$ 时，则有 $\varphi(mn)=\varphi(m)\cdot\varphi(n)$。【1-9 的 27 题证明】

1.11 一次同余方程

设 $a,b\in Z,m\in Z^+$，则 $ax\equiv b\pmod m,a\not\equiv 0\pmod m$ 称为模 m 的**一次同余方程**，或简称为一次同余式。

理解：

含义就是：用 ax 与 b 去模 m，所得的余数相同。

1.12 谱、行列式、特征多项式、代数重数、几何重数、Jordan 标准型、Jordan 块、可对角化矩阵

设方阵 $A\in C^{n\times n}$：

(1)A 的所有特征值的全体叫做 A 的**谱**，记作 $\lambda(A)$；

(2) 因为下面的概念中要用到行列式，所以这里先重申行列式中几条重要的性质：（a）当矩阵的两行进行交换后，行列式改变符号；（b）在矩阵的消元的过程中，行列式不会改变；（c）当矩阵的某一行全为零或有两行一样时，行列式为零；（d）如果矩阵 A 可逆，那么 $\det A\neq 0$，反之，$\det A=0$；（e）$\det AB=\det A\det B$；（f）$\det A^T=\det A$；（g）$\det(A^{-1})=(\det A)^{-1}$。（特别注意下后 4 个性质）

(3)$f(\lambda)=\det(\lambda E-A)$ 叫做 A 的**特征多项式**；

(4) 如果 A 有 r 个不同的特征值 $\lambda_1,\lambda_2,...,\lambda_r$，其重数分别为 $n_1,n_2,...,n_r$，则 $f(\lambda)=(\lambda-\lambda_1)^{n_1}(\lambda-\lambda_2)^{n_2}...(\lambda-\lambda_r)^{n_r}$，$\sum_{i=1}^{r}n_i=n$，其中 n_i 叫做 λ_i 的**代数重数**；

(5) 如果 $\text{rank}(\lambda_i E-A)=n-m_i$，则 m_i 叫做 λ_i 的**几何重数**，它表示 A 的属于 λ_i 的线性无关特征向量的个数。

(6) 对于任意 A，都存在可逆矩阵 $P\in C^{n\times n}$，使得 $P^{-1}AP=J=\text{diag}(J_1(\lambda_1),...,J_r(\lambda_r))$，矩阵 J 叫做 A 的 **Jordan 标准型**。其中 $\lambda_1,\lambda_2,...,\lambda_r$ 不一定不相同；

(7) 其中 $J_i(\lambda_i)=\begin{pmatrix}\lambda_i & 1 & & \\ & \cdots & \cdots & \\ & & \lambda_i & 1\\ & & & \lambda_i\end{pmatrix}$ 叫做一个 **Jordan 块**；

(8) 如果存在可逆矩阵 $P\in C^{n\times n}$，使得 $P^{-1}AP=\text{diag}(\lambda_1,...,\lambda_n)$，则 A 叫做**可对角化矩阵**。

性质：

(1) 代数重数刻画特征值，几何重数刻画特征向量，且有 $1\le m_i\le n_i\le n$ 【1-1 的 1 题证明】；

(2) 不同特征值对应的特征向量线性无关【1.1 的 2 题证明】。也就是说，即便有一些特征值可能会分别对应一组含多个线性无关的特征向量 (几何重数大于 1 的情况)，这些组之间也是线性无关的；

(3) 关于 Jordan 矩阵的几个结论：(a)Jordan 块的个数 r 是线性无关特征向量的个数 (即包括相同特征值所对应的 m_i 个线性无关特征向量个数，以及不同特征值间线性无关特征向量个数，总之它们之间都是相互线性无关的)；(b) 对应于同一特征值的 Jordan 块的个数是该特征值的几何重数，它是相应的特征子空间的维数；(c) 对应于同一特征值的所有 Jordan 块的阶数之和是该特征值的代数重数。

(4) 关于可对角化矩阵，矩阵可对角化当且仅当 Jordan 块中有 $r=n$ 成立。且下列命题等价：(a)A 是可对角化矩阵；(b)C^n 存在由 A 的特征向量构成的一组基底【1-1 的 3 题体会】；(c)A 的标准形式中的 Jordan 块都是一阶的；(d)$m_i=n_i,i=1,2,...,r$。

(5) 对于三阶以上的行列式就要用代数余子式的展开形式来算（且注意！伴随矩阵如果按照正常位置来排列和计算，最后别忘了转置！不过这样也更好，先按原始位置来算，不容易弄晕，最后再转置一下，达到相同的效果！)。

理解：

(1) 关于矩阵特征值和特征向量的问题，前提是矩阵要是一个方阵；

(2) 如 1 和 2 所述，要得到一个矩阵的各特征值的代数重数和几何重数，不仅可以先用特征多项式一一求出矩阵的谱，再一一带入 $\text{rank}(\lambda_i E-A)=n-m_i$ 求出 m_i，还可以通过对矩阵求出对应的 Jordan 标准型来观察结构特征而得到；

(3) 相似对角化有大用处。在大规模科学计算问题中，如果要对一个矩阵求 n 次幂，则可以先将其进行相似对角化得到一个相应的对角矩阵，因此最终可以将对矩阵求 n 次幂的问题转换为对该对角矩阵的对角线元素求 n 次方，因为展开后可发现除两头外的中间部分的可逆矩阵通过 $P^{-1}P=E$ 全消掉了。

1.13 广义特征值、广义特征向量

设 $A,B\in C^{n\times n}$，如果存在 $\lambda\in C$ 和非零向量 $x\in C^n$，使得 $Ax=\lambda Bx$，则称 λ 为矩阵 A 与 B 确定的广义特征值，x 称为与 λ 对应的广义特征向量。

性质：

求广义特征值的方法参见《矩阵理论》P15-16 及 P17 的定理 6，总共分为三种情形：$B=E$ 时、B 可逆时、A,B 都是 Hermite 矩阵时 (即 $A=A^H,B=B^H$，且 B 是正定的，这也是许多科技问题中最常遇到的)。

理解：

广义特征值和广义向量是基于实际问题而提出的，在优化问题中，例如优化目标是 $\min f(x)=x^{-1}Ax$，约束条件为 $x^TBx=1$，则利用拉格朗日乘子法可构造 $F(x,\lambda)=x^TAx-\lambda(x^TBx-1)$，通过 $\nabla F(x,\lambda)=0$ 寻找驻点，化简后得 $Ax=\lambda Bx$。实际上，广义特征值可以理解为拉格朗日乘子法中参数 λ 的最优设定；

1.14 初等矩阵

设 $u,v\in C^n,\sigma\in C$，则形如 $E(u;v;\sigma)=E_n-\sigma uv^H$ 的矩阵叫做初等矩阵。

性质：

(1) 特征向量 $(u,v\neq 0,\sigma\neq 0)$：设 $v^\perp$ 表示与 v 正交的 $n-1$ 维子空间，则 (a)$u\in v^\perp$，设 $u_1,...,u_{n-1}$ 是 $v^\perp$ 的一组基底，它们也是 $E(u;v;\sigma)$ 的 $n-1$ 个线性无关的特征向量；(b)$u\notin v^\perp$，设 $u_1,...,u_{n-1}$ 是 $v^\perp$ 的一组基底，则 $u,u_1,u_2,...,u_{n-1}$ 是 $E(u;v;\sigma)$ 的 n 个线性无关的特征向量；

(2) 特征值：$\lambda(E(u;v;\sigma))=\{1,1,...,1,1-\sigma v^Hu\}$；

(3) 行列式：$\det(E(u;v;\sigma))=1-\sigma v^Hu$；

(4) 逆：$E(u;v;\sigma)^{-1}=E(u,v,\dfrac{\sigma}{\sigma v^Hu-1})$，其中 $1-\sigma v^H\neq 0$；

(5) 非零向量 $a,b\in C^n$，存在 u,v,σ，使得 $E(u,v,\sigma)a=b$，其中 $\sigma u=\dfrac{a-b}{v^Ha}$。

理解：

初等矩阵实际上可以视为单位矩阵发生了一个秩为 1 的扰动后所得到的形式，其中 $\mathrm{rank}(uv^H)\leq\min\{\mathrm{rank}(u),\mathrm{rank}(v)\}=1$。不难验证，所有初等变换矩阵都可以表示成 $E(u;v;\sigma)$ 的形式，参见《矩阵理论》P20。

1.15 初等酉阵 (或 Householder 变换)

设 $u\in C^n$，且 $u^Hu=1$，则 $H(u)=E(u,u;2)=E_n-2uu^H$ 称为初等酉阵（或 Householder 变换）。

性质：

(1)$H(u)^H=H(u)=H(u)^{-1}$，也就是说，初等酉阵为 Hermite 矩阵、酉矩阵和对合矩阵；

(2)$\det H(u)=-1,H(u)=U\begin{pmatrix}-1&&&\\&1&&\\&&...&\\&&&1\end{pmatrix}U^H$，其中 U 为酉阵；

(3)$H(u)$ 是镜像变换，即 $H(u)(a+ru)=a-ru$；

(4) 设 $a,b\in C^n$，则存在单位向量 u，使得 $H(u)a=b$ 的充要条件是 $\|a\|_2=\|b\|_2$ 和 $a^Hb=b^Ha$（《矩阵理论》P21-22 证明）；

(5) $(H(u)x,H(u)y)=(x,y)$，保持内积不变，即保持变换前后的长度和夹角不变；

(6) $\|H(u)x\|=\|x\|$。

理解：

(1) 可以把“镜像变换”这一性质理解为物理学中的入射光与反射光对称，即这里的横轴为 u，纵轴为 a；

(2) 性质 6 的作用之一可以简化范数的计算，因为有时候 $\|x\|$ 可能因为比较复杂而难以直接分析，因此可以先用 Householder 变换来预处理 x，使它的形式更简洁一些。

1.16 Gram 矩阵、Gram 行列式、度量矩阵

设 V 是一个内积空间，$\alpha_1,\alpha_2,...,\alpha_k\in V$，称 $A(\alpha_1,\alpha_2,...,\alpha_k)=\begin{pmatrix}(\alpha_1,\alpha_1)&(\alpha_1,\alpha_2)&...&(\alpha_1,\alpha_k)\\(\alpha_2,\alpha_1)&(\alpha_2,\alpha_2)&...&(\alpha_2,\alpha_k)\\...&...&...&...\\(\alpha_k,\alpha_1)&(\alpha_k,\alpha_2)&...&(\alpha_k,\alpha_k)\end{pmatrix}$，相应地，$G(\alpha_1,\alpha_2,...,\alpha_k)=\det A(\alpha_1,\alpha_2,...,\alpha_k)$ 称为 Gram 行列式。进一步，如果 $\{\alpha_i\}$ 是 V 的一组基底，那么生成的 Gram 矩阵同时还是可逆、正定的，称为度量矩阵。

性质：

(1) $\alpha_1,\alpha_2,...,\alpha_k$ 线性相关 $\Leftrightarrow A(\alpha_1,\alpha_2,...,\alpha_k)$ 奇异 (不可逆)$\Leftrightarrow G(\alpha_1,\alpha_2,...,\alpha_k)=0$；

(2) $\alpha_1,\alpha_2,...,\alpha_k$ 线性无关，则将向量 $\alpha_1,\alpha_2,...,\alpha_k$ 正交化后，它的 Gram 行列式不变，即 $G(\alpha_1,\alpha_2,...,\alpha_k)=G(\beta_1,\beta_2,...,\beta_k)=\|\beta_1\|^2\|\beta_2\|^2...\|\beta_k\|^2$。

理解：

度量矩阵可用于将内积运算转换成为矩阵运算。

1.17 实对称矩阵、Hermite 矩阵

若实矩阵 $A \in R^{n\times n}$ 满足 $A = A^T$, 则称 A 为实对称矩阵。类似地, 若复矩阵 $A \in C^{n\times n}$ 满足 $A = A^H$, 则称 A 为 Hermite 矩阵。

性质:

Hermite 矩阵 $A \in C^{n\times n}$ 满足如下性质:

(1) Hermite 矩阵的特征值都是实数，反 Hermite 矩阵的特征值都是纯虚数;

(2) 并且存在由 n 个单位特征向量构成的标准正交基底;

(3) 可相似对角化，并且过渡矩阵是一个正交矩阵。

理解:

(1) 对于性质 (2)，因为 Hermite 矩阵是正规矩阵，由正规矩阵的充要条件 “可酉相似于一个 n 阶对角矩阵，其元素为该 Hermite 矩阵的特征值”，以及 “不同特征值对应的特征向量线性无关” 可得此结论。

1.18 正交矩阵、酉矩阵

若实矩阵 $A \in R^{n\times n}$ 满足 $A^TA = E$，则称 A 为正交矩阵。类似地，若复矩阵 $A \in C^{n\times n}$ 满足 $A^HA = E$，则称 A 为酉矩阵。

性质:

(1) 酉矩阵 U 的逆 U^{-1} 也是酉矩阵;

(2) 两个酉矩阵之积 U_1U_2 也是酉矩阵;

(3) 酉矩阵的任一特征值的模均等于 1。

理解:

从定义中可以看出，元素是被标准化后的。

1.19 幂等矩阵

若 $A \in C^{n\times n}$ 满足 $A^2 = A$，则称 A 为幂等矩阵。

性质:

(1)A^H 与 $(E - A)$ 也是幂等矩阵;

(2)A 的特征值非零即 1，且可对角化【1-1 的 3 题证明】;

(3)$\text{rank}(A) = \text{tr}(A)$【1-1 的 3 题证明】;

(4)$A(E - A) = (E - A)A = 0$;

(5)$A\alpha = \alpha \Leftrightarrow \alpha \in R(A)$;

(6)$N(A) = R(E - A), R(A) = N(E - A)$;

(7)$C^n = R(A) \oplus N(A)$。

理解:

性质 (7) 是由如下定理得到的: 设 $A \in C^{m\times n}$，则 (1)$\dim R(A) + \dim N(A^H) = m$; (2)$\dim R(A^H) + \dim N(A) = n$; (3)$C^m = R(A) \oplus N(A^H)$; (4)$C^n = R(A^H) \oplus N(A)$。

1.20 Frobenius 范数、极大列和范数、谱范数、极大行和范数

(1) Frobenius 范数定义为 $\|A\|_{m_2}$;

(2) 极大列和范数定义为 $\|A\|_1 = \max\limits_j \sum\limits_{i=1}^{n} |a_{ij}|$，它是从属于 $\|x\|_2$ 的算子范数;

(3) 谱范数定义为 $\|A\|_2 = \sqrt{r(A^HA)}$，它是从属于 $\|x\|_2$ 的算子范数。其中谱半径 $r(A) = \max_i |\lambda_i|$;

(4) 极大行和范数定义为 $\|A\|_\infty = \max\limits_i \sum\limits_{j=1}^{b} |a_{ij}|$，它是从属于 $\|x\|_\infty$ 的行和范数。

性质:

(1) Frobenius 范数具有如下性质：

设 $A \in K^{n\times n}$，则有以下等式成立：(a) 若 $A=(\alpha_1,\alpha_2,...,\alpha_n)$，则 $\|A\|_F^2=\|A\|_{m_2}^2=\sum_{i=1}^{n}\|\alpha_i\|_2^2$，其中 $\|\alpha_i\|_2^2=\alpha_i^H\alpha_i$ 是 K^n 中的向量范数；(b) $\|A\|_{m_2}^2=\mathrm{tr}(A^HA)=\sum_{i=1}^{n}\lambda_i(A^HA)$ 【2-2 的 4 题证明】；(c) 对任意的酉矩阵 $U,V\in K^{n\times n}$，有 $\|A\|_{m_2}=\|U^HAV\|_{m_2}=\|UAV^H\|_{m_2}$。由此还可推出：$\|A\|_{m_2}=\|UA\|_{m_2}=\|AV\|_{m_2}=\|UAV\|_{m_2}$。(《矩阵理论》P60 证明)

(2) 算子范数具有如下性质：

(a) 算子范数是相容的矩阵范数；(b)$\|A\|_a=\max_{x\neq0}\frac{\|Ax\|_a}{\|x\|_a}$ 是与 $\|x\|_a$ 相容的矩阵范数；(c) 算子范数 $\|A\|_a$ 是所有与 $\|x\|_a$ 相容的矩阵范数中最小的一个；(d)$\|E\|_a=\max_{x\neq0}\frac{\|Ex\|_a}{\|x\|_a}=1$ (该性质提供了一个快速判断是否为算子范数的方法，即：如果一个范数作用在单位矩阵上不等于 1，则它不是算子范数)。

(3) 谱范数具有如下性质:

设 $A\in C^{n\times n}$，则：(a) $\|A\|_2=\|A^H\|_2=\|A^T\|_2=\|\overline{A}\|_2$；(b) $\|A^HA\|_2=\|AA^H\|_2=\|A\|_2^2$；(c) 对任何 n 阶酉阵 U 及 V 都有 $\|UA\|_2=\|AV\|_2=\|UAV\|_2=\|A\|_2$；(d) $\|A\|_2=\max_{\|x\|_2=\|y\|_2=1}|y^HAx|$；(e) $\|A\|_2^2\leq\|A\|_1\|A\|_\infty$。

理解：

(1) 注意区分谱函数和 Frobenius 范数，虽然同为 “2”，但含义是完全不同的；

(2) 谱范数在实际应用中不便于计算，但它具有许多良好的性质，在理论推导中经常使用。

1.21 条件数

设 A 是可逆矩阵，称 $K_p(A)=\|A\|_p\|A^{-1}\|_p$ 是矩阵 A 相对矩阵范数 $\|\cdot\|_p$ 的条件数。

性质：

设 $A\in C^{n\times n},\|A\|_a$ 是从属于向量范数 $\|x\|_a$ 的算子范数，则当 $\|A\|_a<1$ 时，$E-A$ 是可逆的，且 $\|(E-A)^{-1}\|_a\leq(1-\|A\|_a)^{-1}$ 成立【3-3 的 13 题证明】。

理解：

条件数给出了由于摄动而引起结果的变化的灵敏度的度量，它在矩阵逆的摄动、线性方程组的摄动分析中有应用，见《矩阵理论》P76 起。为了保证下界不会太小，因此条件数对应的矩阵范数一般采用算子范数。

1.22 正线上三角复 (实) 矩阵、单位上三角复 (实) 矩阵、正线下三角复 (实) 矩阵、单位下三角复 (实) 矩阵：

如果 $a_{ii}(i=1,2,...,n)$ 均为正实数，$a_{ij}\in C(R)(i<j,i=1,2,...,n-1;j=i+1,i+2,...,n)$，则上三角矩阵 $R=\begin{pmatrix}a_{11}&a_{12}&...&a_{1n}\\0&a_{22}&...&a_{2n}\\...&...&...&...\\0&0&...&a_{nn}\end{pmatrix}$ 称为正线上三角复 (实) 矩阵 R，特别地当 $a_{ii}=1$ 时，称为单位上三角复 (实) 矩阵 R^*。类似地，下三角矩阵 $L=\begin{pmatrix}a_{11}&0&...&0\\a_{21}&a_{22}&...&0\\...&...&...&...\\a_{n1}&a_{n2}&...&a_{nn}\end{pmatrix}$ 称为正线下三角复 (实) 矩阵 L，特别地当 $a_{ii}=1$ 时，称为单位下三角复 (实) 矩阵 L^*。

性质：

(1) 上三角矩阵 R 的逆 R^{-1} 也是上三角矩阵，且对角元是 R 对角元的倒数；

(2) 两个上三角矩阵 R_1,R_2 的乘积 R_1R_2 也是上三角矩阵，且对角元是 R_1 与 R_2 对角元之积。

1.23 代数重复度、几何重复度、单纯矩阵

(1) 设 $\lambda_1, \lambda_2, ..., \lambda_k$ 是 $A \in C^{n\times n}$ 的 k 个相异特征值，其重数分别为 $r_1, r_2, ..., r_k$，则称 r_i 为矩阵 A 的特征值 λ_i 的代数重复度。齐次方程组 $Ax = \lambda_i x$ 的解空间 V_{λ_i} 称为 A 对于特征值 λ_i 的特征子空间，而 V_{λ_i} 的维数称为 A 的特征值 λ_i 的几何重复度。

