代数 笔记

任云玮

目录

这是我学习 Michael Artin 的 *Algebra* 时候的笔记，包括对于内容的一些自己的理解以及注记. 其中的内容并**不完整**，略去了部分基础的内容，并且对应的中文翻译也是我按照自己的习惯翻译的，所以请谨慎参考.

1 矩阵

1.1 基础操作

1 定义 (逆) 设 $A \in \mathbf{F}^{n\times n}$，若存在方阵 B，使得

$$AB = I \quad 且 \quad BA = I,$$

则称 A 可逆并称 B 是 A 的逆矩阵，记作 A^{-1}.

评注 逆矩阵相关基础性质略.

2 引理 (不可逆) 存在全为零的行或列的矩阵不可逆.

3 定义 (矩阵元[1]) 定义如下特殊的矩阵 $e_{ij} \in \mathbf{F}^{n\times m}$，它仅在第 i 行第 j 列为 1，在其他位置全为 0.

评注 左乘 e_{ij} 相当于把原矩阵的第 j 行移到第 i 行并将其他行清零. 可以按照如下方式来考虑左乘一个矩阵 P 产生的影响：首先明确左乘是行变换；之后考虑 P 的每一个行 $P_i = (p_{i1}, \ldots, p_{in})$，它表明了矩阵 PA 的第 i 行的构成：是由 A 的第 1 行的 p_{i1} 倍加到第 n 行的第 p_{in} 倍.

4 命题 (矩阵元的性质)

1. 矩阵 $A = (a_{ij})$ 可以写成 $A = \sum_{ij} a_{ij}e_{ij}$ 的形式.
2. $e_{ij}e_{jl} = e_{il}$，　且　$e_{ij}e_{kl} = 0$ 若 $j \neq k$.
3. 对于 $\mathbb{R}^n$ 的标准基 $\{e_i\}$，成立 $e_{ij}e_j = e_i$，　且　$e_{ij}e_k = 0$ 若 $j \neq k$.

评注 在某些时候，可以将矩阵和向量的乘法写为 $(\sum_{ij} a_{ij}e_{ij})(\sum_i b_i e_i)$ 的形式，之后再利用此命题进行化简.

5 定理 (幂零元[2]) 称方阵 A 是幂零的，若存在正整数 k，使得 $A^k = 0$ 成立. 若方阵 A 幂零，则 $I + A$ 可逆.

[1] Matrix Units

[2] nilpotent. 习题 1.13

证明 可以通过构造出逆的方法证 $I+A$ 可逆，即找 B，使得 $(I+A)B=I$ 成立. 从 trivial 的情况开始考虑，若 $k=1$，则 $B=I$；若 $k=2$，则应该尝试构造出 A^2，同时让交错项互相消去，可以发现 $B=I-A$；基于上述想法，我们可以猜测，B 应该满足 $1\pm A\pm A^2\pm\cdots\pm A^{k-1}$ 的形式. 因为这样恰可以通过乘 I 和乘 A，实现错位相消并让最后一项为零. 经验证，如下式的 B 确实满足条件

$$B=\sum_{n=0}^{k-1}(-1)^nA^n. \quad \blacksquare$$

1.2 行消元

6 定义 (初等矩阵[3]) 初等矩阵是指如下三类同单位矩阵十分相近的矩阵：其中 $a\neq 0$，$i\neq j$，

1. $I+ae_{ij}$.
2. 交换 I 的第 i，j 行.
3. 将 I 的 (i,i) 位置换为 a.

将它们左乘到矩阵 A 上，则它们分别对应了一种初等行变换：

1. 将第 j 行乘以 a 加到第 i 行上.
2. 交换 A 的第 i，j 行.
3. 将 A 的第 i 行乘 a.

评注 初等矩阵相关性质略. 对于这些操作的对应关系，可以按照定义 3的评注中的内容来理解. 也可以按照如下方式来记忆：如何从 I 通过行变换得到对应的初等阵，那这个初等阵就对于它所左乘的矩阵进行了何种操作.

7 定义 (行规范形矩阵[4]) 称 $A\in\mathbf{F}^{n\times m}$ 为行规范形矩阵，如果它满足

1. 如果第 i 行全为 0，则对于任意 $j>i$，第 j 行也全为 0.
2. 如果第 i 行不全为 0，则它的第一个非零元素为 1. 称该位置为主元.
3. 主元一定在上一个主元右侧.
4. 主元上方的位置都为 0.