(2) 单纯矩阵 "A 的每个特征值的代数重复度与几何重复度相等"（等价于："A 可相似对角化"（此时相似对角化后的 J 就是一个 λ 为一块）或 "A 有 n 个线性无关的特征向量"）。

性质：

从谱分解的角度看，设 $A \in C^{n\times n}$ 有 k 个相异特征值 λ_i，那么 A 是单纯矩阵的充要条件是存在 k 个矩阵 A_i 满足：(a) $A_iA_j = \begin{cases} A_i & j = i, \\ O & j \neq i. \end{cases}$；(b)$\sum_{i=1}^{k} A_i = E_n$；(c)$A = \sum_{i=1}^{k} \lambda_i A_i$。（《矩阵理论》P98 证明）

1.24 正规矩阵

若 n 阶复矩阵 A 满足 $AA^H = A^HA$，则称 A 为正规矩阵。当 A 为 n 阶实矩阵且满足 $AA^T = A^TA$，则称矩阵 A 是实正规矩阵。

常见的正规矩阵包括：对角矩阵、酉矩阵、Hermite 矩阵 ($A = A^H$)、反 Hermite 矩阵 ($A = -A^H$)；正交矩阵、实对称矩阵、实反对称矩阵都是实正规矩阵；正规矩阵并不一定是 Hermite 矩阵。

性质：

(1) 设 A 是正规矩阵，A 与 B 酉相似，则 B 也是正规矩阵；（【1-8 的 24 题】）

(2) 设 A 是三角矩阵，则 A 是正规矩阵的充要条件是 A 是对角矩阵。（【1-8 的 24 题】）

(3) n 阶复矩阵 A 是正规矩阵的充要条件是 A 与对角矩阵酉相似，即存在 n 阶酉矩阵 U，使得 $A = U(\lambda_1, \lambda_2, ..., \lambda_n)U^H$，其中 $\lambda_1, \lambda_2, ..., \lambda_n$ 是 A 的 n 个特征值（没说互异）。（《矩阵理论》P102 证明）

(4) 从谱分解的角度看，A 是正规矩阵的充要条件，除 12 中性质里的 3 个条件外，还需满足 $A_i^H = A_i (i = 1, 2, ..., k)$。（《矩阵理论》P102 证明）

理解：

性质 (3) 特别关键，用 schur 分解和性质 (1-2) 即可得证。该性质在许多证明过程中起开端的作用。

1.25 拉普拉斯矩阵，归一化的拉普拉斯矩阵

（1）对于一个简单图 G，其拉普拉斯矩阵为 $L = D - A$，其中 D 为度对角矩阵，A 为邻接矩阵（对于无向图的邻接矩阵，其对角线元素为 0）。拉普拉斯矩阵的第 i 行是第 i 个节点产生扰动时对其它节点产生的收益累积。至于如何理解这一点？

首先对一个二元的连续函数 $f(x, y)$ 求梯度，得 $\nabla f = \frac{\partial f}{\partial x}\vec{i} + \frac{\partial f}{\partial y}\vec{j}$，$f$ 的拉普拉斯算子就是其梯度的散度，为 $\Delta f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2}$。其对应的离散形式为 $\Delta f = f(x+1, y) + f(x-1, y) + f(x, y+1) + f(x, y-1) - 4f(x, y)$。可见，是微小扰动后获得的收益。

将上述结论推广到图上，对于图 G，有 n 个节点，每个节点 i 的函数值为 f_i，邻域为 N_i，则对节点 i 进行微扰后，i **可能变成邻域内的任意一个节点** (好好理解和把握这句话！)，有 $\Delta f_i = \sum_{j\in N_i} w_{ij}(f_i - f_j)$，其中 w_{ij} 是节点 i 和 j 之间连边的权重。将上式展开有 $\Delta f_i = \sum_{j\in N_i} w_{ij} f_i - w_{i:} f$。推广到所有节点，有 $\Delta f = (A - D)f = -Lf$。

（2）归一化拉普拉斯算子有两种方式：

第一，**对称归一化的拉普拉斯矩阵 (Symmetric normalized Laplacian)**：$L^{sym} = D^{-\frac{1}{2}}LD^{-\frac{1}{2}} = I - D^{-\frac{1}{2}}AD^{-\frac{1}{2}} = U\Lambda U^T$,with a diagonal matrix of its eigenvalues Λ and U^Tx being the graph Fourier transform of x。比较拉普拉斯矩阵和对称归一的拉普拉斯矩阵的元素。它具有如下性质：(a) 特征值都是 non-negative 和 real 的【证明参见维基百科的 Laplacian matrix 专题】。(b) One has: $L^{sym} = SS^*$, where S is the matrix whose rows are indexed by the vertices and whose columns are indexed by the edges of G

such that each column corresponding to an edge $e = \{u, v\}$ has an entry $\frac{1}{\sqrt{d_u}}$ in the row corresponding to u, an entry $-\frac{1}{\sqrt{d_v}}$ in the row corresponding to v, and has 0 entries elsewhere。

第二，**Random walk normalized Laplacian**：$L^{rw} = D^{-1}L = I - D^{-1}A$。

关于 L^{sym}, L^{rw} 的更多的**若干性质**可参见知乎链接：https://zhuanlan.zhihu.com/p/362416124。

至于为什么要将拉普拉斯矩阵归一化，可以参见回答链接：https://www.quora.com/In-practice-what-are-the-differences-between-the-Laplacian-and-the-normalized-Laplacian-of-a-graph。

图的傅里叶变换：

As a **connected** N nodes graph G's Laplacian L is a real symmetric matrix, it has a complete set of orthonormal eigenvectors. We denote these by χ_l for $l = 0, ..., N-1$, with associated eigenvalues λ_l such that $L\chi_l = \lambda_l\chi_l$ and $0 = \lambda_0 \leq \lambda_1 \leq ... \leq \lambda_{N-1}$, where each of them is real, out of the property of a real symmetrix matrix 【参见1.17节】. For any function $f \in \mathbb{R}^N$ （这儿的意思应该是将 N 个节点分别映射到 $\mathbb{R}$ 上）defined on the vertices of G, its Fourier transform $\hat{f}$ is defined by $\hat{f}(l) = \langle \chi_l, f \rangle = \sum_{n=1}^{N} \chi_l^*(n) f(n)$（还可以写成矩阵形式，$\hat{f} = U^T f$，即向量 = 矩阵 * 向量，这样更容易理解图卷积公式）。The inverse transform is defined by $f(n) = \sum_{l=1}^{N-1} \hat{f}(l)\chi_l(n)$。

Analogously to the classical Fourier transform, graph Fourier transform provides a way to represent a signal in two different domains: the vertex domain and the graph spectral domain. Note that the definition of the graph Fourier transform and its inverse depend on the choice of Laplacian eigenvectors, which are not necessarily unique. The eigenvectors of the normalized Laplacian matrix are also a possible base to define the forward and inverse graph Fourier transform.

理解：

（1）加深对拉普拉斯矩阵和拉普拉斯算子的理解。比如，拉普拉斯矩阵是拉普拉斯算子在图上的离散形式，并且：For the Euclidean space, the Laplace operator is the divergence of the gradient of a function。以及，The Laplace operator measures how much a function differs at a point from the average of the values of the function over small spheres centered at that point。再比如：卡拉普拉斯矩阵的特征值和特征向量的直观含义等等。更多参见链接：https://www.quora.com/In-practice-what-are-the-differences-between-the-Laplacian-and-the-normalized-Laplacian-of-a-graph。

1.26 正奇异值

设 $A \in C_r^{m \times n}$，$A^H A$ 的特征值为 $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_r > \lambda_{r+1} = ... = \lambda_n = 0$，则称 $\sigma_i = \sqrt{\lambda_i}(i = 1, 2, ..., r)$ 为矩阵 A 的正奇异值。

性质：

设 $A \in C^{m \times n}$，则有:

(1)$\text{rank}(A) = \text{rank}(A^H A) = \text{rank}(AA^H)$【1-2 的 4 题证明】;

(2)$A^H A, AA^H$ 的特征值均为非负实数【2-3 的 9 题体会】;

(3)$A^H A$ 与 AA^H 的非零特征值相同（《矩阵理论》P118 证明）。

理解：

之所以用 $A^H A$ 或 AA^H 的形式，是因为这俩都是正规矩阵，因此可以酉相似于对角矩阵，其元素就是它们的特征值。如此一来就可以方便地求出奇异值了。

1.27 酉等价

设 $A, B \in C^{m \times n}$，如果存在酉矩阵 $U \in C^{m \times m}$ 和 $V \in C^{n \times n}$，使得 $A = UBV$，则称 A 与 B 酉等价。

性质：

若 A 与 B 酉等价，则 A 与 B 有相同的正奇异值。

理解：

(1) 注意酉等价和酉相似的区别。酉相似是对于方阵而言的，且用于相似对角化的酉阵只需要一个，而酉等价是对于更一般的情形 (包括非方阵等) 而言的，且酉阵是不同的两个。前者可以看做是后者的特殊情形，

(2) 两个矩阵“等价 (或相似)”意味着其中一个可以通过有限次的初等变换得到另外一个，而初等变换又可以通过矩阵来刻画，将它们组装称可逆矩阵，也就是如上一般所示的矩阵等价 (或相似) 的数学描述形式。

1.28 行盖尔圆盘、列盖尔圆盘

设 $A=(a_{ij})\in C^{n\times n}$，(1)$S_i=\{z\in C:|z-a_{ii}|\le R_i=\sum\limits_{j\ne i}|a_{ij}|\}$ 称为行盖尔圆盘，其中 R_i 称为 S_i 的半径；(2) $G_j=\{z\in C:|z-a_{jj}|\le C_j=\sum\limits_{i\ne j}|a_{ij}|\}$ 称为列盖尔圆盘。

1.29 对角占优矩阵、严格对角占优矩阵

设 $A\in(a_{ij})\in C^{n\times n}$，若 $|a_{ii}|\ge R_i(A)(i=1,...,n)$，则称 A 为行对角占优矩阵；若 A^T 为行对角占优矩阵，则称 A 为列对角占优矩阵；若 A 为行、列对角占优矩阵，则称 A 为对角占优矩阵。若上式为严格不等式，则称 A 为相应的严格对角占优矩阵。

性质：

设 A 为行 (或列) 严格对角占优矩阵，则有：

(1) A 为可逆矩阵，且 $\lambda_i\in\bigcup\limits_{i=1}^{n}S_i$，这里 $S_i=\{z\in C:|z-a_{ii}|<|a_{ii}|\}$；

(2) 若 A 的所有主对角元均为正数，则 A 的所有特征值都有正实部；

(3) 若 A 为 Hermite 矩阵，且 A 的所有主对角元都是正数，则 A 的所有特征值均为正数（《矩阵理论》P141 证明)。

1.30 Rayleigh 商

设 $A\in C^{n\times n}$ 为 Hermite 矩阵，$x\in C^n$，称 $R_A(x)=\dfrac{x^HAx}{x^Hx},x\ne0$ 为 A 的 Reyleigh 商。

性质：

(1) Reyleigh 商具有零齐次性，即 $R_A(kx)=\dfrac{(kx)^HA(kx)}{(kx)^H(kx)}=\dfrac{|k|^2x^HAx}{|k|^2x^Hx}=R_A(x)=k^0R_A(x)$ ；

(2) Reyleigh 商具有平移不变性，即 $R_{A-\alpha E}(x)=\dfrac{x^H(A-\alpha E)x}{x^Hx}=\dfrac{x^HAx-\alpha x^Hx}{x^Hx}=R_A(x)-\alpha$。

理解：

(1) k 齐次函数定义为：若 $\exists k$，使得 $f(lx)=l^kf(x)$，则称之为 k 齐次函数；

(2) Rayleigh 商在实际应用中可以解决最小二乘法的最小残量问题，见《矩阵理论》P147。

1.31 矩阵序列收敛、矩阵级数、部分和、绝对收敛

(1) 设有 $C^{m\times n}$ 中的矩阵序列 $\{A^{(k)}\},A^{(k)}=(a_{ij}^{(k)})_{m\times n}$。若 $\lim\limits_{k\to\infty}a_{ij}^{(k)}=a_{ij},i=1,2,...,m;j=1,2,...,n$，则称矩阵序列 $\{A^{(k)}\}$ 收敛于 $A=(a_{ij})$，或称矩阵 A 为矩阵序列 $\{A^{(k)}\}$ 的极限，记为 $\lim\limits_{k\to+\infty}A^{(k)}=A$ 或 $A^{(k)}\to A(k\to\infty)$。若矩阵序列不收敛，则称发散；

(2) 设 $\{A^{(k)}\}$ 是 $C^{m\times n}$ 的矩阵序列，称无穷和 $A^{(1)}+A^{(2)}+...+A^{(k)}+...$ 为矩阵级数，记为 $\sum\limits_{k=1}^{\infty}A^{(k)}$。对任一正整数 N，称 $S^{(N)}=\sum\limits_{k=1}^{N}A^{(k)}$ 为矩阵级数的部分和。如果由部分和构成的矩阵序列 $\{S^{(N)}\}$ 收敛于 S，即 $\lim\limits_{N\to\infty}S^{(N)}=S$，则称矩阵级数 $\sum\limits_{k=1}^{\infty}A^{(k)}$ 收敛而且有和 S，记为 $S=\sum\limits_{k=1}^{\infty}A^{(k)}$。不收敛的矩阵级数称为发散的；

(3) 如果 mn 个数项级数 $\sum_{k=1}^{\infty} a_{ij}^{(k)}, i=1,2,...,m; j=1,2,...,n$ 都是绝对收敛的，则称矩阵级数 $\sum_{k=1}^{\infty} A^{(k)}$ 是绝对收敛的（《矩阵理论》P161 证明）。

性质：

(1) 若 $\lim_{k\to\infty} A^{(k)} = A$，则有 $\lim_{k\to\infty} \|A^{(k)}\| = \|A\|$，而逆命题不成立【1-3 的 6 题证明】；

(2) 矩阵级数 $\sum_{k=1}^{\infty} A^{(k)}$ 收敛的充分必要条件是 mn 个数项级数 $\sum_{k=1}^{\infty} a_{ij}^{(k)} (i=1,2,...,m; j=1,2,...,n)$ 都收敛；

(3) 矩阵级数 $\sum_{k=1}^{\infty} A^{(k)}$ 绝对收敛的充分必要条件是正项级数 $\sum_{k=1}^{\infty} \|A^{(k)}\|$ 收敛，这里的范数是任一矩阵范数【1-7 的 21 题证明】。

理解：

(1) 矩阵 $A^{(k)}$ 是个变量，比如 $\begin{pmatrix} \frac{(-1)^k}{k} & -1 \\ \frac{1}{k} & (1+\frac{1}{k})^k \end{pmatrix}$；

(2) 由定义可见，$C^{m\times n}$ 中一个矩阵序列的收敛相当于 mn 个数列同时收敛。因此可以用初等分析的方法来研究它；

(3) 如果级数各项的绝对值所构成的级数收敛，则称级数绝对收敛。绝对收敛级数一定收敛。设级数绝对收敛，且其和等于 S，则任意重排后所得的级数也绝对收敛，且有相同的和数。

1.32 矩阵幂级数、Neumann 级数、收敛矩阵

(1) 设 $A \in C^{n\times n}$，若 $\lim_{k\to\infty} A^k = O$，则称 A 为收敛矩阵；

(2) 矩阵幂级数 $\sum_{k=1}^{\infty} A^{(k)} = \sum_{k=0}^{\infty} c_k A^k = c_0 E + c_1 A + c_2 A^2 + ... + c_k A^k + ...$，其中 $A^{(k)} = c_{k-1} A^{k-1}$；

(3) Neumann 级数 $\sum_{k=0}^{\infty} c_k A^k = \sum_{k=0}^{\infty} A^k = E + A + A^2 + ... + A^k + ...$，其中 $c_k = 1$。

性质：

(1) 设 $A \in C^{n\times n}$，则 A 为收敛矩阵的充分必要条件是谱半径 $r(A) < 1$【1-6 的 20 题证明】；

(2) 幂级数敛散性：设幂级数 $f(z) = \sum_{k=0}^{\infty} c_k z^k$ 的收敛半径为 r，如果方阵 A 满足 $r(A) < r$，则矩阵幂级数 $\sum_{k=0}^{\infty} c_k A^k$ 绝对收敛；如果 $r(A) > r$，则矩阵幂级数发散（《矩阵理论》P162 证明）【1-3 的 7 题体会】；

(3) Neumann 级数敛散性：方阵 A 的 Neumann 级数收敛的充分必要条件是 A 为收敛矩阵。此时，该幂级数的和为 $(E-A)^{-1}$【1-7 的 22 题证明】【1-3 的 8 题体会】。

理解：

幂级数收敛半径的计算方法：对于 $\sum_{n=0}^{\infty} a_n x^n$，它的收敛半径 $r = \lim_{n\to\infty} |\frac{a_n}{a_{n+1}}| = \frac{1}{\lim_{n\to\infty} |\frac{a_{n+1}}{a_n}|}$。由此可见，性质 (3) 实际就是性质 (2) 收敛半径为 1 的特殊情形。

1.33 矩阵函数

设幂级数 $\sum_{k=0}^{\infty} a_k z^k$ 的收敛半径为 r，且当 $|z| < r$ 时，幂级数收敛于函数 $f(z)$，即 $f(z) = \sum_{k=0}^{\infty} a_k z^k, |z| < r$。如果 $A \in C^{n\times n}$ 满足 $r(A) < r$，则称收敛的矩阵幂级数 $\sum_{k=1}^{\infty} a_k A^k$ 的和为矩阵函数，记为 $f(A)$，即 $f(A) = \sum_{k=0}^{\infty} a_k A^k$。常用的矩阵函数有：

(1) 矩阵指数函数：$e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k$, $A \in C^{n\times n}$。

(2) 矩阵正弦函数：$\sin A = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} A^{2k+1}$, $A \in C^{n\times n}$。

(3) 矩阵余弦函数：$\cos A=\sum_{k=0}^{\infty}\frac{(-1)^k}{(2k)!}A^{2k}$, $A\in C^{n\times n}$。

(4) $(E-A)^{-1}=\sum_{k=0}^{\infty}A^k$, $r(A)<1$。

(5) $\ln(E+A)=\sum_{k=0}^{\infty}\frac{(-1)^k}{k+1}A^{k+1}$, $r(A)<1$。

(6) $A^2=A, A^2=E$ 等特殊矩阵函数的计算（PPT 5-2）。

矩阵函数值得计算方法主要有：利用相似对角化（即 $f(A)=P\,\mathrm{diag}(f(\lambda_1),f(\lambda_2),...,f(\lambda_n))P^{-1}$）和 Jordan 标准型（即 $f(A)=P\,\mathrm{diag}(f(J_1),f(J_2),...,f(J_n))P^{-1}$），见《矩阵理论》P164-165【1-3 的 9 题体会】【1-4 的 10 题体会】。

性质：

(1) $e^{iA}=\cos A+i\sin A, i=\sqrt{-1}$;

(2) $\cos A=\frac{1}{2}(e^{iA}+e^{-iA})$;

(3) $\sin A=\frac{1}{2i}(e^{iA}-e^{-iA})$;

(4) $\cos(-A)=\cos A, \sin(-A)=-\sin A$;

(5) 若 $AB=BA$, 则 $e^Ae^B=e^Be^A=e^{A+B}$（《矩阵理论》P168 证明），$\sin(A+B)=\sin A\cos B+\cos A\sin B, \cos(A+B)=\cos A\cos B-\sin A\sin B$【1-4 的 11 题证明】;