[3]Elementary Matrix

[4]Reduced Row Echelon Form; Row Canonical Form

评注 这一定义可以看作是单位阵的弱化. 单位阵对角线上为 1，因此要求主元处为 1. 同时由于在消元的过程中可能会出现将某一行消为 0 的情况，因此仅要求矩阵为阶梯形. 而要求主元上方为 0 对应了单位阵只有对角线上有元素.

可以证明，所有的矩阵都可以通过初等行变换化为行规范形矩阵.

8 定理 (Gauss 消元) 设 P 为 k 个初等矩阵的乘积，$A \in \mathbb{F}^{m\times n}$，$B \in \mathbb{F}^m$，则线性方程组 $AX = B$ 与 $(PA)X = PB$ 同解.

评注 证明略. 这一定理给出了消元法解线性方程组的方法，只需要对方程组的两边施相同的行变换，化为行规范形矩阵的形式，即可以直接求解.

9 引理 (齐次线性方程组解的存在性) 设 $m < n$，$A \in \mathbb{F}^{m\times n}$，则齐次线性方程组 $AX = 0$ 必有非零解.

评注 TODO: 用法

10 引理 (行规范形) 一个行规范行矩阵或是单位阵，或它的最后一行为零.

评注 这是一条十分有用的引理. 由于所有的矩阵都可以通过初等行变换化为行规范形，所以只需要设 $A' = PA$ 为 A 的行规范形即可以得到一个行规范行矩阵，再分析 A' 的最后一行，就可以知道 A' 的情况了. 另注意最后一行为零意味着 A 是不可逆的. 相关习题：习题 2.8

11 定理 (可逆的等价条件) 对于方阵 A，下述命题等价：

1. A 可以通过初等行变换化为单位阵.
2. A 是一系列初等矩阵的乘积.
3. A 可逆.

12 命题 对于方阵 A，若 B 是它的左逆元或右逆元，则 A 可逆且 B 是它的逆.

13 定理 (线性方程组) 对于方阵 A，以下命题等价：

1. A 可逆.
2. 对于任意列向量 B，线性方程组 $AX = B$ 有唯一解.
3. 齐次线性方程组 $AX = 0$ 有且仅有零解.

评注 轮转证明即可. 其中 [3.] 与 [2.] 等价意味着一般可以通过研究对应的齐次线性方程组的方式来研究线性方程组.

14 命题 [5] 对于方阵 A，若线性方程组 $AX = B$ 对于某个特定的 B 有唯一解，则对于任意的其他 B，它也有唯一解.

1.3 矩阵的转置

15 命题 [6] 若 A，B 分别是 $n \times n$ 的对称阵，则 AB 是对称阵的充要条件为 $AB = BA$.

1.4 行列式

二阶行列式的几何含义 首先,"乘上一个二阶矩阵"实际上是从 $\mathbb{R}^2$ 到 $\mathbb{R}^2$ 的映射。考虑单位向量 $(1,0)$ 和 $(0,1)$，它们构成的平行四边形面积为 1，经过矩阵 A 映射后，它们变为 (a_1,b_1)，(a_2,b_2)，由两个新的向量构成的平行四边形的有向面积就是 $\det A$ 的值。即行列式的值代表了面积的变化比例。

16 定理 (行列式的唯一性[7]) 设 δ 是定义在 $n \times n$ 方阵全体上的函数，若它满足

1. $\delta(I) = 1$;
2. δ 关于方阵 A 的行是线性的;
3. 若方阵 A 又相邻两行相等，则 $\delta(A) = 0$;

则称 δ 是一个行列式. 这样的函数是唯一的.

评注 利用唯一性来证明不同的公式、元素等相同.

17 定理 对于方阵 A 和 B，成立 $\det(AB) = \det A \det B$.

证明 可以利用推论 19和行规范形来证明.

18 定理 (行列式的性质) 设 δ 是定义在 $n \times n$ 矩阵全体上的行列式函数，则成立

1. 若 A' 由将 A 的第 j 行乘上常数 c 加到第 i 行上得到，且 $i \neq j$，则 $\delta(A') = \delta(A)$.
2. 若 A' 由交换 A 的两行得到，则 $\delta(A') = -\delta(A)$.
3. 若 A' 由将 A 的第 i 行乘上 c 得到，则 $\delta(A') = c\delta(A)$.
4. 若 A 的第 i 行是第 j 行的 c 倍且 $i \neq j$，则 $\delta(A) = 0$.

[5] 习题 2.10

[6] 习题 3.2

[7] 证明需要用到之后的命题.

证明 首先证明 [3.]，接下来证明 [1. 2. 3.] 对于相邻的 i，j 行成立，最后再通过反复交换相邻两行的方法，证明 [1. 2. 3.] 对于任意的 $i \neq j$ 成立. ■

19 推论 (行列式与初等矩阵) 设 δ 是定义在全体 $n \times n$ 矩阵上的行列式函数，E 是初等矩阵. 则对任意方阵 A，成立 $\delta(EA) = \delta(E)\delta(A)$，同时有

1. 若 E 为第一类，则 $\delta(E) = 1$.
2. 若 E 为第二类，则 $\delta(E) = -1$.
3. 若 E 为第三类，则 $\delta(E) = c$.

评注 关于用法，可以设 A' 是 A 的规范形，则 $A = (\prod E_k)A'$，有 $\delta(A) = (\prod \delta(E_k))\delta(A')$.

虽然通过先定义初等矩阵的行列式来定义行列式看上去是符合直觉的，但是由于将一个矩阵拆分成初等矩阵和规范形时，初等矩阵的顺序和类型都是不定的，要说明不同的拆法的结果一样实际上并不方便.

20 定义 (行列式) 一种行列式的计算方法为按照第一列展开，具体公式略. 可以通过对矩阵的大小施归纳法证明这是一个行列式函数.

21 推论

1. 方阵 A 可逆当且仅当 $\det A \neq 0$. 且若 A 可逆，则成立 $\det(A^{-1}) = (\det A)^{-1}$.
2. $\det A = \det A^{\intercal}$.

22 引理 (分块矩阵行列式) 设 A 和 D 都是方阵，则

$$\det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = (\det A)(\det D).$$

1.5 置换

23 定义 (置换[8]) 集合 S 的一个置换是指一个从 S 到 S 的双射.

评注 一般而言，仅考虑 S 为有限集的情况，所以常常可以认为 $S = 1, 2, \ldots, n$ 或是 $S = x_1, x_2, \ldots, x_n$.

24 定义 (置换矩阵) 对于每一个置换 p，称矩阵 P 为其对应的置换矩阵，如果将 P 左乘到一个向量上的效果，等效于用 p 对对应分量置换.

[8] Permutation.

评注 有如下显式公式

$$P = \sum_i e_{pi,i},$$
$$PX = \sum_i e_{pi} x_i = \sum_k e_k x_{p^{-1}k}.$$

即，新的第 k 位元素为原来的第 $p^{-1}(k)$ 位的元素. 只需要利用命题 4即可以验证上述公式.

25 命题 (置换矩阵)

1. 置换矩阵 P 在每一行（列）上都有且仅有一个 1，其他位置都为零. 同时，这样的矩阵也都是置换矩阵.

2. 置换矩阵的行列式为 ± 1.

3. 若置换 p，q 对应的置换矩阵为 P 和 Q，则置换 pq 对应的置换矩阵为 PQ.

评注 关于 [2.]，定义置换的符号 $\operatorname{sign} p = \det P$，若 $\operatorname{sign} p = 1$，则称为偶置换，否则称为奇置换. 每一个置换都可以被分解成数个换位的乘积，有结论这一置换的奇偶性和分解成的换位个数的奇偶性是一致的，哪怕这一分解是不唯一的.

2 群

2.1 复合律

26 定义 (复合律[9]) 设 S 是一个集合，复合律是将 $S \times S$ 映射到 S 中的函数.

27 命题 (唯一性) 在 S 上定义了一个满足交换律的复合律. 则对于 S 中的 n 个元素 $a_1, \ldots, a_n$，可以唯一定义满足如下性质的这 n 个元素的乘积（暂时记为 $[a_1 a_2 \cdots a_n]$）

1. $[a_1] = a_1$.
2. $[a_1 a_2]$ 的结果为对它们施复合律的结果.
3. 对任意整数 $1 \leq i \leq n$，成立 $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$.

28 定义 (单位元) 复合律的单位元是指 S 中的一个元素 e，对任意 $a \in S$，成立

$$ea = a \quad \text{且} \quad ea = a.$$

29 定义 (逆) 设在 S 上定义了复合律，且该复合律满足交换律且有单位元 1，称 $a \in S$ 可逆，若存在 $b \in S$，成立

$$ab = 1 \quad \text{且} \quad ba = 1,$$

称 b 为 a 的逆元.

评注 逆元是取定复合律，取定 S 中一元素后，所对应的 S 中（另）一元素. 在此略去了逆元的一些性质. 需要注意，单侧逆元的存在不能保证该元素可逆. 同时注意，逆表现出了类似于交换律的现象.