(6) $e^Ae^{-A}=e^{-A}e^A=E, (e^A)^{-1}=e^{-A}, (e^A)^m=e^{mA}$。

理解：

(1) 一定要注意性质的前提条件，如性质 (4) 和 (5) 看着相似，但性质 (4) 是建立在 $AB=BA$ 的前提条件下成立的；

(2) 以 Tylor 展开为连接，矩阵函数为矩阵级数提供了特殊的计算方式，同时矩阵级数可作为媒介来理论推导矩阵函数的一些性质。

1.34 单边逆

设 $A\in C^{m\times n}$，如果存在矩阵 $G\in C^{n\times m}$，使得 $GA=E_n(AG=E_m)$ 成立，则称 G 是 A 的左 (右) 逆矩阵，记为 $G=A_L^{-1}(G=A_R^{-1})$。如果 A 有左 (右) 逆矩阵，则称 A 是左 (右) 可逆的。显然，当 $m=n$ 且 A 可逆时，有 $A^{-1}=A_L^{-1}=A_R^{-1}$【1-4 的 12 题体会】。

性质：

(1) 充要条件：设 $A\in C^{m\times n}$，则：(a) A 左可逆 $\Leftrightarrow$ A 为列满秩矩阵 $\Leftrightarrow N(A)=\{0\}$；(b)$A$ 右可逆 $\Leftrightarrow$ A 为行满秩矩阵 $\Leftrightarrow R(A)=C^m$（《矩阵理论》P178 证明）。由公式构造法有：$A_L^{-1}=(A^HA)^{-1}A^H$ 和 $A_R^{-1}=A^H(AA^H)^{-1}$。

(2) 构造方法：(a) 设 $A\in C^{m\times n}$ 是左可逆的矩阵，则 $G=\begin{pmatrix}A_1^{-1}-BA_2A_1^{-1} & B\end{pmatrix}P$ 是 A 的一个左逆矩阵，其中 $B\in C^{n\times(m-n)}$ 为任意矩阵。行初等变换对应的矩阵 P 满足 $PA=\begin{pmatrix}A_1\\A_2\end{pmatrix}$, A_1 是 n 阶可逆方阵；(b) 设 $A\in C^{m\times n}$ 是右可逆的矩阵，则 $G=Q\begin{pmatrix}A_1^{-1}-A_1^{-1}A_2D\\D\end{pmatrix}$ 是 A 的一个右逆矩阵，其中 $D\in C^{(n-m)\times m}$ 为任意矩阵，列初等变换对应的矩阵 Q 满足 $AQ=\begin{pmatrix}A_1 & A_2\end{pmatrix}$, A_1 是 m 阶可逆方阵【补充：《矩阵理论》P179-180】。

(3) 常用结论：单边逆与求解方程组 $Ax=b$ 之间的关系：(a) 设 $A\in C^{m\times n}$ 是左可逆的矩阵，A_L^{-1} 是 A 的一个左逆矩阵，则方程组 $Ax=b$ 有解的充要条件是 $(E_m-AA_L^{-1})b=0$，且有唯一解为 $x=(A^HA)^{-1}A^Hb$；(b) 设 $A\in C^{m\times n}$ 是右可逆的矩阵，则方程组 $Ax=b$ 对任何 $b\in C^m$ 都有解，若 $b\neq 0$ 时，则方程组的解可表示成 $x=A_R^{-1}b$，其中 A_R^{-1} 是 A 的一个右逆矩阵（《矩阵理论》P181-182 证明）。

理解：

(1) 代数中矩阵求逆归根结底就是为了求解非齐次线性方程组 $Ax=b$ 的解 $x=A^{-1}b$，但是当 A 不是方阵、或 A 是满足 $\det A=0$ 的方阵时，求解上述问题就有一定的麻烦了。为了解决这类问题的需要，

将逆矩阵推广到非方阵或奇异方阵上，从而产生了广义逆矩阵的概念。以上是公式构造法，用于理论分析，具体的计算过程见《矩阵理论》P179-181;

(2) 性质 (2) 中的构造方法是为了避免公式构造法中对 A^HA 进行求解时的巨大计算量。

1.35 广义逆

$A \in C^{m\times n}$，若存在 $G \in C^{n\times m}$，使得 $AGb = b, \forall b \in R(A)$，则称 G 是 A 的广义逆矩阵，并记为 $G = A^-$。

性质：

(1) 充要条件：设 $A \in C^{m\times n}$，则 $G \in C^{n\times m}$ 是 A 的广义逆矩阵的充要条件是它满足 $AGA = A$。(《矩阵理论》P183 证明)

(2) 构造方法：设 $A \in C^{m\times n}$，A^- 是 A 的任意给定的广义逆矩阵，则有 $A\{1\} = \{G|G = A^- + U - A^-AUAA^-, \forall U \in C^{n\times m}\} = \{G|G = A^- + (E_n - A^-A)V + W(E_m - AA^-), \forall V, W \in C^{n\times m}\}$。(显然是不唯一的)

(3) 常用结论：设 $A \in C^{m\times n}, \lambda \in C$，则：(a) $(A^T)^- = (A^-)^T, (A^H)^- = (A^-)^H$；(b) AA^- 与 A^-A 均为幂等矩阵，且 $\mathrm{rank}(A) = \mathrm{rank}(AA^-) = \mathrm{rank}(A^-A) \le \mathrm{rank}(A^-)$ (用得较多)；(c) λ^-A^- 是 λA 的广义逆矩阵，其中 $\lambda^- = \begin{cases} 0 & \lambda = 0, \\ \lambda^{-1} & \lambda \neq 0. \end{cases}$；(d) 设 S 是 m 阶可逆矩阵，T 是 n 阶可逆矩阵，且 $B = SAT$，则 $T^{-1}A^-S^{-1}$ 是 B 的广义逆矩阵；(e) $R(AA^-) = R(A), N(A^-A) = N(A)$；(f) 若 $ABA = A, (AB)^H = AB$，则 $AB = P_{R(A)}$；(g) $\mathrm{rank}(A) = n$ 的充要条件是 $A^-A = E_n$；(h) $\mathrm{rank}(A) = m$ 的充要条件是 $AA^- = E_m$。(《矩阵理论》P184-185 证明

(4) 计算方法：见《矩阵理论》P186。

理解：

对于单边逆，在充要条件中已明确指出行满秩或列满秩矩阵才存在，然而许多矩阵并非是行满秩或列满秩，因此引入了更一般矩阵的逆矩阵问题，即广义逆。

1.36 自反广义逆

设 $A \in C^{m\times n}$，如果存在 $G \in C^{n\times m}$ 使得 $AGA = A, GAG = G$ 同时成立，则称 G 为 A 的自反广义逆矩阵，记为 $G = A_r^-$ 【1-4 的 13 题】。

性质：

(1) 充要条件：任何矩阵都有自反广义逆矩阵，且不唯一 (《矩阵理论》P188 证明)。

(2) 构造方法：(a) 由外界构造：设 $X, Y \in C^{n\times m}$ 均为 $A \in C^{m\times n}$ 的广义逆矩阵，则 $Z = XAY$ 是 A 的自反广义逆；(b) 由自身构造：$A \in C^{m\times n}, A^-$ 是 A 的广义逆矩阵，则 A^- 是 A 的自反广义逆矩阵的充要条件是 $\mathrm{rank}(A) = \mathrm{rank}(A^-)$；(c) 由自身构造：设 $A \in C^{m\times n}$，则 $X = (A^HA)^-A^H, Y = A^H(AA^H)^-$ 均是 A 的自反广义逆矩阵 (《矩阵理论》P189-191 证明)。

(3) 常用结论：(a) 设 $A \in C^{m\times n}, X \in C^{n\times m}$，则从下列任意两个等式成立都可以推出第三个等式成立：(a) $\mathrm{rank}(A) = \mathrm{rank}(X)$；(b)$AXA = A$；(c)$XAX = A$ (《矩阵理论》P190 证明)；(b)AA_r^- 和 A_r^-A 都是幂等矩阵。(《矩阵理论》P191 证明)

(4) 计算方法：见《矩阵理论》P193 起第四节。

理解：

对于满秩方阵 A，我们知道 A 是可逆矩阵，由 $(A^{-1})^{-1} = A$ 可得 $AA^{-1}A = A, A^{-1}AA^{-1} = A^{-1}$ 同时成立。但这一事实对于广义逆矩阵一般不成立，也就是说，矩阵 A 未必是其广义逆矩阵的广义逆矩阵。因此这里引入自反广义逆矩阵 (与泛函分析的自反性相联系)。

1.37 M-P 广义逆

设 $A \in C^{m\times n}$，如果有 $G \in C^{n\times m}$，使得 $AGA = A, GAG = G, (AG)^H = AG, (GA)^H = GA$，则称 G 是 A 的 M-P 广义逆矩阵，记为 $G = A^+$，且唯一【1-8 的 23 题证明】【1-5 的 15 题体会】。

性质：

(1) 充要条件：任何矩阵都有 M-P 广义逆，且唯一；

(2) 构造方法：设 $A \in C_r^{m\times n}$ 且 $A=BD$ 是 A 的最大秩分解，则 $G=D^H(DD^H)^{-1}(B^HB)^{-1}B^H$ 就是 A 的一个 M-P 广义逆矩阵 A^+（《矩阵理论》P201 证明）；

(3) 常用结论：设 $A \in C^{m\times n}$，则有：(a) $(A^+)^+=A$；(b) $(A^T)^+=(A^+)^T,(A^H)^+=(A^+)^H$；(c) $A^+=(A^HA)^+A^H=A^H(AA^H)^+$（常用）；(d) $R(A^+)=R(A^H)$；(e)$AA^+=P_{R(A)},A^+A=P_{R(A^H)}$；(f) $R(A)=R(A^H) \Leftrightarrow AA^+=A^+A$；(g) $(A^HA)^+=A^+(A^H)^+,(AA^H)^+=(A^H)^+A^+$；(h)$(A^HA)^+=A^+(AA^H)^+=A^H(AA^H)^+(A^H)$；(i)$AA^+=(AA^H)(AA^H)^+=(AA^H)^+(AA^H),A^+A=(A^HA)(A^HA)^+=(A^HA)^+(A^HA)$（《矩阵理论》P202-203 证明）。设 $A\in C^{m\times l},B\in C^{l\times n}$，则 $(AB)^+=B^+A^+$ 的充要条件是 $R(A^HAB)\subset R(B),R(BB^HA^H)\subset R(A^H)$（《矩阵理论》P204 证明）【1-5 的 16 题体会】；

(5) 计算方法：(a) 计算方法之最大秩分解法：如果 A 是行满秩矩阵，则 $A^+=A^H(AA^H)^{-1}$；如果 A 是列满秩矩阵，则 $A^+=(A^HA)^{-1}A^H$；对于任意 $A\in C_r^{m\times n},A=BD$ 是 A 的最大秩分解，则 $A^+=D^+B^+=D^H(DD^H)^{-1}(B^HB)^{-1}B^H$ 【1-5 的 14 题体会】；(b) 计算方法之奇异值分解法，见《矩阵理论》P208 起，要掌握它与奇异值的 3 个关系及证明；

(6) 应用：求解相容线性方程组的的通解、最小范数解【1-6 的 18 题体会】，求解不相容线性方程组的最小二乘解和通解【1-6 的 19 题体会】。

理解：

(1) 上述诸多广义逆的发展实际上是密切联系的，A_r^- 在继承了 A_R^{-1},A_L^{-1},A^- 的良好性质的基础上，又建立起“自反性”。之后，A^+ 在继承了 A_r^- 的良好性质后，还进一步迎来了“唯一性”；

(2) 在上述性质 (3) 中的常用结论 (c) 之所以常用，是因为它可以将 A^+ 的计算转换为 $(A^HA)^+$ 的计算，再乘个 A^H。因为当 $A_{m\times n}$ 中的 m,n 一个远大于另一个时，则可以通过 A^HA 或 AA^H 来转换为低阶的来计算。

1.38 半群、含幺半群、群、可换群或 Abel 群

设 G 是一个非空集合，若在 G 上定义一个二元运算 $\cdot$，则概念与所需满足条件的对应关系为：

(1) **半群**：封闭性、结合律（$\forall a,b,c\in G,(a\cdot b)\cdot c=a\cdot(b\cdot c)$）；

(2) **含幺半群**：封闭性、结合律、单位元（$\exists e,\forall a\in G,a\cdot e=e\cdot a=a$）；

(3) **群**：封闭性、结合律、单位元、逆元（$\forall a\in G,\exists a^{-1},a^{-1}\cdot a=a\cdot a^{-1}=e$）；

(4) **可换群或 Abel 群**：封闭性、结合律、单位元、逆元、交换律（$\forall a,b\in G,a\cdot b=b\cdot a$）。

理解：

(1) 由结合律、单位元和逆元还可以推出群满足“消去律”，即 $a,b,c\in G$, 若 $a\cdot b=a\cdot c$，则 $b=c$。证明过程：$b=e\cdot b=(a^{-1}\cdot a)\cdot b=a^{-1}\cdot(a\cdot b)=a^{-1}\cdot(a\cdot c)=c$；

(2) 在定义中，不要狭义地将 $\cdot$ 理解为乘操作，它是二元运算，可以是集合的交或并等等。此外，对单位元的理解也不要一贯地将其视为 1 或 E，比如 0 对于 $(Z,+)$ 就是一个单位元，因为它满足 $e\cdot a=a\cdot e=a$，即 $0+a=a+0=a$。以及对逆元的理解，也不要将其单纯地理解为可逆矩阵或倒数，因为 $a^{-1}a=aa^{-1}=e$ 中的 e 也不一定非要是 1 或 E，例如 $-x$ 就是 $(Z,+)$ 的一个逆元，因为其满足 $(-x)+x=x+(-x)=0$；

(3) 《应用近世代数》P40-41 的定理 2.1.3、定理 2.1.4 和定理 2.1.5 能够帮助我们从不同的角度来理解群。

例子：

要会判断一个代数系统是否构成群。可以先从逆元入手（即挑出特殊元素，比如乘群中的 0 元素，来看它是否有逆元），如果存在某种二元运算下无逆元的元素，则直接排除掉可以构成群。

(1) “$(\mathbb{Z},+)$”、“$(\mathbb{Q},+)$”、“$(\mathbb{R},+)$”、“$(\mathbb{C},+)$”、“$(\mathbb{Q}^*,\cdot)$”、“$(\mathbb{R}^*,\cdot)$”、“$(\mathbb{C}^*,\cdot)$”、“$(Z_n,+)$”、“$(Z_n^*,\cdot)$”、“$(R^{n\times n},+)$”都是**可换群**。但是，$(Q,\cdot)$、$(R,\cdot)$、$(C,\cdot)$ 不是群，因为其元素 0 无逆元，但把 0 元素排除掉以后就可以了，但把零元素除掉后 $(Z^*,\cdot)$ 也不是群，因为除 -1 和 1 外，其他元素均无逆元。

其中，$(Z_n,+)$ 是**整数模 n 的同余类加法群**，即在 $Z_n=\{\overline{0},\overline{1},...\overline{n-1}\}$ 中定义模 n 的加法为 $\overline{a}+\overline{b}=\overline{a+b}$。$(Z_n^*,\cdot)$ 是**整数模 n 的同余类乘法群**，即在 $Z_n^*=\{\overline{k}|\overline{k}\in Z_n,(k,n)=1\}$ 中定义模 n 的乘法为 $\overline{a}\cdot\overline{b}=\overline{ab}$。本质上来看，$(Z_n^*,\cdot)$ 把 $(Z_n,\cdot)$ 中无逆元的元素都去掉了。

(2) “$(2^A,\cup)$”、“$(2^A,\cap)$”、“$(R^{n\times n},\cdot)$” 是**含幺半群**;

(3) “$(\mathbb{Z},-)$” 不是**半群**。

(4) 再比如, $S=\{\omega=a_1a_2...a_n|a_i=0或1,i=1,2,...,n\}$, 在 S 中定义二元运算 $+$, $\omega_1=a_1...a_n,\omega_2=b_1...b_n,\omega_1+\omega_2=c_1...c_n$, 其中 $c_i=a_i+b_i\pmod 2, i=1,2,...,n$, 则 $(S,+)$ 是一个群, 此群称为**二进制码词群**。

具体参见《应用近世代数》P39。$(Z_n,+)$ 和 $(Z_n^*,\cdot)$ 都是密码学中很有用的两个群。

【1-10 的 30 题证明 $(Z_n^*,\cdot)$ 是群, 1-10 的 31 题证明 $(Z_n,+)$ 是群。别忘了还要证明封闭性!】

【1-10 的 32 题和 33 题例子, 群与矩阵（如: $G=\{A=(a_{ij})_{n\times n}|a_{ij}\in\mathbb{Z},\det A=1\}$ 对矩阵乘法构成群, 重点体会这里的 $\det A=1$ 作为条件的意义）和变换联系。别忘了还要证明单位元和逆元属于集合!】

1.39 子群、真子群

设 S 是群 G 的一个非空子集, 若 S 对 G 的运算也构成群, 则称 S 是 G 的一个**子群**, 记作 $S\le G$。当 $S\le G$ 且 $S\ne G$ 时, 称 S 是 G 的**真子群**, 记作 $S<G$。

性质:

(1) 设 $H\le G$, 则 H 的单位元就是 G 的单位元;

(2) $H_1,H_2\le G\Rightarrow H_1\cap H_2\le G$;

(3) $H_1,H_2\le G$ 则 $H_1\cup H_2\le G\Leftrightarrow H_1\subseteq H_2$ 或 $H_2\subseteq H_1$;

(4) $H_1,H_2\le G$ 则 $H_1H_2\le G\Leftrightarrow H_1H_2=H_2H_1$（注意表示: $H_1H_2=\{h_1h_2|\forall h_i\in H_i\}$);

(5) $|H_1H_2|=\dfrac{|H_1||H_2|}{|H_1\cap H_2|}$（常用于计数)。

(《应用近世代数》P47 证明)

例子:

对任何取定的一个正整数 m, 子集 $H_m=\{mk|k\in\mathbb{Z}\}$ 对加法都构成群, 所以 $H_m\le Z(m=0,1,2,...)$。反之, 可以证明 $\mathbb{Z}$ 的任何一个子群只能是某个 H_m。注意理解, 因为 $k\in\mathbb{Z}$ 是无限的, 所以 $\mathbb{Z}$ 和 H_m 都看作是无限的。在有限集条件下, H_m 比 $\mathbb{Z}$ 要少, 但是在无限情况下, 可以看做 H_m 和 $\mathbb{Z}$ 都是无限多, 因此 $H_m\le\mathbb{Z}$ 而非 $H_m<\mathbb{Z}$;

理解:

集合论中我们研究子集, 在群论中我们也自然地想到去考虑子群。

1.40 全线性群 $GL_3(\mathbb{R})$ 及其子群

全线性群（或一般线性群） $GL_n(F)$ 是数域 F 上 $n\times n$ 可逆矩阵全体组成的矩阵乘法群。**特殊线性群** $SL_n(F)=\{A|A\in GL_n(F),\det A=1\}$。易得 $SL_n(F)\le GL_n(F)$【证明: 从 $GL_n(F)$ 中抽取出子集 $SL_n(F)$ 后, 我们用 4.2 的定理 1 中的判别条件可以验证: $\forall A,B\in SL_n(F)$ 有 $|AB^{-1}|=|A||B|^{-1}=1$, 所以 $AB^{-1}\in SL_n(F)$】

有了上述结论作支撑后, 我们可以讨论 $GL_3(\mathbb{R})$ 的子群, 包括:

(1) $SL_3^{\pm}(\mathbb{R})=\{A|A\in\mathbb{R}^{3\times3},|A|=\pm1\}$。表示所有体积不变的线性变换的集合, 即对 $\mathbb{R}_3$ 中任意三个向量 $\alpha_1,\alpha_2,\alpha_3$ 所构成的平行六面体的体积与经过变换后的三个向量 $A\alpha_1,A\alpha_2,A\alpha_3$ 所构成的平行六面体的体积相同;

(2) $SL_3(\mathbb{R})=\{A|A\in R^{3\times3},|A|=1\}$。它是保持体积不变且保持定向不变的所有线性变换的集合。即指对任意三个向量 $\alpha_1,\alpha_2,\alpha_3$ 所成的左手系或右手系关系经过变换后仍保持不变;

(3) $O_3(\mathbb{R})=\{A|A\in\mathbb{R}^{3\times3},A'A=I\}$。所有正交矩阵的集合, 几何意义是保持向量长度不变的所有线性变换的集合;

(4) $SO_3=\{A|A\in\mathbb{R}^{3\times3},A'A=I,|A|=1\}$（三维旋转群)。$|A|$ 的正交变换是旋转, 它保持空间向量的长度和定向都不变。