2.2 群

30 定义 (群) 称定义了复合律的集合 G 为群，若它满足如下性质：

1. 该复合律满足结合律.
2. G 包含单位元.
3. G 中的每个元素都可逆.

[9]Law of Composition. 和“满足交换律”中的“律”不同，这里的复合律指代一个函数.

评注 常常的，G 是一个映射的集合而复合律为映射的复合. 另外在有些情况下，需要先证明 G 在给定的运算下是封闭的，即该运算确实是一个复合律.

31 定义 (阶) 对于一个有限群，定义它所包含的元素个数为阶.

32 命题 (消去律) 群有消去律. 即对于群 G 以及 $a, b, c \in G$，若 $ab = ac$，则 $b = c$.

33 定义 (对称群) 定义 n 阶对称群 S_n 为 $\{1, 2, \ldots, n\}$ 上的置换全体，以及置换的复合所组成的群.

34 命题 (2 阶对称群) TODO

35 定义 (子群) 称群 G 的子集 H 为一个子群，若它满足

1. 闭合：若 $a, b \in H$，则 $ab \in H$.
2. 单位元：$1 \in H$.
3. 逆：若 $a \in H$，则 $a^{-1} \in H$.

评注 实际上可以证明，如果 H 有单位元，则它一定是 G 的单位元. 对于逆也是一样的.

2.3 整数加法群的子群

36 定理 定义 $\mathbb{Z}a = \{n \in \mathbb{Z} \,|\, n = ka, k \in \mathbb{Z}\}$. 设 S 是加法群 $\mathbb{Z}^+$ 的一个子群，则 S 或是 $\{0\}$，或有形式 $\mathbb{Z}a$，其中 a 是 S 中最小的正整数.

证明 首先处理 trivial 的情况；并证明 S 中有正整数；设 a 是 S 中最小正整数，并证明 $\mathbb{Z}a$ 和 S 互相包含，在证明中可以利用带余数除法. ■

37 定义 (最大公约数) 定义 $S = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} \,|\, n = ra + sb, r, s \in \mathbb{Z}\}$. 由于 S 是 $\mathbb{Z}^+$ 的一个子群，所以若 $a, b \neq 0$，则 $S = \mathbb{Z}d$. 称 d 为 a，b 的最大公约数.

评注 要证明 a 和 b 互素，只需要证明 $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}$ 即可.

38 定理 (最大公约数) 设 $a, b \neq 0$，$d = \gcd(a, b)$，则成立

1. d 整除 a 和 b.
2. 若 e 整除 a 和 b，则 e 整除 d.
3. 存在 $r, s \in \mathbb{Z}$，成立 $d = ra + sb$.

评注 这一定理表明了将 d 称为最大公约数的原因，其中 [3.] 一定程度上来说十分好用.

39 推论 (互素) a，b 互素的充要条件为存在 $r, s \in \mathbb{Z}$，成立 $ra + sb = 1$.

证明 必要性是显然的. 对于充分性，设 $S = \mathbb{Z}a + \mathbb{Z}b$，因为 $1 \in S$，所以 $S = \mathbb{Z}$，从而 $\gcd(a, b) = 1$. ■

40 推论 设 p 是一个素数且 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$.

证明 若 p 不整除 a，由于 p 是素数，则 $\gcd(a, p) = 1$，即存在 $r, s \in \mathbb{Z}$，成立

$$ra + sp = 1 \quad \Rightarrow \quad rab + spb = b.$$

由于 $p \mid rab$，$p \mid spb$，所以 $p \mid b$. ■

41 定义 (最小公倍数) 称 d 为 $0 \neq a, b \in \mathbb{Z}$ 的最小公倍数，若 $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}d$. 相关性质略.

2.4 循环群

42 定义 (循环子群) 称 H 是群 G 的一个循环子群，若存在 $x \in G$，成立

$$H = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}.$$

评注 H 是包含 G 的最小子群. 常常的，H 仅仅是一个有限群.

43 定理 记 $\langle x \rangle$ 是由 x 生成的 G 的循环子群，$S = \{k \in \mathbb{Z} | x^k = 1\}$.

1. S 是 $\mathbb{Z}^+$ 的子群.
2. $x^r = x^s$ 当且仅当 $r - s \in S$.
3. 若 S 非平凡，设 $S = \mathbb{Z}n$. 则 $S = \{1, x, \dots, x^{n-1}\}$.

评注 关于 [3.]，如果 $\langle x \rangle$ 是无限的，则只有 $0 \in S$，即 S 是平凡的. 所以 S 非平凡表明了 $\langle x \rangle$ 是有限群. 而此命题给出了 $\langle x \rangle$ 的具体组成.

证明 [1. 2.] 的证明是显然的，下证明 [3.]. 考虑 S 中的元素 x^p，设 $p = nq + r$，其中 $0 \leq r < n$，则 $x^p = x^{nq}x^r$，而 $nq \in S$，所以 $x^p = x^r \in \{1, x, \dots, x^{n-1}\}$. 而显然 $\{1, \dots, x^{n-1}\} \subset \langle x \rangle$. 所以 $\langle x \rangle = \{1, \dots, x^{n-1}\}$. ■

44 命题 设 x 是群中的一个阶为有限值 n 的元素，设 $k = nq + r$，其中 $0 \leq r < n$，则

1. $x^k = x^r$.
2. $x^k = 1$ 当且仅当 $r = 0$.
3. 设 $d = \gcd(k, n)$，则 x^k 的阶为 n/d.

评注 这一命题描述了 $\langle x\rangle$ 中的元素的性质. 其中 [3.] 给出了 x 以外的元素的计算方法.

证明 下证明 [3.]. 设 x^k 的阶为 m. 由于 $x^{mk}=1$，所以 $n\,|\,mk$，从而 $n/d\,|\,mk/d$，而 $d=\gcd(n,k)$，因此 $n/d\,|\,m$，即 $n/d\le m$. 同时 $x^{k(n/d)}=x^{(k/d)n}=1$，所以 $n/d\ge m$. 综上，$n/d=m$. ■

45 命题 (逆元的阶) 设 x 是群 G 中的元素，则 x 与 x^{-1} 的阶相同.

评注 由于当 x 的阶数大于 2 时，$x\neq x^{-1}$，所以阶大于 2 的元素都是成对出现的.

2.5 同态

46 定义 (同态[10]) 设 G 和 G' 为群，则称 $\varphi:G\to G'$ 为同态，若对于任意 $a,b\in G$，成立 $\varphi(ab)=\varphi(a)\varphi(b)$.

评注 注意，可以在某一边，或者两边使用加法记号. 对于任意两个群，有平凡的同态 $\varphi(x)=1_{G'}$. 若 H 是 G 的子群，则 $\varphi(x)=x$ 也是一个同态.

47 定理 设 $\varphi:G\to G'$ 是一个群的同态.

1. 设 $a_1,\dots,a_k\in G$，则 $\varphi(a_1\cdots a_k)=\varphi(a_1)\cdots\varphi(a_k)$.
2. $\varphi(1_G)=1_{G'}$.
3. $\varphi(a^{-1})=\varphi(a)^{-}1$.

48 定义 (像) 对于同态 $\varphi:G\to G'$，称 $\varphi(G)=\{x\in G'\,|\,\exists a\in G\,\text{s.t.}\,x=\varphi(a)\}$ 为 φ 的像.

评注 $\varphi(G)$ 是 G' 的一个子群，证明略.

49 定义 (核) 对于同态 $\varphi:G\to G'$，称 $\ker\varphi=\{x\in G\,|\,\varphi(x)=1\}$ 为 φ 的核.

评注 $\varphi(G)$ 是 G 的一个子群. 核控制了整个同态的行为，确定了核即可以确定哪对 G 中的元素会被映射到 G' 中的相同元素上.

50 定义 (陪集) 设 H 是群 G 的子群而 $a\in G$，则称 $aH=\{g\in G\,|\,\exists h\in H\,\text{s.t.}\,g=ah\}$ 为左陪集. 同样的，可以定义右陪集.

评注 可以将陪集理解为 H 被 a 作用后的结果.

51 定理 设 $\varphi : G \to G'$ 是一个群同态，$a, b \in G$. 记 φ 的核为 K. 则以下命题等价

1. $\varphi(a) = \varphi(b)$.
2. $a^{-1}b \in K$.
3. $b \in aK$.
4. $aK = bK$.

评注 [2.] 表示在 φ 的含义下，a^{-1} 和 b^{-1} 的效果是差不多的，都可以让 b 被映射到 1 上，即表明 a 和 b 是差不多的. 而 [2. 3.] 可以根据 定义 50的评注加以理解. [1.] 实际上表示 a 和 b 同余，[1. 3. 4.] 描述了同余的元素的陪集之间的关联.

同余类就是陪集!!

证明 下仅给出思路. 先证明 [1. 2.] 等价，再证明 [2.]⇒[3.]，[3.]⇒[1.]，最后证明 [3. 4.] 等价即可. 注意在 [1. 2.] 中 a 和 b 的地位是完全相同的.