它们之间有关系: $SO_3<SL_3(\mathbb{R})<SL_3^{\pm}(\mathbb{R})<GL_3(\mathbb{R})$。

理解:

对于上述例子中的（3），要理解它们是什么的集合，且几何意义是进行了怎样的变换。具体见《应用近世代数》P47-48。

1.41 阶或周期

设 G 是群，$a \in G$，使 $a^n = e$（在加群中该式变为 $na = 0$）成立的**最小**正整数 n 称为 a 的阶或周期，记作 $\circ(a)$。若没有这样的正整数存在，则称 a 的阶是无限的。单位元的阶是 1。

例子：

在 $(\mathbb{Z}, +)$ 中除 0 以外的元素都是无限阶的。在 $(\mathbb{Z}_n, +)$ 中元素的阶都是有限的，比如 $(Z_6, +)$ 中 $\circ(\overline{1}) = 6, \circ(\overline{2}) = 3$。在 $(Z_8^*, *) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$，有 $\circ(\overline{3}) = \circ(\overline{5}) = \circ(\overline{7}) = 2$，比如 $\overline{3}^2 \mod 8 = \overline{9} \mod 8 = \overline{1}$。

性质：

（1）有限群中每一个元素的阶是有限的。但无限群中不一定存在无限阶的元素，例如由复数域上所有单位根构成的乘法群中每个元素都是有限阶的；

（2）设 G 是群，若除单位元外其他元素都是 2 阶元，则 G 是 Abel 群。【证明：由 $a^2 = 1$ 得 $a = a^{-1}$，$\forall a, b \in G$, 有 $ab \in G$ 及 $(ab)^2 = 1$，所以 $ab = (ab)^{-1} = (ba)^{-1} = ba$】

（3）对于 $(Z_n, +, \cdot)$ 群，阶等于 d 的元素的个数为 $\varphi(d)$，且有 $n = \sum_{d|n} \varphi(d)$。（特别注意，阶一定要是使得成立的那个最小的正整数哦，最小的！）

理解：

与“最小多项式”概念类比。

1.42 循环子群、循环群

设 G 是群，$a \in G$，令 $H = \{a^k | k \in Z\}$（对于加群则为 ka），因为 $\forall a^{k_1}, a^{k_2} \in H$ 有 $a^{k_1}(a^{k_2})^{-1} = a^{k_1 - k_2} \in H$，由定理得，所以 H 是 G 的子群，此子群称为由 a 生成的**循环子群**，记作 $\langle a \rangle$，a 称为它的**生成元**。若 $G = \langle a \rangle$，则称 G 是**循环群**。

由它可以与子群相联系，即提供了找出一个群的所有子群的方法。具体来说，把群中的每个元素作为生成元，然后由该生成元生成一个循环子群。最后把不重复的提取出来，即为群的全部子群。

理解：

循环群是线性代数中“基”的来源，以及下面的生成群。尤其在矩阵情形下，如证明 $SL_n(\mathbb{Z})$ 的最小生成元集，会尤为凸显这个思想。循环群可以理解为“由一个种子生成的群”，或者说是等同于“其中一个元素的阶等于群的阶”，比如 $(Z_5, +)$ 共五个元素，除 $\circ(\overline{0}) = 0$ 外其它元素的阶都为 5，所以是个循环群。也不难验证这一点，比如用元素 $\overline{1}$ 就可以生成 $(Z_5, +)$ 中的其他 4 个元素。这里有个推论可以用于快速判断一些特殊情形：若 $|G| = p$(素数)，则 $G = C_p$(p 阶循环群)，即**素数阶群必为循环群**。又如 $(Z_{40}, +)$ 是一个循环群，即 $Z_{40} = \langle \overline{1} \rangle$；

1.43 生成群

循环子群是由一个元素生成的，由几个元素或一个子集也可生成一个子群。

设 S 是群 G 的一个非空子集，包含 S 的 G 的最小子群称为**由 S 生成的子群**，记作 $\langle S \rangle$，S 称为它的**生成元集**，$\langle S \rangle$ 可表示为 $\langle S \rangle = \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} ... a_k^{\varepsilon_k} | a_i \in S, \varepsilon_i \in Z, k = 1, 2, ...\}$，含义就是可以由这些元素表示出来（类比算数基本定理）。注意哦，因为 $\varepsilon_i \in Z$，所以比如在矩阵情形下还可以为 -1，即求逆运算哦。

如果 $G = \langle S \rangle$，且任何 S 的真子集的生成子群均不是 G，则称 S 是 G 的**极小生成元集**。任何一个子群都有一个极小生成元集。当 $|S| < \infty$ 时，元素个数最少的生成元集称为**最小生成元集**。

例子：

如 $Z_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} = \langle \overline{3}, \overline{5} \rangle$，选法不一定，也可以把 $\overline{1}$ 放进去，但是多余，即不能构成最小生成集。

【1-9 的 27 题，证明 $SL_2(\mathbb{Z})$ 的最小生成元集。很好的一道题，感受思想吧。记住 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$，

$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}^k = \begin{pmatrix}1 & 0\\ k & 1\end{pmatrix}, k \in \mathbb{Z}$】

【《应用近世代数》P54 的例 2.3.4 和习题 2.3 的 2 题，找出二面体群 D_n 的所有子群和所有最小生成元集】

1.44 群的同构

首先要强调一下，映射是不可以“一对多”的哟~只能“一对一”或“多对一”!

设 $(G,\bullet)$ 与 $(G'.\circ)$ 是两个群，若存在一个 G 到 G' 的双射 f 满足 $f(a\bullet b)=f(a)\circ f(b),\forall a,b,\in G$（在 G' 中进行比较的），就说 f 是 G 到 G' 的一个**同构映射**，并称 G 与 G' **同构**，记作 $G\overset{f}{\cong}G'$（可以看出，同构的概念一定是关于某个映射而言的）。

【1-9 的 29 题；1-11 的 37 题；1-12 的 38 题，对于不同构的情形，也要能够快速找出反例来证明】

理解：

同构的概念是说：有些群虽然元素和运算符号不一样，但从群的代数结构与性质上看，它们是完全相同的。一个同构映射 f 不仅保持运算关系，而且使两个群的所有代数性质都一一对应。两个同构的群，如果不管它们的元素和运算表示符号的差异而只考虑它们的代数性质，我们就把它们等同起来看作一个群。这也就是研究同构的意义。

在现实应用中，当我们要研究一个复杂代数系统的性质时，我们可以先为它找到一个同构的、更简单的代数系统，然后将问题转换为研究这个更简单的代数系统。比如任何循环群都与 Z 或 Z_n 同构。

在两个集合或群之间建议同构 haineng 之间建立同构还能够在证明过程中起到很好的作用，比如证明两个集合元素个数相等时【1-8 的 25 题证明有限集合 A 有关系 $|2^A|=2^{|A|}$】。

1.45 对称群、变换群、n 次对称群、n 次置换群

设 A 是一个非空集合，

（1）A 上的所有可逆变换构成的群称为 A 上的**对称群**。此群的任何子群都叫做 A 上的**变换群**；

（2）当 $|A|=n$ 时，A 上的对称群称为 n **次对称群**，记作 S_n。S_n 的任何一个子群称为 n **次置换群**。（$|S_n|=n!$，其中的元素也是置换，S_n 是所有 n 次置换的集合，要会写出元素 2 行的矩阵形式，就是置换，然后通过性质定理把它们展开成轮换或对换乘积的形式的写法）。

理解：

（1）理解置换群：对应于群的定义，例如在正多面体的旋转问题中，“集合”为顶点标号，“二元运算”为置换或轮换的复合，在这组定义下它是满足群的定义的。即存在“单位元”，表示自己与自己进行置换，也存在“逆元”，表示换过去后又换回来。因此，别看置换群在写法上长得“怪”，这只是一种表示方法，不影响它构成群这一事实；

（2）理解“对称群”：设 A 是一个非空集合，A^A 是 A 上的所有变换的集合，在 A^A 上定义二元运算为映射的复合（即 $f:A'\to B,g:B\to C,h:C\to D$，其中 $f,g,h\in A^A,A',B,C,D\subset A$），由于映射的复合满足结合律（即 $[h(gf)](x)=[(hg)f](x)$，注意是从右往左看，从 x 出发哦），所以 A^A 对映射的复合（也是二元运算哦）构成一个“半群”。如果记 S 是 A 上的全体可逆变换的集合，则 S 对映射的复合构成群，此群称为 A 上的“对称群”(这里的集合中的元素是映射，定义的运算是映射的复合。特别注意：映射也可以是群的元素哦，如【1-10 的 33 题】那样子)；

（3）变换群和置换群在群论中有很重要的作用，任何群都可用它们来表示，例如 Cayley 定理；

（4）也不要把这四个群理解的太死板，不要只理解为交换操作。其实它们之中的二元运算还可以是其他的，例如证明 Cayley 定理时构造的，只要能够满足对映射复合构成群的条件即可。

1.46 轮换、n 次置换、偶（奇）置换、n 次交错群、置换的类型、二面体群、正多面体旋转群

下面这些概念都是用于研究置换群的。

（1）设 r 是一个 n 次置换，满足：(a) $r(a_1)=a_2, r(a_2)=a_3, ..., r(a_l)=a_1$（即从 n 个元素中抽取 l 个（可以不邻近）作为一个子集，将该子集中的每个元素依次“向前”移动一个位置）；(b) $r(a)=a$，当 $a \neq a_i (i=1,2,...,l)$。则称 r 是一个长度为 l 的**轮换**。长度为 2 的轮换称为**对换**；

n 次置换也是在“交换次序”，但不一定像轮换那样“规则”。轮换一定是置换，但置换不一定是轮换；

（2）由定理 4.1 中的 5 可知，任一置换 σ 都可以分解为对换之积：$\sigma=\pi_1\pi_2...\pi_s$。对换个数 s 的奇偶性是惟一确定的，因此可用 s（或 $N(\sigma)=\sum_{i=1}^{k}(l_i-1)$，来源于 σ 的轮换分解式 $\sigma=r_1r_2...r_k$，因为长度为 2 为对换，所以长度为 l 的轮换可以分解成 $l-1$ 个对换，这和前面的这个公式是一个意思）的奇偶性来规定 σ 的奇偶性。当对换个数 s（或 $N(\sigma)$）是偶（奇）时，σ 称为**偶（奇）置换**；

（3）n 次对称群 S_n 中所有的**偶**置换构成一个子群，此子群称为 **n 次交错群**，记作 A_n；

（4）一个 n 次置换 σ，如果 σ 的标准轮换分解式是由 λ_1 个 1-轮换、λ_2 个 2-轮换、...、λ_n 个 n 轮换组成，则称 σ 是一个 $1^{\lambda_1}2^{\lambda_2}...n^{\lambda_n}$ **型置换**，其中 $1\cdot\lambda_1+2\cdot\lambda_2+...+n\cdot\lambda_n=n$。在 S_n 中，$1^{\lambda_1}2^{\lambda_2}...n^{\lambda_n}$ 型置换的个数为 $\frac{n!}{1^{\lambda_1}2^{\lambda_2}...n^{\lambda_n}\lambda_1!\lambda_2!...\lambda_n!}$；

（5）对二维空间中正（$n\geq 3$）边形的顶点集合进行旋转或绕对称轴翻转的变换（即对应其顶点集合的一个置换），且对变换的复合是封闭的，有单位元，并且每个元素有逆元，所以构成群，称之为二**面体群** D_n；

（6）对于三维空间中正多面体保持空间位置不变的旋转，每一个旋转对应其顶点集合的一个置换。两个置换相乘就是一个旋转接着另一个旋转，一个旋转的逆就是与它反向的旋转，因此，所有旋转构成一个群，称为此**正多面体旋转群**，可以用一个置换群来表示。

例子：

见《应用近世代数》P59 的例题 2.4.2，求正方体的旋转群。分绕三类轴的旋转进行讨论，即通过对面中心的轴、通过对顶点的轴和通过对边中心的轴。然后找出所有可能的旋转方式并用轮换（即基于定理的置换分解式）来表示。一共有 1(单位元)+9+8+6=24 个元素。

这个例子其实就是置换群在实际中应用的一个例子。

性质：

（1）长度为奇数的轮换是偶置换，长度为偶数的轮换是奇置换【1-12 的 39 题证明】；

（2）两个置换 σ_1,σ_2 相乘时，乘积的奇偶性遵循：偶偶得偶，奇奇得偶，奇偶得奇，偶奇得奇。

（3）n 次交错群 $|A_n|=n!/2$；【1-12 的 39 题证明】

（4）任何一个置换群的元素或都是偶置换，或奇偶置换各半；

（5）正多面体旋转群都是三维旋转群 SO_3 的子群；

（6）对于长度为 l 的轮换 r，显然有 $\circ(r)=l$。

【《应用近世代数》P58 证明】

1.47 左陪集、右陪集、指数

这些概念是针对群内子群的，为了研究它们的性质。这些概念都在为拉格朗日定理作铺垫，拉格朗日定理可以用来确定一个群内可能存在的子群、元素的阶等。

（1）设 $(G,\cdot)$ 是一个群，$H\leq G, a\in G$，则 $a\cdot H$ 称为 H 的一个**左陪集**，$H\cdot a$ 称为 H 的一个**右陪集**（即说成是由元素 a 确定的左（右）陪集）。当 G 是可换群时，子群 H 的左右陪集是相等的。一般来说，陪集 aH 称为以 a 为代表元的陪集，同一陪集可以有不同的代表元；

（2）设 G 是群，$H\leq G$，H 在 G 中的左（右）陪集个数（注意要去重哦，即仅算代表元的等价类数）称为 H 在 G 中的**指数**，记作 $[G:H]$（由定理 4.2 的 7 知，当左陪集的集合与右陪集的集合是有限集合时，左陪集的个数与右陪集的个数是相等的）。

性质：

（1）$aH=H\Leftrightarrow a\in H$；

（2）$b\in aH\Leftrightarrow aH=bH$。这说明陪集中任何一个元素都可以作为代表元（于是可以从中找一个最简单的元素作为代表元，来写出陪集）；

（3）两个陪集相等的条件：$aH=bH\Leftrightarrow a^{-1}b\in H (Ha=Hb\Leftrightarrow ba^{-1}\in H)$；

(4) 对任何 $a,b\in G$ 有 $aH=bH$ 或 $aH\cap bH=\emptyset$。因而 H 的所有左陪集的集合 $\{aH|a\in G\}$ 构成 G 的一个划分（这个在证明中挺常用）【《应用近世代数》P63 证明】【1-12 的 40 题】。

【1-12 的 41 题证明四个等价描述】

理解：

陪集在证明过程中的作用，比如【1-12 的 39 题】。陪集也体现了“等价”的思想，如【《应用近世代数》P62 的例 2.5.1 就只写到 $m-1$，因为循环群 H_m 同构于 $(Z_m,+)$，代表元从 0 到 $m-1$。由性质，陪集要么相等要么相互独立，因此写的时候只写代表咯，这就是等价和划分的思想。注意代表元要从子群切入，就是为了最后的不重复】和【1-12 的 40 题】。

1.48 正规子群、换位子、换位子群

正规子群对刻画群的性质有十分重要的作用，它是一类特殊的子群，可以产生商群。

(1) 设 G 是群，$H\leq G$，若 $\forall g\in G$ 有 $gH=Hg$，则称 H 是 G 的**正规子群**（或不变子群），记作 $H\trianglelefteq G$。用 $H\triangleleft G$ 表示 H 是 G 的**真正规子群**。

任何群都有两个平凡的正规子群：$\{e\}$ 和 G 本身。**如果 G 是可换群，则 G 的任何子群都是正规子群**。

(2) 群 G 中形式为 $aba^{-1}b^{-1}$ 的元素称为 a,b 的**换位子**，由 G 中所有的换位子生成的子群称为**换位子群**。

正规子群的判别方法：

用定义来判别一个子群是否为正规子群并不总是方便的，所以下面给出正规子群的一些性质，使我们有更多的判别方法。

设 H 是 G 的子群，则以下几个命题是相互等价的：

(a) $\forall a\in G$，有 $aH=Ha$；

(b) $\forall a\in G,\forall h\in H$，有 $aha^{-1}\in H$；

(c) $\forall a\in G$，有 $aHa^{-1}\subseteq H$；

(d) $\forall a\in G$，有 $aHa^{-1}=H$。

【《应用近世代数》P68 证明】

通常用上述的 (b) 来进行判断。并且该条性质也常用于证明正规子群中的一些常见结论。【1-13 的 42 题】

性质：

(1) 设 $A\trianglelefteq G,B\trianglelefteq G$，则 $A\cap B\trianglelefteq G,AB\trianglelefteq G$；【《应用近世代数》P69 证明，证明正规子群时要先证是子群，然后再证是正规子群】

(2) 设 $A\trianglelefteq G,B\leq G$，则 $A\cap B\trianglelefteq B,AB\leq G$；【1-13 的 43 题证明】

(3) 设 $A\trianglelefteq G,B\trianglelefteq G$，且 $A\cap B=\{e\}$，则 $\forall a\in A,b\in B$，有 $ab=ba$；【《应用近世代数》P69 证明】

(4) 指数为 2 的子群必是正规子群。【《应用近世代数》P67 的例 2.6.1 证明】

理解：

正规子群的意义：想要 $(g_1H)(g_2H)=g_1g_2H$ 成立，该怎么办呢?看以下变换：$(g_1H)(g_2H)=g_1(Hg_2)H=g_1g_2HH=g_1g_2H$，如此一来就可以。显然，要让该变换成立，中间关键的一步就是使得 $Hg_2=g_2H$ 成立。

1.49 商群

设 $H\trianglelefteq G$，则 G 关于 H 的左陪集的集合与 G 关于 H 的右陪集的集合相等，称为 G 关于 H 的陪集的集合，记作 G/H，即 $G/H=\{aH|a\in G\}=\{Ha|a\in G\}$。定义由 H 决定的 G 中元素之间的等价关系 $\sim_H$ 为 $a\sim_H b\Leftrightarrow a^{-1}b\in H$。有时用同余记号表示：$a^{-1}b\in H\Leftrightarrow a\equiv b\pmod H$。每一个陪集记作 $\overline{a}=aH$，称为模 H 的一个同余类。因而 G/H 又可表示为 $G/H=\{\overline{a}|a\in G\}$。

设 $H\trianglelefteq G$，则 G/H 关于子集乘法构成的群称为 G 关于 H 的**商群**。

理解：

对于 G/H 的理解，简而言之就是关于 H 而言的，H 是 G 的一个正规子群，$G/H=\{\overline{a}|a\in G\}$。（陪集可能会重复，里面的应该都是代表，做到不重不漏）

1.50 单群

若群 $G \neq \{e\}$, G 中除 $\{e\}$ 和 G 本身外, 无其他的正规子群, 则称 G 是**单群**。【《应用近世代数》P71 例子。如可换群中的 $(Z_p, +)$, p 为素数, 且在可换群中只有它们是单群; 又如非可换群中的 $A_n(n \geq 5), SO_3$】

1.51 极大正规子群

设 N 为 G 的非平凡正规子群, 若有正规子群 H 使 $N < H$, 则必有 $H = G$。这时, 称 N 为 G 的一个**极大正规子群**。单群内无极大正规子群。并有以下性质: 设 G 是群, $N \trianglelefteq G$, 则 G/N 是单群 $\Leftrightarrow$ N 是 G 的极大正规子群。【《应用近世代数》P84 证明】

理解:

这个关于极大正规子群的定义是在说, 这个正规子群不属于除了 G (因为 G 是 G 的平凡正规子群嘛) 这个最大的正规子群外的其它任何正规子群的子群 (因为正规子群之间也存在子群的从属关系)。

1.52 中心、中心化子

(1) 设 G 是一个群, 和 G 中所有元素都可交换的元素构成的集合称为群的**中心**, 记作 $C(G)$ 或 C, 即 $C(G) = \{a | a \in G, \forall x \in G, ax = xa\}$。

(2) 设 A 是群 G 的一个非空子集, G 中和 A 的所有元素均可交换的元素构成的集合, 记作 $C_G(A)$, 即 $C_G(A) = \{g | g \in G, \forall a \in A, ag = ga\}$, 称为 A 在 G 中的**中心化子**。当 $A = \{a\}$ 时, 它的中心化子记作 $C_G(a)$ 或 $C(a)$, 即 $C_G(a) = \{g | g \in G, ag = ga\}$, 称为元素 a 在 G 中的中心化子。

【1-13 的 44 题例子】

性质:

(1) $C(G)$ 是 G 的一个非空子集;

(2) $C(G)$ 是 G 的一个子群;

(3) $C(G)$ 是 G 的正规子群;

(4) $C_G(A) \leq G$ 且 $C(G) \leq C_G(A)$;

(5) $\langle a \rangle \leq C_G(a)$, 当 $a \in C$ 时, $C_G(a) = G$。

【《应用近世代数》P72 证明】

理解:

对 $C(G), C_G(A), C_G(a)$ 的定义, 其共同特点都是从 G 中去找符合要求的元素, 区别在于它们所需要满足的要求依次放宽了 (即与之可以交换的元素的范围依次被进一步缩小)。

1.53 共轭、共轭类

设 G 是群, $a, b \in G$, 若存在 $g \in G$ 使 $gag^{-1} = b$, 则称 a 与 b **共轭**。容易验证, 群中元素之间的共轭关系是一种等价关系, 每一个等价类称为一个**共轭类**, 记作 $K_a = \{gag^{-1} | g \in G\}$。

性质:

中心内元素共轭类的特点:

(1) $a \in C(G)$ 的充分必要条件是 a 所在的共轭类只含 a 本身一个元素, 因而 G 可表示为 $G = C \cup (\bigcup\limits_{a \notin C} K_a)$。其中 $\bigcup\limits_{a \notin C}$ 是对非中心内的共轭类代表元求并; (这里就凸显出了中心的不同之处)

(2) 当 $|G| < \infty$ 时, 有 $|G| = |C| + \sum\limits_{a \notin C} |K_a|$。

【《应用近世代数》P73 证明】

理解:

由等价关系的性质可知, 一个群内所有的共轭类构成群的一个划分。如果我们把群的元素考虑为矩阵, 那么就更好理解了, 即 $P^{-1}AP = B, A = PBP^{-1}$, 这不就类似于矩阵的相似吗。

1.54 类方程

设 G 是有限群，C 是 G 的中心，则有 $|G| = |C| + \sum_{a \notin C} [G : C(a)]$。其中和式是对非中心内的共轭类的代表元求和。此方程称为**类方程**。【《应用近世代数》P74 证明】

1.55 共轭子群、自共轭子群、正规化子

设 G 是群，$H \leq G, g \in G$，则不难验证 $K = gHg^{-1}$ 也是一个子群，称为 H 的**共轭子群**，并称 K 与 H **共轭**。如果 H 是正规子群，则 $\forall g \in G$ 有 $gHg^{-1} = H$，即正规子群的共轭子群必是它自己，因此，**正规子群又称为自共轭子群**。【1-14 的 45 题例子】

设 $H \leq G$, H 所在的共轭类记作 K_H, 则可以表示为 $K_H = \{gHg^{-1} | g \in G\}$。当 $H \trianglelefteq G$ 时 $K_H = \{H\}$。若 H 不是 G 的正规子群，总可以找到一个包含 H 的子群 N，使 H 是 N 的正规子群，例如 H 本身就是。令 $N_G(H) = \{g | g \in G, gHg^{-1} = H\}$，不难验证 $N_G(H) \leq G$，且与 H 有以下关系：$H \trianglelefteq N_G(H)$。称 $N_G(H)$ 为 H 在 G 中的**正规化子**。【1-14 的 46 题例子】

1.56 同态、单同态、满同态、同态像、全原像、自然同态

设 $(G, \cdot), (G', \circ)$ 是两个群，若存在映射 $f : G \to G'$ 满足 $\forall a, b \in G$，均有 $f(a \cdot b) = f(a) \circ f(b)$，则称 f 是 G 到 G' 的一个**同态映射**（或简称同态）。若 f 是单射，则称 f 是**单同态**。若 f 是满射，则称 f 是**满同态**，这时称 G 与 G' 同态，记作 $G \overset{f}{\sim} G'$。若 f 是双射，则 f 就是 G 到 G' 的同构。所以同构是一种特殊的同态。

$\operatorname{Im} f = f(G)$ 称 G 在 f 作用下的**同态像**。$T \subset G'$，$f^{-1}(T)$ 表示子集 T 的**全原像**（注意是全原像哦，因为原像可以有多个）。

设 G 是群，$H \trianglelefteq G, G' = G/H$，作映射 $\varphi : a \mapsto aH (G \to G/H)$（商群的定义哦 ）。因为 $\varphi(ab) = abH = aHbH = \varphi(a)\varphi(b)$，所以 φ 是同态，且是满同态，故 $G \sim G/H$。此同态称为群 G 到它的商群 G/H 的**自然同态**。

理解：

同态描写了两个群的某种相似性。尽量用“同构和同态”来理解代数。比如研究对两个空间之间的线性变换，我们分别把它们的“基”抽取出来研究，从一个空间到另一个空间的“基”怎么变，空间就怎么变。其实线性空间中“基”的概念其实就源自于循环群的生成元。

1.57 同态核

设 f 是 G 到 G' 的同态，令 $K = \{a | a \in G, f(a) = e'\} = f^{-1}(e')$（其中 $e' \in G'$ 且为单位元哦），则称 K 是同态 f 的**核**，记作 $\ker f$（注意是针对 f 而言的）。

性质：

设 f 是 G 到 G' 的同态，$K = \ker f$，则

（1）$K \trianglelefteq G$;

（2）$\forall a' \in \operatorname{Im} f$，若 $f(a) = a'$，则 $f^{-1}(a') = aK$（把核找出来的一个作用，相当于把全原像都给找出来了，可以看做是个左陪集哦）;

（3）f 是单同态 $\Leftrightarrow K = \{e\}$。

【《应用近世代数》P80-81 证明】

理解：

同态核就是单位元 e 的全原像，它是 G 的一个子群。

1.58 自同态、自同构、自同态半群、自同构群、内自同构、内自同构群

设 f 是 G 到 G 本身的一个**同态**（或**同构**），则称 f 是 G 上的一个**自同态**（或**自同构**）。G 上的所有自同态的集合对变换的复合构成一个含幺半群，称为 G 上的**自同态半群**，记作 EndG。G 上的所有自同构的集合对变换的复合构成一个群，称为 G 上的**自同构群**，记作 AutG。【1-15 的 48 题和 50 题】

在群 G 中，取定一个元素 a，定义 G 上的一个变换 σ_a 为：对任何 $x \in G$ 有 $\sigma_a(x) = axa^{-1}$，则 σ_a 是 G 上的一个自同构，这个自同构称为一个**内自同构**。G 上的全体内自同构构成一个群，称为**内自同构群**，记作 InnG，即 InnG=$\{\sigma_a | a \in G, \text{对任何} x \in G \text{有} \sigma_a(x) = axa^{-1}\}$。

性质：

设 G 是群，则

（1）InnG $\trianglelefteq$AutG；

（2）$G/C \cong$InnG。

【《应用近世代数》P85 证明】

理解：

这些都是对于变换而言的哦！联系之前学的对称群等等，不要再理解为仅为置换操作了，像这些，比如双射操作同构，也是可逆的，组成的也是个对称群哦。

1.59 群作用

设 G 是一个群，Ω 是一个集合（称为目标集），若 $\forall g \in G$ 对应 Ω 上的一个变换 $g(x)$ 满足：（a）$e(x) = x, \forall x \in \Omega$；（b）$g_1 g_2(x) = g_1(g_2(x)), \forall x \in \Omega$。则称 G 作用于 Ω 上，$g(x)$ 称为 g 对 x 的作用。【《应用近世代数》P87-88 例子】

理解：

不难证明，$g(x)$ 是 Ω 上的一个可逆变换，对应关系是 G 到 Ω 上的变换群的一个同态。有了群对集合的作用这一概念，可以进一步利用群分析集合的性质。

1.60 轨道

设 Ω 为目标集，群 G 作用于 Ω 上，$a \in \Omega$，则集合 $\Omega_a = \{g(a)|_{g \in G}\}$，称为 Ω 在 G 作用下的一个**轨道**（即目标集的一个子集），a 称为此轨道的代表元。

性质：

（1）若在 Ω 中定义二元关系 $\sim$ 为：$a \sim b \Leftrightarrow \exists g \in G$ 使 $g(a) = b$，则 $\sim$ 是 Ω 中的一个等价关系，且每一个等价类 $\overline{a}$ 就是一个轨道 Ω；

（2）$b \in \Omega_a \Leftrightarrow \Omega_a = \Omega_b$，即轨道中任一元素都有资格作为代表元；

（3）$\{\Omega_a | a \in \Omega\}$ 构成 Ω 的一个划分，因而有 $|\Omega| = \sum_{a \in \Omega} |\Omega_a|$，其中和式是对轨道的代表元求和（可以看到目标集合 Ω 在群 G 的作用下被划分为轨道的并，反过来，可用轨道来研究群 G 的结构，并解决轨道长度与轨道数的问题）。

1.61 不动点、稳定子群

（1）设 $g \in G, a \in \Omega$，若 $g(a) = a$，则称 a 是 g 的一个**不动点**。以 a 为不动点的所有群元素的集合记作 $G_a = \{g | g \in G, g(a) = a\}$，有 $G_a \leq G$【《应用近世代数》P89 证明】。

（2）设群 G 作用于集合 Ω 上，$a \in \Omega$，则子群 $G_a = \{g | g \in G, g(a) = a\}$，称为 a 的**稳定子群**，又记作 $\text{Stab}_G a$。【1-16 的 51 题例子】

性质：

下面性质都是对于稳定子群而言的。

（1）**轨道公式**：$|\Omega_a| = [G : G_a]$；

（2）由轨道公式和 Lagrange 定理可得：（a）$|G| = |\Omega_a||G_a|$；（b）$|\Omega| = \sum_{a \in \Omega} [G : G_a]$，其中和式是对轨道的代表元求和；

（3）同一轨道上的元素的稳定子群是互相共轭的：$G_{g(a)} = gG_a g^{-1}$。

【《应用近世代数》P90 证明】

理解：

在置换操作下，G_a 实际上就是表示顶点 a 不动的那些置换操作（即从置换群中提取出来满足条件的相应元素）。

1.62 群的直积

设 G_1 G_2 是两个群，$G_1 \times G_2 = \{(a,b)|a \in G_1, b \in G_2\}$ 在 $G_1 \times G_2$ 中定义乘法：$(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2)$，则 $G_1 \times G_2$ 关于这种乘法构成群，并称 $G_1 \times G_2$ 是 G_1 和 G_2 的**直积**。【《应用近世代数》P104 证明】

理解：

群的直积可以把没有关联的群组合起来。

1.63 环、可换环

设 A 是一个非空集合，在 A 中定义两种二元运算，一种叫做加法，记作 $+$，另一种叫做乘法，记作 $\cdot$。且满足

（1）$(A,+)$ 是一个可换群;

（2）$(A,\cdot)$ 是一个半群；（也可以进一步构成群哦，没说不能是群，只是说至少得是半群）

（3）左、右分配律成立，即对于任何 $a,b,c \in A$，有 $a(b+c) = ab+ac, (a+b)c = ac+bc$。

则称代数系 $(A,+,\cdot)$ 是一个**环**。如果 $(A,+,\cdot)$ 对乘法也是可交换的（没说要是 Abel 群哦），则称 A 是**可换环**。

例子：

（1）Z 对 $+$ 和 $\cdot$ 构成可换环，称为**整数环**；Q, R, C 对 $+$ 和 $\cdot$ 构成环；

（2）$Z[i] = \{a+bi|a,b \in Z, i = \sqrt{-1}\}$ 对复数加法和复数乘法构成环，称为 **Gauss 整数环**；

（3）$(Z_n,+,\cdot)$ 是环，称为**整数模 n 的同余类（或剩余类）环**；

（4）$(M_n(Z),+,\cdot)$ 是一个环，其中 $M_n(Z) = \{(a_{ij})_{n\times n}|a_{ij} \in Z\}$（注意是方阵哦），称为**整数环上的全矩阵环**；

（5）$Z[x] = \{a_0 + a_1x + a_2x^2 + ... + a_nx^n|a_i \in Z, n \geq 0$整数$\}$（注意 n 的取值，说明多项式是有限的哦）对多项式加法和多项式乘法构成环，称为**整数环上的多项式环**。类似地，$(Q[x],+,\cdot)$ 是有理数域上的多项式环，$(R[x],+,\cdot)$，$(C[x],+,\cdot)$ 等也是多项式环；

（6）$(E(G),\oplus,\cdot)$ 是环，其中 $(G,+)$ 是一个加群，$E(G)$ 是 G 上的全体自同态的集合，定义 $(f\oplus g)(x) = f(x)+g(x), (f\cdot g)(x) = f(g(x)), \forall x \in G$，称为加群 G 上的**自同态环**。（再次理解，群的元素也可以是函数哦，这样就和分析学联系起来了）

【《应用近世代数》P116-117 证明】

理解：

（1）环的实质其实就一句话：环是有两种运算、对加法是可换群、对乘法是半群，并适合分配律的代数系统。判断一个代数系统是否为环时，可以先从条件（1）入手，即看它对加法是否构成可换群，若不是则直接否决。对于条件（3），因为环包含加法和乘法两种运算，它们在一起可能会“打架”，所以需要用左、右分配律来协调它们。

（2）对于环中加法和乘法的定义，也不用非得统一的数学运算，也可以用加法表和乘法表来进行定义，如【《应用近世代数》P118 的例 3.1.7】。其他代数系统也是一样的。

1.64 零元、负元、单位元、逆元、正则元或单位

（1）设 $(A,+,\cdot)$ 是一个环，加群 $(A,+)$ 中的单位元通常记作 0，称为**零元**。元素 a 在加群中的逆元记作 $-a$，称为 a 的**负元**；环中的**单位元**指乘法半群 $(A,\cdot)$ 中的单位元，记作 1。环中一个元素 a 的**逆元**指的是它在乘法半群中的逆元，记作 a^{-1}。

（2）环中的乘法可逆元又叫做**正则元**或**单位**，特别是“单位”这个名词不要与“单位元”混淆。

理解：

上述这些都是环内一些特殊的元素。

1.65 左零因子、右零因子、零因子

设 A 是一个环，$a,b\in A$，若 $ab=0$ 且 $a\neq 0$ 和 $b\neq 0$，则称 a 为**左零因子**，b 为**右零因子**。若一个元素既是左零因子又是有零因子，则称它为**零因子**。

1.66 整环、除环

（1）设 $(A,+,\cdot)$ 是环。若 $A\neq\{0\}$，可交换，且无零因子，则称 A 是**整环**；

（2）若 A 满足：（a）A 中至少有两个元 0 和 1，（b）$A^*=A\backslash\{0\}$ 构成乘法群（也就是说每个非零元均有逆元），则称 A 是一个**除环**；

【《应用近世代数》P120 例子】

例子：

实四元数除环【1-16 的 52 题】。

1.67 幂等元、幂零元

满足 $a^2=a$ 的元素称为**幂等元**。满足 $a^n=0,n\in Z^+$ 的元素称为**幂零元**。【1-16 的 53 题】

性质：

在一个整环中，除零元外无其他的幂零元，除零元与单位元外无其他的幂等元。【《应用近世代数》P122 证明】

1.68 子环、扩环

设 $(A,+,\cdot)$ 是一个环，S 是 A 的一个非空子集，若 S 对 $+$ 和 $\cdot$ 也构成一个环，则称 S 是 A 的一个**子环**，A 是 S 的一个**扩环**。$\{0\}$ 和 A 本身也是 A 的子环，这两个子环称为平凡子环。

性质：

对于一般的一个子集，检验它是否是子环，可以利用以下的性质：

（1）设 S 是环 A 的一个非空子集，则 S 是 A 的子环的充要条件是对任何 $a,b\in S$ 有 $a-b\in S$ 和 $ab\in S$；

（2）S_1,S_2 都是 A 的子环，则 $S_1\cap S_2$ 也是 A 的子环。

1.69 左理想、右理想、理想、单环

（1）设 A 是一个环，I 是它的一个子环，对任意的 $a\in I$ 和任意 $x\in A$，若满足（1）$xa\in I$，则称 I 是 A 的一个**左理想**；若满足（2）$ax\in I$，则称 I 是 A 的一个**右理想**；若同时满足性质（1）和（2），则称 I 是 A 的一个**理想**。如果 A 是可换环，则左理想也是右理想，因而也是理想。$\{0\}$ 和 A 本身也是 A 的理想，称为**平凡理想**。【1-16 的 54 题，1-17 的 55 题】

（2）如果一个环内无非平凡理想，则称这个环为**单环**。

性质：

检验一个非空子集 H 是理想的充分必要条件为：

环 A 中非空子集 H 的理想的充分必要条件是满足 (1)$\forall a,b\in H$ 有 $a-b\in H$；(2) $\forall a\in H$ 和 $\forall x\in A$ 有 $ax,xa\in H$。（也就是先验证它是个子环，然后再看是否满足理想的定义）【《应用近世代数》P125 例子】

当 A 是可换环时，条件（2）可以简化为 $ax\in H$。因此在判断前可以先判断 A 是否是可换环。对上述性质左适当修改可用于判断 H 是否是左理想或右理想。

理解：

（1）我们把条件 $\forall x\in A$ 有 $xa,ax\in I$ 称为 I 对 A 是**吸收的**。**理想就是对环吸收的子环**。正规子群是对群元素可交换的子群。环中的理想和群中的正规子群是两个对应的概念，有类似的作用。

（2）同群论中陪集的概念一样，“左”和“右”都是针对最大的（即非子集的）集合中元素而言的，看它在左边还是右边。其实，上面的这些概念都和群论是对应的：“子环、左理想、右理想、理想、单环、极大理想”对应于“子群、左陪集、右陪集、正规子群、单群、极大正规子群”

1.70 生成子环、生成理想

（1）设 A 是环，S 是 A 的一个非空子集，则 A 的包含 S 的最小子环称为**由 S 生成的子环**或称为 S **的生成子环**，记作 $[S]$，它是 A 的包含 S 的所有子环的交。

（2）包含 S 的最小理想称为**由 S 生成的理想**或称为 S **的生成理想**，记作 (S)，它是包含 S 的所有理想的交。

例子：

在 $(Z,+,\cdot)$ 中整数 m 的生成理想为 $(m)=\{km|k\in\mathbb{Z}\}=m\mathbb{Z}$，在 $(F[x],+,\cdot)$ 中元素 x 的生成理想为 $(x)=\{xf(x)|f(x)\in F[x]\}=\{a_1x+a_2x^2+...+a_nx^n|a_i\in F,n\in Z^+\}$。更多例子参见【《应用近世代数》P126 例子】。

理解：

抓住两点：（1）这些概念都是针对于 A 中的一个非空子集 S 而言的；（2）最小。

1.71 商环

设 I 为环 A 的子环，在 A 中定义关系 $\sim$：$a\sim b$，若 $a+(-b)=a-b\in I$，则关系 $\sim$ 对加法为同余关系，a 所在的等价类为 $a+I$。关系 $\sim$ 对乘法也为同余关系的充分必要条件是 I 为 A 的理想。若 I 为理想，则在商集合 $A/\sim=A/I$ 中可定义加法、乘法为：$(a+I)+(b+I)=(a+b)+I,\forall a,b\in A$，$(a+I)\cdot(b+I)=ab+I,\forall a,b\in A$。$A/I$ 对这种加法与乘法也构成环，称为 A 对 I 的**商环**。

也可以定义为：设 A 是环，I 是 A 的一个理想，A 作为加群关于 I 的商群 A/I 对模 I 的加法与乘法（即上面所定义的那样）所做成的环，称为 A 关于 I 的**商环**或称为 A 模 I 的同余类环，仍记作 A/I。