52 推论 (单射) 同态 φ 是单射当且仅当 $\ker\varphi = \{1\}$.

评注 在证明一个同态是单射的时候，这一命题是常用的.

53 定义 (正规子群) 称 N 是 G 的正规子群，若对任意 $a \in N$，$g \in G$，共轭 $gag^{-1} \in N$.

评注 若 G 是 Abel 群，则 N 必然是一个正规子群.

54 定理 同态的核是一个正规子群.

55 定义 (中心) 称 Z 为群 G 的中心，若 $Z = \{z \in G \,|\, \forall x \in G,\, zx = xz\}$.

56 命题 [11] $GL_n(\mathbb{R})$ 的中心为 $\{kI \,|\, k \neq 0\}$.

证明 记 $GL_n(\mathbb{R})$ 的中心为 Z，显然 $\{kI\} \subset Z$. 设 K_i 为对角线上第 i 个元素为 2，其他元素为 1 的对角阵，设 $C \in Z$，则

$$CK_i = K_iC \quad \Rightarrow \quad 2c_{i,j} = c_{i,j},\, 2c_{j,i} = c_{j,i}, \quad j \in 1, 2, \ldots, i-1, i+1, \ldots, n.$$

所以 C 为对角阵. 设 $C = \operatorname{diag}\ldots, c_i, \ldots, c_j, \ldots$，设 $K_{ij} = I + e_{ij}$. 考虑 CK_{ij} 和 $K_{ij}C$ 的第 (i, j) 位置元素，有 $c_i = c_j$. 所以 $Z \subset \{kI\}$. 综上，$Z = \{kI\}$. ■

[11] 习题 5.6

评注 一般而言，在检验和可逆矩阵相关的性质的时候，可以先在初等矩阵检验.

2.6 同构

57 定义 (同构[12]) 若一个群的同态是双射，则称它为一个同构. 若在群 G 和 G' 中存在一个同构，则称它们是同构的.

58 引理 若 $\varphi : G \to G'$ 是同构，则 φ^{-1} 也是一个同构.

证明 双射的反函数是双射是显然的，所以需要证明的是 φ^{-1} 是一个同态.

评注 这一引理表明了，对于同构的两个群，我们无法仅通过它们的运算过程来区分两者.

59 定义 (同构类) 称和给定的群 G 同构的群的全体为 G 的同构类.

60 定义 (自同构[13]) 称从群自身到自身的同构为自同构.

评注 显然 I 是自同构. g 的共轭作用 $\varphi(x) = gxg^{-1}$ 也是一个自同构. 注意，这里的 x 是 G 中的元素，其结果也是，而在正规子群的定义的中，这两者有要求是子群 N 中的元素. 另外一般而言，确认两个元素 x，y 是否共轭即尝试求解方程 $yg = gx$.

61 引理 (交换子) 设 a, b 是群 G 中的两个元素，$ab = ba$ 当前仅当 $aba^{-1} = b$，当且仅当 $aba^{-1}b^{-1} = 1$. 称 $aba^{-1}b^{-1}$ 为交换子.

62 命题 [14] 同态 $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ 只可能是 $\varphi(x) = kx$ 的形式，其中 $k \in \mathbb{Z}$.

证明 首先由于 φ 是同态，所以 $\varphi(0) = 0$. 对于正整数 x，$\varphi(x) = \varphi(1)x$，$\varphi(-x) = -\varphi(x) = \varphi(1)(-x)$. ■

评注 取 $k = 1$，则 φ 是同构. 对于 $k \neq 0$，φ 都是单射. 对于 $k = \pm 1$，φ 是满射.

2.7 等价关系与划分

63 命题 (核的陪集) 设 K 是同态 $\varphi : G \to G'$ 的核. 则包含了元素 a 的 φ 的纤维是陪集 aK. 这些陪集构成了 G 的一个划分，它们分别对应了 $\varphi(G)$ 中的一个元素.

评注 纤维实际上就是一个同余类，而根据定理 51可知，同余类中的元素和核 K 的陪集都是同一个.

[14] 习题 2.6.2

2.8 陪集

64 命题 设 H 是 G 的子群，则 H 的左陪集是同余关系下的等价类. 其中定义同余关系为

$$a \equiv b \quad 若 \quad \exists h \in H \,\text{s.t.}\, b = ah.$$

评注 若要验证这一命题，首先需要验证如此定义的同余关系确实是一个等价关系，接下来需要证明对于任意 $x, y \in aH$，存在 $h \in H$，成立 $x = yh$. 对于右陪集，也有类似的结论，只是它们所确定的划分并非同一个.

65 推论 子群 H 的左陪集构成了 G 的一个划分.

66 定义 (指数[15]) 定义子群 H 的左陪集的个数为 H 在 G 中的指数.

67 引理 (左陪集与阶) G 的子群 H 的所有左陪集 aH 的阶数都相等.

证明 $h \mapsto ah$ 是一个双射，所以所有左陪集的阶数都与 H 相同. ■

68 定理 (Lagrange) 设 H 是有限群 G 的一个子群，则 H 的阶数整除 G 的阶数.

评注 实际上由之前的引理可知，G 的阶数为 H 的阶数和指数的乘积，即

$$|G| = |H|[G : H]. \tag{1}$$

69 推论 有限群 G 的元素 x 的阶数整除 G 的阶数.

70 推论 设 G 的阶数 p 为素数，而 $a \in G$ 不是单位元，则 $G = \langle a \rangle$.

证明 根据推论 69，$\langle a \rangle$ 的阶数为 p，因此 $\langle a \rangle$ 的指数为 1. 所以它的唯一左陪集，即它本身，构成了 G 的一个划分，即 $G = \langle a \rangle$. ■

评注 这一推论说明了，所有的阶数为素数 p 的群都是同构的，即它们是 p 阶循环群.

71 命题 $[G : \ker \varphi] = |\operatorname{im} \varphi|$.

评注 这一命题描述了 $\ker \varphi$ 的陪集和 $\operatorname{im} \varphi$ 中的元素一一对应这一事实.

72 推论 设 $\varphi : G \to G'$ 是有限群的同态，则

1. $|G| = |\ker \varphi||\operatorname{im} \varphi|$.
2. $|\ker \varphi|$ 整除 $|G|$.
3. $|\operatorname{im} \varphi|$ 整除 $|G|$ 和 $|G'|$.

73 定理 (指数可乘性) 设 $K \subset H \subset G$ 是群 G 的子群，则 $[G : K] = [G : H][H : K]$.

证明 由于 G 不一定有限，所以不能够直接应用 (1). 大致的思路是利用陪集构成了一个划分：H 的陪集构成了 G 的一个划分，而对于每一个陪集，利用 K 的陪集所产生 H 的划分，可以对于每个陪集对应出一个划分. 将这两者拼在一起，就得到了 G 的令一个划分，而这个划分中的每个集合，都是 K 的陪集.

虽然一定程度上，并不能直接说这个划分就是 K 的全体陪集，但是证明也并不复杂，假设有 $n+1$ 个陪集，分别则有 $n+1$ 个代表元，把它们放入之前的 n 个集合中，根据鸽巢原理，至少有两个落在同一个等价类中.

对于指数有无限的情况，证明是类似的. ■

74 定理 设 H 是群 G 的子群，记 $gHg^{-1} = \{ghg^{-1} \mid g \in G, h \in H\}$. 则如下命题等价：

1. H 是正规子群，即对于任意 $g \in G$，$h \in H$，成立 $ghg^{-1} \in H$.
2. 对于任意 $g \in G$，$gHg^{-1} = H$.
3. 对于任意 $g \in G$，$gH = Hg$.
4. 任意 H 的左陪集也是一个右陪集.

证明 假设 [1.] 成立，则显然有 $gHg^{-1} \subset H$. 同理，$g^{-1}Hg \subset H$. 对前式子两边同时左乘 g，右乘 g^{-1}，得[16]$H \subset gHg^{-1}$. 所以 [2.] 成立. 同时，[2.] 可推出 [1.] 是显然的. 同样的 [2. 3.] 的等价性以及 [3.] 推出 [4.] 都是类似或显然的.

对于 [4.] 推出 [3.]，我们所需要说明的是，[4.] 中保证的 gH 所等于的右陪集恰好是 Hg. 设 $gH = Hk$，取 $1 \in H$，可以发现 Hk 和 Hg 有共同元素 g，根据等价类的定义，成立 $Hk = Hg$. ■

75 命题 设 G 的子群 H 是唯一一个阶为 r 的子群，则 H 正规.

证明 H，gH，gHg^{-1} 的阶数都为 r，所以 $H = gHg^{-1}$. 根据定理 74，H 正规. ■

76 定理 (线性方程组) 考虑 $(\mathbb{R}^m, +)$. 设齐次线性方程组 $AX = 0$ 的解全体为 W，则线性方程组的 $AX = B(B \neq 0)$ 的解全体组成的集合或不存在，或是 W 的陪集.