理解：

对 A/H 的理解，也可以与商群类似理解。简而言之，I 是 A 的一个理想（类似于商群中 H 是 G 的一个正规子群），$A/I=\{a+I|a\in A\}$（类似于商群中 $G/H=\{aH|a\in G\}$）。所以正规子群和理想在群和环中扮演了比较重要的作用哦！

1.72 极大理想

设 M 是环 A 的非平凡理想，若有理想 H 且 $H\supset M$，则 $H=A$，就称 M 是 A 的一个**极大理想**。【1-18 的 59 题】

1.73 环同态、环同构、同态核

（1）设 A 和 A' 是两个环，若有一个 A 到 A' 的映射 f 满足以下条件：对任何 $a,b\in A$ 有 $f(a+b)=f(a)+f(b)$，$f(ab)=f(a)f(b)$，则称 f 是一个 A 到 A' 的**同态**。如果 f 是双射，则称 f 是 A 到 A' 的一个**同构**。【1-17 的 56 题，57 题和 58 题】

（2）设 f 是环 A 到环 A' 的一个同态，则 A' 的零元 $0'$ 的全部原像 $f^{-1}(0')$ 称为 f 的**同态核**，记作 $\ker f$。即 $\ker f=f^{-1}(0')=\{x\in A|f(x)=0'\}$（注意理解，“零元”是加群 $(A,+)$ 中的单位元哦 ~）。同态核是 A 的一个理想。f 是单同态的充分必要条件是 $\ker f=\{0\}$。

理解：

与群同态相比，对于环，保持运算指的是两种运算。因为这里的运算都很规整，$+$ 或 $\cdot$，因为环嘛，对运算进行了限制，不像群那样开放。

1.74 分式域

设 D 是一个整环，则包含 D 的最小域可表示为 $P=\{\frac{b}{a}|a,b\in D且a\neq 0\}$，其中 $\frac{b}{a}=ba^{-1}$，称 P 为 D 的**分式域**，记作 $P(D)$。【《应用近世代数》P132-133 证明】

1.75 因子、倍元、相伴、真因子

设 D 是有单位元的整环，$a,b\in D$。

（1）若有 $c=ab$，则称 a 是 c 的**因子**，c 是 a 的**倍元**，并称 a 可整除 c，记作 $a|c$。

（2）若 $a|b$ 且 $b|a$，则称 a 与 b **相伴**，记作 $a\sim b$（是等价关系哦）。

（3）若 $c=ab$ 且 a 和 b 都是不可逆元，则称 a 是 c 的**真因子**。

性质：

（1）可逆元是任何元素的因子；【因为若 $u\in U(D),a\in D$，则 $a=u(u^{-1}a)$】

（2）两元素相伴，则它们差一可逆元因子；【设 $a\sim b$, 则 $b=ua,a=vb$，得 $b=uvb$，由消去律得 $uv=1$，所以 u 和 v 都是可逆元】

（3）可逆元无真因子，且所有可逆元都与 1 相伴。【设 $u\in U(D),u=ab$，可得 $u^{-1}u=u^{-1}ab=a(u^{-1}b)=(u^{-1}a)b=1$，所以 a,b 都是可逆元】

理解：

（1）元 0 是任何元素的倍元，单位元 1 是任何元素的因子。相伴关系是等价关系。

（2）对于真因子的理解，类比对素数的分解，素数分解后会有 1,1 是可逆元，那么分解后的两个数不都是不可逆元了，所以不是真因子。把这里的“真”理解为“有效”，即不是 1 和它本身外的分解式有效的，是“真”的。回到这里则类比定义为非素数分解得到的因子不是真因子。同样地，后面既约元的定义也很像素数，即无真因子，也就是分解都是“假”的，“无效”的，也就是类似于素数的 1 和它本身。所以把既约元（不可约元）理解为素数。这也迎合了在下面的惟一分解整环是类比于算术基本定理，算术基本定理分解出的也都是素数，而惟一分解整环分解出的都是既约元。

值得特别注意的是，一个区别在于，既约元和下面的惟一分解整环的分解元素都是对于整环中“非零”和“不可逆”元而言的。

1.76 不可约元或既约元、素元

设 $a,b\in D,p\in D^*\backslash U(D)$，其中 D^* 表示 $D\backslash\{0\}$，$U(D)$ 表示环中所有可逆元的集合（因为可逆元无真因子，所以要先排除可逆元来进行一般情况的讨论）。

（1）若 p 无真因子，则称 p 是**不可约元或既约元**；

（2）若当 $p|ab$ 时必有 $p|a$ 或 $p|b$，则称 p 是**素元**。

【1-18 的 60 题，判断元素是否为既约元】

性质：

设 D 是有单位元的整环，则 D 中的素元必是既约元，但一个既约元不一定是素元。【《应用近世代数》P135 证明和例题 3.4.1 的反例】

1.77 最大公因子

设 D 是有单位元的整环，$a,b\in D$，若有 $d\in D$ 满足（1）$d|a,d|b$；（2）若有 d' 满足 $d'|a$ 和 $d'|b$，则 $d'|d$。则称 d 是 a 和 b 的**最大公因子**，并记作 $d\sim(a,b)$。

1.78 互素

设 $a,b\in D$，若 $(a,b)\sim 1$，则称 a 和 b **互素**。

1.79 惟一分解整环

设 D 是一个有单位元的整环，若对任何一个 $a\in D^*\backslash U(D)$ 有

（1）a 可分解为有限个既约元之积：$a=p_1p_2...p_s$，其中 $p_i(i=1,2,...,s)$ 为既约元；（与算术基本定理作类比，同时也能从素数的角度来理解既约元）

（2）若 $a=p_1p_2...p_s=q_1q_2...q_t$，其中 $p_i(1\le i\le s),q_j(1\le j\le t)$ 均为既约元，则 $s=t$，且适当调换次序后可使 $p_i\sim q_i(i=1,2,...,s)$（即相伴），则称 D 是**惟一分解整环**。

性质：

（1）设 D 是唯一分解环，则 D 中任何两个（不全为 0）元素均有最大公因子，因而 D 中每一个既约元也是素元。【《应用近世代数》P137-138 证明】（该性质将 2 个概念合二为一了）

（2）设 D 是惟一分解整环，则 $D[x]$ 也是惟一分解整环。【《应用近世代数》P144-145 证明】

理解：

惟一分解整环解决了分解的存在性和惟一性问题，它是算术基本定理推广而来的。

1.80 主理想、主理想整环

环中由一个元素生成的理想称为**主理想**。如果在一个有单位元的整环中每一个理想都是主理想，则此环称为**主理想整环**。

性质：

主理想整环是惟一分解整环的。【《应用近世代数》P139-140 证明】

1.81 欧氏整环

设 D 是一个有单位元的整环，若存在一个 D^* 到正整数集合的映射 v 满足对任何 $a \in D^*, b \in D$ 均有 $q, r \in D$ 使 $b = qa + r$，其中 $r = 0$ 或 $v(r) < v(a)$，则称 D 是一个**欧氏整环**。$v(a)$ 称为 a 的范数。

【1-18 的 61 题，证明 Gauss 整数环是欧氏整环】

性质：

欧氏整环是主理想整环，因而是惟一分解整环。【《应用近世代数》P141-142 证明】【《应用近世代数》P142 例子】

1.82 本原多项式

设 $\varphi(x) = a_0 + a_1 x + ... + a_n x^n \in D[x]$ 且 $\varphi(x) \neq 0$，若 $(a_0, a_1, a_2, ..., a_n) \sim 1$，则称 $\varphi(x)$ 是**本原多项式**。（其中设 D 是惟一分解整环，$D[x]$ 是 D 上的多项式环，显然 $D \subset D[x]$，$U(D[x]) = U(D)$,$D[x]$ 也是整环）

性质：

Gauss 引理：两个本原多项式之积仍为本原多项式。【《应用近世代数》P144 证明】

1.83 域、有限域

（1）若 A 是一个可换的除环，则 A 是**域**；

（2）具有有限个元素的域，称为**有限域**。Z_p 是最简单的有限域。

理解：

域的概念其实就是：环 $(A, +, \cdot)$ 含有 0 和 1，且 $(A^*, \cdot)$ 是可换群。由于域是一种特殊的环，所以有关环的性质都适合域，而且有些性质更为简单，例如，域内没有非平凡理想，因为两个域之间的同态只有零同态核同构；由于域中每一个非零元素都有逆元，域内没有零因子，也不存在因子分解问题（注意这里指的不是多项式分解问题哦）。

1.84 子域、扩域、素域

设 $(K, +, \cdot)$ 是域，F 是 K 的非空子集，且 $(F, +, \cdot)$ 也是域，则称 F 是 K 的**子域**，K 是 F 的**扩域**，记作 $F \leq K$。

设 S 是域 F 中的一个非空子集，则包含 S 的最小子域，称为由 S 生成的子域，记作 $\langle S \rangle$。由元素 1 生成的子域称为**素域**。

性质：

设 F 是域，则元素 1 在 $(F, +)$ 中的阶数或为某个素数 p，或为无穷大。

理解：

素域是任何一个域中最小的域，并且表征了这个域的特性，因此，首先应搞清楚素域的结构。

1.85 特征

设 F 是域，若元素 1 在 $(F,+)$ 中的阶数为素数 p，则称 p 为域 F 的**特征**。若元素 1 在 $(F,+)$ 中的阶数为无穷大，则称 F 的特征为 0，F 的特征记作 chF，故有 $chF=\begin{cases} p, & 0^+(1)=p, \\ 0, & 0^+(1)=\infty. \end{cases}$。

性质：

设 F 是域，F_0 是 F 的素域（素域是由 1 生成的，但没说只有 1，1 可以生成很多大小（元素个数多少）不同的素域），则 $F_0\cong\begin{cases} (Q,+,\cdot), & chF=0, \\ (Z_p,+,\cdot), & chF=p. \end{cases}$。【《应用近世代数》P156 证明】

例子：

设 $Z[i]$ 为 Gauss 整数环，求域 $Z[i]/(2+i)$ 的特征。

令 $F=Z[i]/(2+i)$，考虑 $\overline{1}$ 在加群 $(F,+)$ 中的阶。因为 $5=(2+i)(2-i)=(2+i)$（注意后面的 $(2+i)$ 是由 $2+i$ 生成的理想），故 $\overline{5}=\overline{0}$，所以 $0^+(\overline{1})=5$，$chF=5$。

理解：

从上面的性质可以将域分为两类：(1) 若 $chF=0$，则 F 是 Q 上的扩域，是无限域；(2) 若 $chF=p$，则 F 是 Z_p 上的扩域，这时 F 可以是有限域，也可以是无限域。当然，如果 F 是有限域，则 chF 必然是某个素数。

1.86 向量空间或线性空间

设 V 是一个加群，F 是一个域，对任何 $\alpha\in F, v\in V$ 定义一个元素 $\alpha v\in V$ 满足以下性质：$\alpha,\beta\in F, u,v\in V$ 有

(1) $\alpha(u+v)=\alpha u+\alpha v$；

(2) $(\alpha+\beta)u=\alpha u+\beta u$；

(3) $\alpha(\beta u)=(\alpha\beta)u$；

(4) $1v=v$。

则称 V 是域 F 上的一**个向量空间或线性空间**。

理解：

上述定义不仅把数 F 上的向量空间推广到了一般的域 F 上的向量空间，而且利用群的概念从形式上简化了定义的叙述。

1.87 扩张次数、有限扩张、无限扩张、望远镜公式

对于域 F 及它的扩域 K，由于 **K 是 F 上的线性空间**，此空间的维数就称为 K 对 F 的**扩张次数**，记作 $(K:F)$。当 $(K:F)$ 有限时，称 K 是 F 上的**有限扩张**，否则称为**无限扩张**。

如果 F,K,E 都是域，且 $F\subseteq K\subseteq E$，都是有限扩张，则有以下的所谓“**望远镜公式**”：$(E:F)=(E:K)(K:F)$。

【《应用近世代数》P157 例子，主要还是找基来确定维数】

1.88 代数元、超越元、r 次代数元、代数数、超越数

扩张次数反映了扩域与子域之间的相对大小，但还没有反映它们的元素在性质上的差别。我们对域中的元素作以下的分类：设 K 是 F 的扩域，$u\in K$。

(1) 若 u 是 F 上的一个多项式 $f(x)$ 的根，则称 u 是 F 上的**代数元**，否则称为**超越元**。

(2) 设 u 在 F 上的最小多项式（指 u 是根的次数最低的首 1 多项式）为 $m(x)$，且 $\deg m(x)=r$，则称 u 是 F 上的 r **次代数元**。

(3) 有理数域 Q 上的代数元称为**代数数**，Q 上的超越元称为**超越数**。例如 $\sqrt{2},1+i$ 等都是代数数，而 π,e 是超越数。

理解：

这样，我们把扩域上的元素相对于子域分成两大类：代数元和超越元。

1.89 F 添加 S 所构成的扩域、单扩张

设 E 是 F 的扩域，$S \subseteq E$ 是一个非空子集，我们把包含 F 与 S 的最小子域称为 **F 添加 S 所构成的扩域**，记作 $F(S)$。添加一个元素 $u \in E$ 所得之扩域记作 $F(u)$，称为 F 上的**单扩张**。

性质：

对于单扩张有以下明显的表达式。设 E 是 F 的扩域，$u \in E$，则：

（1）$F(u) = \{a_0 + a_1 u + ... + a_{n-1}u^{n-1} | a_i \in F\} \cong F[x]/(m(x))$，当 u 是 F 上的代数元，且 $m(x)$ 是 u 在 F 上的最小多项式，$\deg m(x) = n$；

（2）$F(u) = \{\dfrac{f(u)}{g(u)} | f(x), g(x) \in F[x], g \neq 0\} \cong F(x)$ 的分式域，当 u 是 F 上的超越元。

【《应用近世代数》P158-159 证明】

1.90 分裂域或根域

设 $f(x) \in F[x], E_f$ 是 F 的扩域且满足以下条件：（1）$f(x)$ 在 E_f 上可分裂为线性因子；（2）E_f 可由 F 上添加 $f(x)$ 的所有根而得到。则称 E_f 是 $f(x)$ 在 F 上的**分裂域或根域**。

1.91 有限域、Galois 域

首先讨论如何构造一个有限域。我们已经知道，一个有限域 F 的特征必然是某个素数 p，F 的素域为 Z_p，设 F 对 Z_p 的扩张次数为 $n : (F, Z_p) = n$，则不难得到 F 的元素个数为 $|F| = p^n$。如何把这个域的元素都表示出来呢？我们用分裂域的理论：

考虑在多项式环 $Z_p[x]$ 中任取一个 n 次不可约首 1 多项式（首项系数为 1 的多项式）$q(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$，令 $E = Z_p[x]/(q(x)) = \{\overline{b_0 + b_1 x + ... + b_{n-1}x^{n-1}} | b_i \in Z_p\}$，则 E 是域，且其元素个数为 p^n。E 包含 $q(x)$ 的一个根 $\overline{x}$。设 α 是 $q(x)$ 的任意一个根，则 E 也可以表示为 $E = \{b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} | b_i \in Z_p\}$。【《应用近世代数》P127 的例 3.2.4 推导】【1-20 的 65 题例子】

运用 4.4 中的定理 3，我们可任取一个 Z_p 上的 n 次不可约多项式来构造 p^n 阶有限域。我们把 p^n 阶有限域记作 $GF(P^n)$ 或 F_{p^n}，称为 **Galois 域**。

推论：

（1）$GF(p^n) \cong E_f \cong Z_p[x]/(p(x))$，其中 $p(x)$ 为 Z_p 上任一 n 次不可约多项式，$f(x) = x^{p^n} - x$。并由扩域的构造，得 $(GF(p^n) : Z_p) = n$；

（2）有限域 $GF(p^n)$ 是由多项式 $f(x) = x^{p^n} - x \in Z_p[x]$ 在其分裂域上的全部根组成。

理解：

有限域在计算机科学、通信理论和组合理论等方面有很多应用，即便是对于非数学专业的其他领域来说，应用都很多。由于它的元素个数是有限的，因为它的结构比较清楚。

1.92 本原元、n 次本原元、n 次本原多项式

$GF(p^n)$ 的非零元的集合 $GF(p^n)^*$ 是一个乘群，具有以下性质：

（1）$GF(p^n)^*$ 是一个 $p^n - 1$ 阶循环群。特别是有 $(Z_p^*, \cdot) \cong C_{p-1}$。$GF(p^n)^*$ 的生成元又叫**本原元**。

（2）乘群 $GF(p^n)^*$ 中 $p^n - 1$ 阶的元素 α 称为域 $GF(p^n)$ 的 **n 次本原元**。$GF(p^n)$ 的本原元 α 在 Z_p 上的最小多项式称为 Z_p 上的 **n 次本原多项式**。

【《应用近世代数》P173 例子，在 AES 密码标准中的例子】

2 矩阵等式

1. 维数定理： $\dim(V_1) + \dim(V_2) = \dim(V_1 + V_2) + \dim(V_1 \cap V_2)$。

理解：

可以看出，子空间和的维数一般比子空间的维数之和小。从几何直观上理解，“子空间的和” 其实可以理解成一种升维，“子空间的交” 其实可以理解成一种降维，可以在二维平面上将 x 轴和 y 轴看作 V_1, V_2，以及在三维空间中将 xOy, xOz 平面看作 V_1, V_2 来直观理解。

2. A 可逆的充要条件是 A 不具有非零特征值，此时有 $\operatorname{tr} A = \sum\limits_{i=1}^{n} a_{ii} = \sum\limits_{i=1}^{n} \lambda_i$，以及 $\det A = \prod\limits_{i=1}^{n} \lambda_i$。

3. 线性变换 T 在基底 $(\varepsilon_1, ..., \varepsilon_n)$ 下的矩阵为 A，在 $(\varepsilon_1', ..., \varepsilon_n')$ 下的矩阵为 B，若 $(\varepsilon_1', ..., \varepsilon_n') = (\varepsilon_1, ..., \varepsilon_n)C$，则有 $B = C^{-1}AC$。

理解：

线性变换与矩阵特征值的关系，即在基底 $(\varepsilon_1, ..., \varepsilon_n)$ 下，$T\alpha = \lambda\alpha$ 可转换为 $Ax = \lambda x$，其中 $\alpha = \sum\limits_{i=1}^{n} x_i\varepsilon_i$，$x_i$ 为表出系数（《矩阵理论》P13 推导过程）。这样做的目的是把抽象的问题转换为具体的问题，即转换为对矩阵的研究。

4. 矩阵的三角分解：

(1) 设 $A \in C_n^{n\times n}, A = U_1R = LU_2$ 唯一，其中 U_1, U_2 是酉矩阵，R 是正线上三角复矩阵，L 是正线下三角复矩阵。类似地，$A \in R_n^{n\times n}, A = Q_1R = LQ_2$ 唯一，其中 Q_1, Q_2 是正交矩阵，R 是正线上三角实矩阵，L 是正线下三角实矩阵。(《矩阵理论 P86 证明》)

(2) 设 A 是实对称正定矩阵，则存在唯一正线上三角实矩阵 R，使得 $A = R^TR$ 唯一。类似地，设 A 是正定 Hermite 矩阵，则存在唯一正线上三角复矩阵 R，使得 $A = R^HR$ 唯一。(《矩阵理论》P88 证明)

(3) 设 $A \in C_n^{n\times n}$，用 D 表示对角矩阵，则下列命题等价：(a)A 的各阶顺序主子式不等于零 (即可逆)；(b)$A = LR^*$ 唯一，且 L 的主对角线上元素不为零；(c)$A = L^*DR^*$ 唯一，且 D 的主对角线上元素不为零；(d)$A = L^*R$ 唯一，且 R 的主对角线上元素不为零。(《矩阵理论》P89 证明)

(4) 设 $A \in C_m^{m\times n}$，则存在 $A = \begin{pmatrix} L & O \end{pmatrix} U$，其中 L 是 m 阶正线下三角复矩阵，U 是 n 阶酉矩阵。设 $A \in C_n^{m\times n}$，则存在 $A = U \begin{pmatrix} R \\ O \end{pmatrix}$，其中 U 是 m 阶酉矩阵，R 是 n 阶上三角复矩阵。(《矩阵理论》P92 证明)

(5) 设 $A \in C_m^{m\times n}$，$A = LU$ 唯一，其中 L 是 m 阶正线下三角矩阵，$U \in U_m^{m\times n}$ 表示以 m 个两两正交的单位向量为行组成的矩阵的集合。设 $A \in C_n^{m\times n}$，$A = UR$ 唯一，其中 R 是 n 阶正线上三角矩阵，$U \in U_n^{m\times n}$ 表示以 n 个两两正交的单位向量为列组成的矩阵的集合。(《矩阵理论》P92 证明)

(6) 设 $A \in C_r^{m\times n}$，则存在酉矩阵 $U \in C^{m\times m}, V \in C^{n\times n}$ 及 r 阶正线下三角矩阵 L，使得 $A = U \begin{pmatrix} L & O \\ O & O \end{pmatrix} V$。设 $A \in C_r^{m\times n}$，则存在酉矩阵 $U \in C^{m\times m}, V \in C^{n\times n}$ 及 r 阶正线上三角矩阵 R，使得 $A = U \begin{pmatrix} R & O \\ O & O \end{pmatrix} V$。(《矩阵理论》P94 证明)

理解：

施密特正交化过程的直观理解：假设有任意三个向量 $\alpha_1, \alpha_2, \alpha_3$，现在要将它们正交化为 $\beta_1, \beta_2, \beta_3$。首先，初始化 $\beta_1 = \dfrac{\alpha_1}{\|\alpha_1\|}$。然后，用 β_1, β_2 来表示 $\alpha_2 = k_{21}\beta_1 + k_{22}\beta_2$，有 $\beta_2 = \dfrac{\alpha_2 - k_{21}\beta_1}{k_{22}}$，其中系数 k_{21}, k_{22} 为未知，将 α_2 与 β_1 做内积后得 k_{21}，并将 k_{22} 设置为归一化系数。最后，用 $\beta_1, \beta_2, \beta_3$ 来表示 $\alpha_3 = k_{31}\beta_1 + k_{32}\beta_2 + k_{33}\beta_3$，有 $\beta_3 = \dfrac{\alpha_3 - k_{31}\beta_1 - k_{32}\beta_2}{k_{33}}$，其中 k_{31}, k_{32}, k_{33} 为未知，将 α_3 与 β_1, β_2 做内积后得 k_{31}, k_{32}，并将 k_{33} 设置为归一化系数。对于一般情形，以此类推即可一一求得。

5. 矩阵的谱分解：

(1) 设 $A \in C^{n\times n}$ 是单纯矩阵或正规矩阵，则 A 可分解为一系列幂等矩阵 $A_i (i = 1, 2, ..., n)$ 的加权和，即 $A = \sum\limits_{i=1}^{n} \lambda_i A_i$，其中 λ_i 是 A 的特征值。(《矩阵理论》P96 证明)

(2) (shur 分解) 设 $A \in C^{n\times n}$，则存在酉矩阵 U，使得 $A = URU^H$，其中 R 是一个上三角矩阵且主对角线上的元素为 A 的特征值。(《矩阵理论》P101 证明)

性质：

(1) 谱分解中的 A_i 具有如下性质：(a) 幂等性：$A_i^2 = A_i$；(b) 分离性：$A_iA_j = O (i \neq j)$；(c) 可加

性：$\sum_{i=1}^{n} A_i = E_n$。上述 3 条是对于单纯矩阵和正规矩阵都满足的，除此之外，正规矩阵的谱分解中还有 $A_i^H = A_i$ 成立。

(2) 对于正规矩阵的谱分解所得到的 A_i，不仅可以看做是正交投影算子，而且还满足 (a)A_i 是唯一的；(b)$\text{rank}(A_i) = r_i (i = 1, 2, ..., k)$ 且 $\sum_{i=1}^{k} r_i = n$。（《矩阵理论》P104 证明）

理解：

与矩阵的相似对角化在大规模科学计算问题中的应用类似，可将对矩阵 A 的幂乘问题进行如下转换：$A^l = \sum_{i=1}^{n} \lambda_i^l A_i$。

6. 矩阵的最大秩分解：

设 $A \in C_r^{m\times n}$，则存在矩阵 $B \in C_r^{m\times r}, D \in C_r^{r\times n}$，使得 $A = BD$。（《矩阵理论》P114 证明）

性质：

设 $A \in C_r^{m\times n}$，且 $A = B_1D_1 = B_2D_2$ 均为 A 的最大秩分解，则 (a) 存在 r 阶可逆矩阵 Q，使得 $B_1 = B_2Q, D_1 = Q^{-1}D_2$；(b)$D_1^H(D_1D_1^H)^{-1}(B_1^HB_1)^{-1}B_1^H = D_2^H(D_2D_2^H)^{-1}(B_2^HB_2)^{-1}B_2^H$。（《矩阵理论》P116 证明）

7. 矩阵的奇异值分解：

设 $A \in C_r^{m\times n}, \sigma_1, \sigma_2, ..., \sigma_r$ 是 A 的 r 个正奇异值，则存在 m 阶酉矩阵 U 及 n 阶酉矩阵 V，使得 $A = U\begin{pmatrix} D & O \\ O & O \end{pmatrix}V$，其中 $D = \text{diag}(\delta_1, \delta_2, ..., \delta_r)$，而 δ_i 是满足 $|\delta_i| = \sigma_i (i = 1, 2, ..., r)$ 的复数。（《矩阵理论》P120 证明）

性质：

一些补充性质见《矩阵理论》P121。

8. 设 $\lim_{k\to+\infty} A^{(k)} = A$, $\lim_{k\to+\infty} B^{(k)} = B$，其中 $A^{(k)}, B^{(k)}, A, B$ 为适当阶的矩阵，$a, b \in C$，则：

(1) $\lim_{k\to+\infty}(aA^{(k)} + bB^{(k)}) = aA + bB$；

(2) $\lim_{k\to+\infty} A^{(k)}B^{(k)} = AB$；

(3) 当 $A^{(k)}$ 与 A 均可逆时，$\lim_{k\to+\infty}(A^{(k)})^{-1} = A^{-1}$。（《矩阵理论》P159 证明）

3 矩阵不等式

1. 如果 $\|\cdot\|_m : C^{n\times n} \to R$ 是一相容的矩阵范数，则对任一 $A \in C^{n\times n}$，有 $|\lambda_i| \le \|A\|_m$，其中 $_i$ 是 A 的特征值。（《矩阵理论》P64 证明）

2. 设 $A = A^H$，则 $\|A\|_2 \le \|A\|_\infty \le \|A\|_1 \le n\|A\|_2$。（PPT CH4P1 证明）

3. 特征值界的代数估计：

(1) (schur 不等式) 设 $A = (a_{ij}) \in C^{n\times n}$ 的特征值为 $\lambda_1, \lambda_2, ..., \lambda_n$，则 $\sum_{i=1}^{n} |\lambda_i|^2 \le \sum_{i=1}^{n}\sum_{j=1}^{n} |a_{ij}|^2 = \|A\|_F^2$，且等号成立当且仅当 A 为正规矩阵。（《矩阵理论 P》126 证明）

(2) (Hirsch) 设 $A = (a_{ij}) \in C^{n\times n}$ 的特征值为 $\lambda_1, \lambda_2, ..., \lambda_n$，则有：

(a) $|\lambda_i| \le n\max_{i,j}|a_{ij}|$；(b) $|\text{Re}(\lambda_i)| \le n\max_{i,j}|b_{ij}|$；(c) $|\text{Im}(\lambda_i)| \le n\max_{i,j}|c_{ij}|$。

其中，$B = (b_{ij}) = (A + A^H)/2$, $C = (c_{ij}) = (A - A^H)/2$，分别为 Hermite 矩阵和反 Hermite 矩阵，且 A, B, C 的特征值分别为 $\{\lambda_1, \lambda_2, ..., \lambda_n\}, \{\mu_1, \mu_2, ..., \mu_n\}, \{i\gamma_1, i\gamma_2, ..., i\gamma_n\}$，且满足 $|\lambda_1| \ge |\lambda_2| \ge ... \ge |\lambda_n|, \mu_1 \ge \mu_2 \ge ... \ge \mu_n, \gamma_1 \ge \gamma_2 \ge ... \ge \gamma_n$。（《矩阵理论》P128 证明）

(3) (Bendixson) 设 A 为 n 阶实矩阵，则 A 的任一特征值 λ_i 满足 $|\text{Im}(\lambda_i)| \le \sqrt{\frac{n(n-1)}{2}}\max_{i,j}|c_{ij}|$。（《矩阵理论》P128 证明）

(4) 设 $A \in C^{n\times n}, B, C, \lambda_i, \mu_i, \gamma_i$ 定义同上，则:

(a)$\mu_n \le \text{Re}(\lambda_i) \le \mu_1$；(b)$\gamma_n \le \text{Im}(\lambda_i) \le \gamma_1$。（《矩阵理论》P130 证明）

(5) (Browne) 设 $A \in C^{n\times n}$ 的特征值为 $\lambda_1, \lambda_2, ..., \lambda_n$，奇异值为 $\sigma_1 \le \sigma_2 \le ... \le \sigma_n$，则有 $\sigma_n \le |\lambda_i| \le \sigma_1 (i = 1, 2, ..., n)$。(《矩阵理论》P131 证明)

(6) (Hadamard 不等式) 设 $A \in (a_{ij}) \in C^{n\times n}$，则有：$\prod_{i=1}^{n} |\lambda_i(A)| = |\det A| \le [\prod_{j=1}^{n} (\sum_{i=1}^{n} |a_{ij}|^2)]^{\frac{1}{2}}$。(《矩阵理论》P132 证明)

理解：

在实际应用中的大量问题，往往不需要精确地计算出矩阵的特征值，仅需估计出它们所在的范围就够了。例如，线性代数方程组迭代求解收敛性的分析，要估计一个矩阵的特征值是否都在复平面的单位圆内；与差分法的稳定性相关的问题，要判定矩阵的特征值是否都落在单位圆上；系统与控制理论中，通过估计矩阵特征值是否都有负实部，即是否都位于复平面的左半平面内，便可知系统的稳定性；等等。

4. 特征值界的几何估计：

(1) 设 $A = (a_{ij}) \in C^{n\times n}$，则 A 的任一特征值 $\lambda_i \in S = \bigcup_{j=1}^{n} S_j (i = 1, 2, ..., n)$。且对于列盖尔圆盘同理。(《矩阵理论》P134 证明)

(2) 设 n 阶方阵 A 的 n 个盖尔圆盘中有 k 个的并形成一个连通区域，且它与余下的 $n-k$ 个圆盘都不相交，则在这个区域中恰好有 A 的 k 个特征值。(《矩阵理论》P136 证明)

(3) 只要 S 为可逆矩阵，$S^{-1}AS$ 就和 A 有相同的特征值，所以可以把盖尔圆盘定理应用于 $S^{-1}AS$ 得到新的结果，对 S 的某个选择，所得的界就可能更精准。一个特别方便的选择是取 $S = D = \mathrm{diag}(p_1, p_2, ..., p_n), p_i > 0 (i = 1, 2, ..., n)$，记 $r_i = \frac{1}{p_i} \sum_{j=1, j\ne i}^{n} |a_{ij}| p_j, Q_i = \{z \in C : |z - a_{ii}| \le r_i\}$，和 $t_j = p_j \sum_{i=1, i\ne j}^{n} \frac{|a_{ij}|}{p_i}, P_j = \{z \in C : |z - a_{ii}| \le t_j\}$。则有：设 $A = (a_{ij}) \in C^{n\times n}, p_1, p_2, ..., p_n$ 为一组正数，则 A 的任一特征值 $\lambda_i \in (\bigcup_{i=1}^{n} Q_i) \cap (\bigcup_{j=1}^{n} P_j)$。(《矩阵理论》P139 证明)

(5) 设 $A = (a_{ij}) \in C^{n\times n}$，则谱半径 $r(A)$ 满足：(a) $r(A) \le \min\{\max_i \sum_{j=1}^{n} |a_{ij}|, \max_j \sum_{i=1}^{n} |a_{ij}|\}$；(b) $r(A) \le \min_{p_1, p_2, ..., p_n > 0} \max_{0\le n} \frac{1}{p_i} \sum_{j=1}^{n} p_j |a_{ij}|$ 和 $r(A) \le \min_{p_1, p_2, ..., p_n > 0} \max_{1\le j\le n} \frac{1}{p_j} \sum_{i=1}^{n} p_i |a_{ij}|$。

性质：

(1) 设 $A = (a_{ij}) \in C^{n\times n}$，则 A 的全部特征值均落在平面区域 $T = (\bigcup_{i=1}^{n} S_i) \cap (\bigcup_{j=1}^{n} G_j)$。

(2) 设 n 阶矩阵 A 的 n 个圆盘两两互不相交，则 A 相似于对角矩阵。

(3) 设 n 阶实矩阵 A 的 n 个圆盘两两互不相交，则 A 的特征值全为实数。

5. 特征值界的变分估计：

设 $A \in C^{n\times n}$ 为 Hermite 矩阵，

(1) (Rayleigh-Ritz) 则有：(a) $\lambda_n x^H x \le x^H A x \le \lambda_1 x^H x, \forall x \in C^n$；(b) $\lambda_{\max} = \lambda_1 = \max_{x\ne 0} R(x) = \max_{x^H x = 1} x^H A x$；(c) $\lambda_{\min} = \lambda_n = \min_{x\ne 0} R(x) = \min_{x^H x = 1} x^H A x$。(《矩阵理论》P147 证明)

(2) $\lambda_n \le \lambda_{n-1} \le ... \le \lambda_2 \le \lambda_1, \varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_2, \varepsilon_1$ 为对应的标准正交特征向量，令 $U_1 = \mathrm{span}(\varepsilon_1, \varepsilon_n), U_2 = U_1^{\perp} = \mathrm{span}(\varepsilon_{n-1}, ..., \varepsilon_2)$，则 $\lambda_{n-1} = \min_{0\ne x\in U_2} R(x), \lambda_2 = \max_{0\ne x\in U_2} R(x)$。(课件 CH4P4 证明)

(3) $\lambda_n \le \lambda_{n-1} \le ... \le \lambda_2 \le \lambda_1, \varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_2, \varepsilon_1$ 为对应的标准正交特征向量，令 $U = \mathrm{span}(\varepsilon_t, ..., \varepsilon_s), a \le s \le t \le n$，则 $\lambda_t = \min_{0\ne x\in U} R(x), \lambda_s = \max_{0\ne x\in U} R(x)$。(课件 CH4P4 证明)

(4) (Courant-Fischer) $\lambda_n \le \lambda_{n-1} \le ... \le \lambda_2 \le \lambda_1$,$k$ 为给定的正整数，$a \le k \le n$，则

(a) $\lambda_i = \max_{W, \dim W = i} \min_{x\in W, x\ne 0} R(x) = \max_{W, \dim W = i} \min_{u\in W, \|u\|_2 = 1} u^H A u$；

(b) $_i = \min_{W, \dim W = n-i+1} \max_{x\in W, x\ne 0} R(x) = \min_{W, \dim W = n-i+1} \max_{u\in W, \|u\|_2 = 1} u^H A u$。

(5) 设 W 与 V 为 C^n 内的子空间，若 $\dim W > \dim V$，则存在 $0 \ne x \in W$，使得 $x \perp V$。(课件 CH4P4 证明)

(6) (Weyl) 设 $A, B \in C^{n\times n}$ 为 Hermite 矩阵，则 $\forall k = 1, 2, ..., n$，有 $\lambda_k(A) + \lambda_n(B) \le \lambda_k(A + B) \le \lambda_k(a) + \lambda_1(B)$。(《矩阵理论》P149 证明)

6. 设 $A \in C^{n\times n}, \forall \varepsilon > 0$，则存在与 A, ε 有关的常数 $c = c(A, \varepsilon)$，使得 $|(A^k)_{ij}| \leq c[r(A) + \varepsilon]^k, k = 1, 2, ...; i, j = 1, ..., n$。（《矩阵理论》P160 证明）

4 定理

4.1 数

1. 算术基本定理：

每一个不等于 1 的正整数 a 可以分解为素数的幂之积：$a = p_1^{\varepsilon_1} p_2^{\varepsilon_2} ... p_s^{\varepsilon_s}$，其中 $p_1, p_2, ..., p_s$ 为互不相同的素数，$\varepsilon_i \in Z^+$（1 不是素数哦）。除因子的次序外分解式是惟一的。此分解式称为**整数的标准分解式**。

2. 最大公因子定理：

$a, b \in Z$，a, b 不全为 0，$d = (a, b)$，则存在（没说惟一）$p, q \in Z$ 使 $pa + qb = d$。【《应用近世代数》P26 证明】

求解方法：

(1) 辗转相除法【《应用近世代数》P26。先从上往下，新一轮的开始由两次余数引导；再从下往上】【4-1 的 1 题】；

(2) 大衍求一术（递推算法，适合于编程）【《应用近世代数》P27，但书上过分复杂化了，直接用老师讲的矩阵初等行变换的方法做】【4-1 的 2 题】。

3. 包含与排斥原理：

(1) $|\bigcap_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cup A_j| + \sum_{1\leq i<j<k\leq n} |A_i \cup A_j \cup A_k| - ... + (-1)^{n-1} |\bigcup_{i=1}^{n} A_i|$；

(2) $|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{1\leq i<j<k\leq n} |A_i \cap A_j \cap A_k| - ... + (-1)^{n-1} |\bigcap_{i=1}^{n} A_i|$。

【《应用近世代数》P11 证明】

4. 同余方程 $ax \equiv b \pmod m, a \not\equiv 0 \pmod m$ 有解的充分必要条件是 $(a, m)|b$。令 $a = a_1(a, m), b = b_1(a, m), m = m_1(a, m)$，则 $x \equiv rb_1 \pmod{m_1}$ 或 $x = rb_1 + lm_1 (l \in Z)$ 称为方程的一**般解或通解**；【《应用近世代数》P30 证明】

求解方法：

(1) 求 (a, m)，若 $(a, m)|b$，则方程有解；（一定要先判断同余方程是否有解）

(2) 求 a_1, b_1, m_1；

(3) 求 $p, q \in Z$，满足 $pa_1 + qm_1 = 1$；

(4) $x = pb_1 + lm_1 (l \in Z)$ 或 $x \equiv pb_1 \pmod{m_1}$，就是方程的通解。

5. 孙子定理（或中国剩余定理）：

设 $m_1, m_2, ..., m_k (k \geq 1)$ 为 k 个两两互素的正整数，令 $M = m_1 m_2 ... m_k = m_1 M_1 = m_2 M_2 = ... = m_k M_k$，则同余方程组 $\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ ... \\ x \equiv b_k \pmod{m_k}. \end{cases}$ 的一般解为 $x \equiv b_1 c_1 M_1 + b_2 c_2 M_2 + ... + b_k c_k M_k \pmod M$，其中 c_i 是满足同余方程 $M_i x \equiv 1 \pmod{m_i}$ 的一个特解，$i = 1, 2, ..., k$。【4-1 的 3 题】

理解：

拉格朗日插值法其实就是该定理的另一个版本。

6. Euler 定理：

设 n 为大于 1 的整数，$a \in Z$ 且 $(a, n) = 1$，则 $a^{\varphi(n)} \equiv 1 \pmod n$。【《应用近世代数》P66 证明，用拉格朗日定理证明，现代密码学的重要基础】

推论：

(1) 设 p 是素数，$(a, p) = 1$，则 $a^{p-1} \equiv 1 \pmod p$；

(2) 设 p 是素数，$\forall a \in Z$，则 $a^p \equiv a \pmod p$。

7. Welson 定理：

设 p 为素数，则 $(p-1)! \equiv -1 \pmod{p}$。【《应用近世代数》P66 证明，拉格朗日定理证明，现代密码学的重要基础】

4.2 群

1. 设 S 是群 G 的一个非空子集，则以下三个命题互相等价：

(1) S 是 G 的子群；

(2) 对任何 $a,b \in S$ 有 $ab \in S$ 和 $a^{-1} \in S$；

(3) 对任何 $a,b \in S$ 有 $ab^{-1} \in S$。

（《应用近世代数》P46-47 证明）

理解：

条件 (2) 和 (3) 都是常用的检验一个子集是否是子群的准则。对于有限子集 H 来说，H 是子群的条件还可以简化为：对任何 $a,b \in H$ 有 $ab \in H$。即只要封闭性成立就是子群。

2. (1) 设 G 是群，$a \in G$，则 $a^m = 1 \Leftrightarrow \circ(a)|m$（《应用近世代数》P48 证明。证明 $\Rightarrow$ 时用带余除法来衔接）。

(2) 设 G 是群，$a,b \in G, \circ(a) = m, \circ(b) = n$，若 $(m,n) = 1$ 和 $ab = ba$，则 $\circ(ab) = mn$【1-11 的 36 题证明】。

(3) 设 G 是群，$a \in G, \circ(a) = n$，m 为任意正整数，则 $\circ(a^m) = n/(m,n)$。【1-11 的 35 题证明】

3. 从同构的角度看循环群：

(1) 设 $G = \langle a \rangle$ 是由 a 生成的循环群，则 (a) 当 $\circ(a) = \infty$ 时，$G \cong (Z,+)$，称 G 为无限循环群；(b) 当 $\circ(a) = n$ 时，$G \cong (Z_n,+)$，这时称 G 为 n 阶循环群，记作 C_n。【把它们分别表示出来，然后建立双射。还是很显然的】

(2) 讨论上述循环群所同构的群的生成元有 (a) $(Z,+)$ 的生成元只能是 1 或 -1；(b) $(Z_n,+)$ 的生成元只能是 $\overline{a}$，其中 $(a,n) = 1$。【因 $\overline{1} \in Z_n$，故必有 k，使得 $k\overline{a} = \overline{1} \Leftrightarrow \exists p, ka + pn = 1$(逆向变换，对后式两边 $\bmod n$ 就可以得到前式) $\Leftrightarrow (a,n) = 1$（最大公因子定理)】因而生成元的个数为 $\varphi(n)$；

(3) 循环群的子群仍是循环群，且 (a) $(Z,+)$ 的全部子群为 $H_m = \langle m \rangle, m = 0,1,2,...$；(b) $(Z_n,+)$ 的全部子群为 $\langle \overline{0} \rangle$ 和 $\langle \overline{d} \rangle, d|n$。

（《应用近世代数》P53-54 证明）

理解：

所有循环群都同构于 $(Z,+)$ 或 $(Z_n,+)$，所以今后凡遇到循环群都可以用 Z 或 Z_n 来代替。

从上述三条环环相扣的定理可以看出。**生成元**和**子群**还是蛮重要的俩概念，毕竟它们能够帮忙研究清楚结构。然后同构后也可以通过这俩概念把两个群的结构性质给摸清。

4. 群重排定理：

设 $(G,\bullet)$ 为有限群，$\forall g_0 \in G$，有 $g_0G = G$，其中 $g_0G = \{g_0g | \forall g \in G\}$。（《应用近世代数》P55）

理解：

还可以写作形式：$G = G^{-1} = g_0G = Gg_0 = g_0^{-1}Gg_0$。

5. 设 σ 是任一个 n 次置换，则：

(1) σ 可分解为不相交的轮换之积：$\sigma = r_1r_2...r_k$。若不计因子次序，则分解式是唯一的。此处的不相交指的是任何两个轮换中无相同元素；

(2) $\circ(\sigma) = [l_1,l_2,...,l_k](l_1,...,l_k$的最小公倍数)，其中 l_i 是 r_i 的长度；【《应用近世代数》P57 证明，用到定理 2(1) 和 $\circ(r) = l$】

(3) σ 可分解为对换之积：$\sigma = \pi_1\pi_2...\pi_s$。其中 $\pi_i(i = 1,2,...,s)$ 是对换，且对换的个数 s 的奇偶性由 σ 唯一确定，与分解方法无关（注意：这些对换一般来说不再是不相交了，并且分解形式不唯一）。

【4-2 的 5 题，证明 S_n 的生成元】

理解：

在证明 (1) 的 “存在性” 的过程中，我们可以得到对一个置换进行轮换分解的步骤：(1) 从 $\{1,2,...,n\}$ 中任选一个数作为 i_1，依次求出 $\sigma(i_1) = i_2, \sigma(i_2) = i_3, ...$ 直到这个序列中第一次重复出现在 $\sigma(i_{l_1}) = i_k(1 < k < l_1)$，即存在 i_{l_1} 使得 $\sigma_{i_{l_1}} = i_1$（否则与 σ 是双射矛盾）；(2) 重复上述过程。

6. Cayley 定理：

任何一个群同构于一个变换群，任何一个有限群同构于一个置换群。【4-2 的 4 题证明】

理解：

用证明 Catley 定理的构造方法，可以对任何一个群，找出与它同构的变换群或置换群。

7. 设 G 是群，$H \leq G, S_L = \{aH | a \in G\}, S_R = \{Ha | a \in G\}$，则存在 S_L 到 S_R 的双射（这个定理要说的其实就是：当左陪集的集合与右陪集的集合是有限集合时，左陪集的个数与右陪集的个数是相等的）。【《应用近世代数》P64 证明】

理解：

子群的左、右陪集在一般情况下并不一定相等，但在左陪集的集合与右陪集的集合（注意是陪集的集合哦！因为陪集由元素确定，所有元素确定出来的就是个陪集的集合！）之间可以建立一一对应关系。即通过上述定理。

8. 拉格朗日定理：

设 G 是有限群，$H \leq G$，则 $|G| = |H|[G : H]$。【证明：设 $[G : H] = m$，于是存在 $a_1, ..., a_m \in G$，使 $G = \bigcup_{i=1}^{m} a_i H$ 且 $a_i H \cap a_j H = \emptyset, i \neq j$，且每一个陪集中元素的个数均为 $|a_i H| = |H|$，所以有 $|G| = m|H| = |H|[G : H]$】

推论：

（1）设 G 是有限群，$H \leq G$，则 $|H| | |G|$；

（2）当 $|G| < \infty$ 时，对任何 $a \in G$ 有 $\circ(a) | |G|$，因而有 $a^{|G|} = e$；

（3）若 $|G| = p$（素数），则 $G = C_p$(p 阶循环群)，即素数阶群必为循环群；

（4）若 $g_1 g_2 = g_2 g_1$，且 $\langle g_1 \rangle \cap \langle g_2 \rangle = \{e\}$，则有 $\circ(g_1 g_2) = [\circ(g_1), \circ(g_2)]$。

应用：

该定理及推论可以被用来确定一个群内可能存在的子群、元素的阶等，从而搞清一个群的结构。具体而言，以前我们在确定一个群内的子群时，主要利用元素的生成子群。有了 Lagrange 定理，则首先可由 $|G|$ 的因子来确定可能存在的子群的阶数或元素的阶数，然后根据子群的阶数来寻找子群。【4-3 的 7 题，“元素的阶是群的阶的因子”】

理解：

当 G 是有限群时，子群的阶数与指数也都是有限的，拉格朗日定理则是建立了它们之间的关系。

9. 设 G 是群，A, B 是 G 的两个有限子群，则有 $|AB| = \dfrac{|A||B|}{|A \cap B|}$。【4-2 的 6 题证明，要善用 “左陪集能够划分群” 这一性质】【4-3 的 8 题，运用该结论】

10. 设 $H \trianglelefteq G$，则 G/H 对子集乘法构成群。【《应用近世代数》P70 证明】

11. 设 G 是有限可换群，p 为素数，且 $p | |G|$，则 G 中有 p 阶元。【《应用近世代数》P71 证明】

12. 设 G 是群，$a \in G, K_a = \{gag^{-1} | g \in G\}$，且 $|K_a| < \infty$，则有 $|K_a| = [G : C_G(a)]$。【《应用近世代数》P74 证明】

13. 设 G 是有限群，$G \leq G$，$N(H)$ 为 H 在 G 中的正规化子，则与 H 共轭的子群的个数为 $|K_H| = [G : N(H)]$。【《应用近世代数》P75 证明】

14. 在对称群 S_n 中，σ_1 与 σ_2 共轭的充分必要条件是 σ_1 与 σ_2 类型相同（其中 σ 表示置换）。【《应用近世代数》P76】

15. 同态基本定理：

设 f 是 G 到 G' 的满同态（注意条件），$K = \ker f$，则

（1）$G/K \cong G'$；

（2）设 φ 是 G 到 G/K 的自然同态，则存在 G/K 到 G' 的同构 σ 使 $f = \sigma\varphi$（注意顺序）。

【《应用近世代数》P81 证明】【1-14 的 47 题】

16. 子群对应定理

设 f 是 G 到 G' 的满同态，$K = \ker f$，$S = \{H | H \leq G \ \ H \geq K\}$，$S' = \{N | N \leq G'\}$，则存在一个 S 到 S' 的双射。【《应用近世代数》P83 证明】【1-15 的 49 题】

17. 第一同构定理或商群同构定理：

设 f 是群 G 到群 G' 的满同态，$K=\ker f, H\trianglelefteq G$ 且 $H\geq K$，则 $G/H\cong G'/f(H)(\cong \dfrac{G/K}{H/K})$。【《应用近世代数》P83 证明】

18. 第二同构定理：

设 G 是群，$N\trianglelefteq G, H\leq G$，则 $HN/N\cong H/(H\cap N)$。【《应用近世代数》P84 证明】

19.Burnside 引理：

设有限群 G 作用于有限集 X 上，则 X 在 G 作用下的轨道数目为 $N=\dfrac{1}{|G|}\sum\limits_{g\in G}\chi(g)$，其中 $\chi(g)$ 为元素 g 在 X 上的不动点数目，和式是对每一个群元素求和。【《应用近世代数》P91-92 证明】

20. 设 G 是群，A,B 是 G 的两个子群，并满足（a）$A,B\trianglelefteq G$;（b）$G=AB$;（c）$A\cap B=\{e\}$，则 $G\cong A\times B$。【《应用近世代数》P105 证明】

4.3 环

1. 环中无左（右）零因子的充分必要条件是乘法消去律成立：$a\neq 0, ab=ac\Rightarrow b=c$，$a\neq 0, ba=ca\Rightarrow b=c$。【《应用近世代数》P120 证明】

2. $(Z_n,+,\cdot)$ 是域的充要条件是 n 为素数。【《应用近世代数》P120 证明】

3. 一个非零的有限的无左（右）零因子环是除环。【《应用近世代数》P121 证明】

推论：

有限整环是域。

4. 若 A 为交换环，则 A/I 也是交换环。若 A 为幺环，则 A/I 也是幺环且 $1+I$ 为幺元。

5. 设 A 是有单位元的可换环，M 是 A 的一个极大理想，则 A/M 是域。【《应用近世代数》P128 证明】

6. 有限整环是域。

7. 同态基本定理：

设 f 是环 A 到环 A' 的一个满同态，$K=\ker f$，则（1）$A/K\cong A'$;（2）$\sigma: a+K\mapsto f(a)$（由商环的定义）是 A/K 到 A' 的同构，设 φ 是 A 到 A/K 的自然同态：$\varphi(a)=a+K, \forall a\in A$，则有 $f=\sigma\varphi$。

如果 f 不是 A 到 A' 的满同态，则映射 $\sigma: a+K\mapsto f(a)$ 将 A/K 同构嵌入 A' 中。

8. 子环对应定理：

设 f 是环 A 到 A' 的满同态，$K=\ker f$，S 是 A 中的所有包含 K 的子环的集合。S' 是 A' 中所有子环的集合，则映射 $\varphi:(K\subseteq)H\to f(H)$，是 S 到 S' 的双射，且对理想也有类似的性质。

9. 商环同构定理：

设 f 是环 A 到环 A' 的满同态，I 是 A 的一个理想且 $I\supseteq \ker f(=K)$，则 $A/I\cong A'/f(I)(\cong (A/K)/(I/K))$。

10. 第二同构定理：

设 A 是环，S 是子环，I 是理想，则 $(S+I)/I\cong S/(S\cap I)$。

11. 设 D 是有单位元的整环，若对 D 中任何两个元素均有最大公因子存在，则 D 中的每个既约元也是素元。【《应用近世代数》P136】

12. 设 D 是有单位元的整环，则以下命题等价：

（1）D 是惟一分解整环；

（2）D 满足下列两个条件：（a）D 中的任何真因子序列 $a_1,a_2,...,a_i,...$（其中 a_{i+1} 是 a_i 的真因子）只能含有有限项（对应于理想生成链，解决了存在性问题）。（b）D 中任何两元素均有最大公因子。

（3）D 满足下列两个条件：（a）同（2）中的条件（a）;（b）D 中每一个既约元都是素元。

【《应用近世代数》P138-139 证明】

13. 域的乘群的任何有限子群是循环群。【《应用近世代数》P139 证明】

14. $0\neq f(x)\in Z[x]$ 可分解成两个低次有理系数多项式的乘积 $\Rightarrow f(x)$ 可分解成两个低次整系数多项式的乘积。

【PPT 环论 37-39 的 3 个例子】

15. 多项式的可约性判断

(1) 设 D 是惟一分解整环，P 是 D 的分式域，$f(x)=\sum_{i=1}^{n}a_ix^i\in D[x]$，若 $\frac{r}{s}\in P,(r,s)\sim 1$，是 $f(x)$ 在 P 上的一个根，则 $r|a_n,s|a_0$。若一个多项式 $f(x)\in D[x]$ 如果在 P 上有根，则 $f(x)$ 在 $P[x]$ 中可约，由定理知在 $D[x]$ 中也可约。【《应用近世代数》P146】

然而，该定理对于 $n\geq 4$ 的多项式而言，可分解为两个次数不小于 2 的多项式，因为没有根不能说明 $f(x)$ 不可约。对于**判断次数不小于 4 的多项式是否可约**，可以用下列的 Eisenstein 定理。

(2) Eisenstein 定理：设 D 是惟一分解整环，$f(x)=\sum_{i=0}^{n}a_ix^i\in D[x]$ 是本原多项式且 $\deg f(x)\geq 1$（表示次数），若有 D 中的不可约元（也是素元）p 满足：

(a) $p|a_i(i=0,1,2,...,n-1)$ 但 $p\nmid a_n$；

(b) $p^2\nmid a_0$。

则 $f(x)$ 在 $D[x]$ 中不可约，也在 $P[x]$ 中不可约，其中 P 是 D 的分式域。

【《应用近世代数》P146-147 证明】【《应用近世代数》P147-148 例子】

有时候不能找到 p，但不能说明多项式可约，因此还可以对其进行变换，用下述定理，看变换后能不能找到。

(3) 设 D 是惟一分解整环，$f(x)\in D[x]$，则 $f(x)$ 在 $D[x]$ 中（不）可约 $\Leftrightarrow$ $f(x+1)$ 在 $D[x]$ 中（不）可约（变换时也不要太死板，比如 $f(x)=x^5-5x+1$，也可以通过令 $x=x-1$ 变换得 $f(x-1)=x^5-5x^4+10x^3-10x^2+5$。也可以多次更深入地变换吧）。

【1-19 的 62 题】

推论：

(1) 设 $F[x]$ 为域 F 上的一元多项式环，$f_1(x),f_2(x),g(x)\in F[x]$ 且 $g(x)\neq 0$，则 $f_1(x)\equiv f_2(x)\pmod{g(x)}\Leftrightarrow g(x)|(f_1(x)-f_2(x))$，而且 $f_1(x)\equiv f_2(x)\pmod{g(x)}$ 无论对 $F[x]$ 的加法或乘法都是同余关系；

(2) 设 $F[x]$ 为域 F 上的一元多项式环且 $f(x)\in F[x](c\in F)$，则 $f(x)\equiv f(c)(\pmod{x-c})$ 且 $(x-c)|f(x)$ iff $f(c)=0$。

理解：

对于 Eisenstein 定理，貌似只有在有理数域上才可以使用，并且一定要注意前提条件是本原多项式哦，还有 $\deg f(x)\geq 1$。而且对于次数小于 4 的，推荐优先使用试根法，反证也挺好算的，而且也不用为 Eisenstein 定理一直找不到 p 做变换而苦恼。

4.4 域

1. 设 F 是一个域，$f(x)\in F[x],\deg f(x)\geq 1$，则 $f(x)$ 在 F 上的分裂域存在，而且在 F-同构意义下是惟一的。

推论：

(1) 对任意一个域 F 和正整数 n，可构造一个扩域 E，使 $(E:F)=n$。只需在 $F[x]$ 中选定一个 n 次不可约多项式 $f(x)$，则 $E=F[x]/(f(x))=\{\overline{r(x)}|r(x)=0\}$或 $\deg r(x)<n\}$ 满足 $(E:F)=n$ 且 E 包含 $f(x)$ 的一个根：$\overline{x}=x+f(x)$；【1-19 的 64 题，不可知根在其分裂域上的表示形式的情形】

(2) 对 F 上任意一个 n 次多项式 $f(x)$，若它在其分裂域中的根为 $u_1,u_2,...,u_n$，则可通过逐次添加根的方法得到分裂域 $E_f=F(u_1,u_2,...,u_n)$，从而可得 $(E:F(u_1,u_2,...,u_n))\leq n!$。【1-19 的 63 题，可知根在其分裂域上的表示形式的情形】

2. 代数基本定理：

任意一个复系数 $n(n>0)$ 次多项式至少有一个复数根。【《应用近世代数》P168-169 证明，用分裂域的理论，即上述定理，来证明】

3. 任何两个元素个数相同的有限域都是同构的，且都同构于多项式 $f(x)=x^{p^n}-x$ 在 Z_p 上的分裂域。【《应用近世代数》P171 证明】

注意，要对 $GF(p^n)$ 的元素进行运算时，必须给出 $Z_p[x]/(q(x))$ 中的具体的生成多项式 $q(x)$。【《应用近世代数》P172 理解】

4. 设 $p(x) \in Z_p[x]$ 是 Z_p 上的一个 n 次不可约多项式，u 是 $p(x)$ 在其分裂域 E_p 上的一个根，则 $p(x)$ 在 E_p 上的全部根为 $u, u^p, ..., u^{p^{n-1}}$。【《应用近世代数》P174-175 证明和例子】

5. 有限域上元素和多项式的性质

（1）$GF(p^n)$ 中每一个元素都是 p 次幂，也都是 p 次方根；

（2）$GF(p^n)$ 中本原元的数目为 $\varphi(p^n-1)$，这里 φ 是 Euler 函数；

（3）Z_p 上 n 次本原多项式的个数为 $J_p(n) = \varphi(p^n-1)/n$；

（4）$GF(p^n)$ 由所有 $m|(m|n)$ 次不可约多项式的根组成。

【《应用近世代数》P176-177 证明】

6. 设 F 是有限域，且 $|F| = q$, 则有：

（1）$|GL_n(F)| = (q^n-1)(q^n-q^)...(q^n-q^{n-1})$；

（2）$|SL_n(F)| = \dfrac{(q^n-1)(q^n-q^)...(q^n-q^{n-1})}{q-1}$。

【《应用近世代数》P177 证明】

5 应用

5.1 数学归纳法原理、超限归纳法原理

正整数集 Z^+ 是良序集。由正整数集的良序性可以得到**数学归纳法原理**：

设 M 是由正整数构成的集合，若 $1 \in M$，且当 $n-1 \in M$ 时必有 $n \in M$，则 M 是正整数集。如果一个命题与正整数有关，首先证明命题对 1 成立，然后假设命题对 $n-1$ 成立，若能证明命题对 n 也是真的，则命题对所有正整数都是真的【《应用近世代数》P23 证明】。

数学归纳法可以推广到任何良序集，这就是所谓的**超限归纳法原理**：

设 $(S, \leq)$ 是一个良序集，$P(x)$ 是与元素 $x \in S$ 有关的一个命题，如果（1）对于 S 中的最小元 a_0，$P(a_0)$ 成立；（2）假定对任何 $x < a$，$P(x)$ 成立，可证明 $P(a)$ 也成立。则 $P(x)$ 对任何 $x \in S$ 都成立。

5.2 对称群（置换）与“项链问题”、“正多面体着色问题”和“图的计数问题”

参见【《应用近世代数》P93-101】。

5.3 环与编码问题、多项式编码及其实现

参见【《应用近世代数》P148-153】。