证明 实际上可以将左乘 A 看作一个同态 $A : \mathbb{R}^m \to \mathbb{R}^n$，而 W 即为它的核. 根据 命题 63，只要 $AX = B$ 的解集不为空，则它就是核 W 的一个陪集. ■

分析群的阶数的方法 一般来说，会给出一个群的阶数、群中元素的阶数等相关信息中的一部分，要求给出剩余的相关信息. 可以考虑如下的方法，首先根据定理 68，Lagrange 定理，知道群和子群阶数的整除相关的信息. 接着，如果是循环子群，则可以利用 命题 44来得到其他一部分子群的阶数. 另外的，如果给定的信息中包含素数，则常常可以利用推论 70得到更多的信息.

[16]这一操作的合法性由陪集的定义保证.

2.9 模运算

77 命题

1. 同余关系是等价关系.
2. a 模 n 的同余类为 $\mathbb{Z}n$ 的左陪集 $a+\mathbb{Z}n$.
3. 共有 n 个模 n 的同余类，分别为 $\bar{0},\dots,\overline{n-1}$.

78 定理 在模 n 意义下，若 $a\equiv a'$，$b\equiv b$，则 $a'+b'\equiv a+b$，$a'b'\equiv ab$.

评注 即，我们可以定义

$$\overline{a+b}=\bar{a}+\bar{b},\quad \overline{ab}=\bar{a}\bar{b}.$$

与此同时，可以证明它们满足分配律等性质.

79 定理 (中国剩余定理) 设 $a,b,u,v\in\mathbb{Z}$ 且 $\gcd(a,b)=1$，则存在 $x\in\mathbb{Z}$，成立 $x\equiv u \mod a$ 且 $x\equiv v \mod b$.

证明 首先取 $u=0$，$k=1$，则方程等价于 $k_1a+k_2b=1$，由于 a 和 b 互素，所以根据推论 39，存在整数 k_1 和 k_2 使上式成立. 考虑一般的 u 和 v，则方程等价于 $n_1a+n_2b=v-u$. 取 $n_1=(v-u)k_1$，$n_2=(v-u)k_2$，它满足上式. ■

2.10 对应定理

80 命题 设同态 $\varphi:G\to\mathcal{G}$ 的核为 K，设 $\mathcal{H}$ 是 $\mathcal{G}$ 的一个子群. 记 $H=\varphi^{-1}(\mathcal{H})$. 则

1. H 是 G 的一个包含 K 的子群.
2. 若 $\mathcal{H}$ 是正规子群，则 H 也是.
3. 若 φ 是满射且 H 是正规子群，则 $\mathcal{H}$ 也是.

81 定理 (对应定理[17]) 设满射同态 $\varphi:G\to\mathcal{G}$ 的核为 K. 则在 $\mathcal{G}$ 的子群与 G 的包含 K 的子群之间存在一个双射，它为

$$K\subset H\subset G\mapsto\varphi(H)$$
$$\mathcal{H}\subset\mathcal{G}\mapsto\varphi^{-1}(\mathcal{H}).$$

且满足 H 是正规子群当且仅当 $\mathcal{G}$ 为正规子群，以及 $|H|=|\mathcal{H}||K|$.

评注 这一定理使得我们可以通过研究一个同态的群的子群来研究某个群本身的子群.

证明 设 H 和 $\mathcal{H}$ 分别是 G 和 $\mathcal{G}$ 的子群，且 $K \subset H$，则证明包括对以下内容的验证：

1. $\varphi(H)$ 是 $\mathcal{G}$ 的子群.

2. $\varphi^{-1}(\mathcal{H})$ 是 G 的子群，且包含 K.

3. $\mathcal{H}$ 是正规子群当且仅当 H 是正规子群.

4.（双射）$\varphi(\varphi^{-1}(\mathcal{H})) = \mathcal{H}$，$\varphi^{-1}(\varphi(H)) = H$.

5. $|\varphi^{-1}(\mathcal{H})| = |\mathcal{H}||K|$.

其中 [1.] 是显然的，而 [2. 3.] 由命题 80保证. 对于 [4.] 由于 φ 是满射，所以前者显然成立. 对于后者，$H \subset \varphi^{-1}(\varphi(H))$ 显然成立，考虑另一方向. 设 $x \in \varphi^{-1}(\varphi(H))$，则存在 $h \in H$，成立 $\varphi(x) = \varphi(h)$，从而 $\varphi(h^{-1}x) = 1$，即 $h^{-1}x \in K \subset H$，所以 $x \in H$. 综上，[4.] 成立. 至于 [5.]，注意到 H 是一个子群，而 $\mathcal{H}$ 是像集以及 K 是对应同态的核，则利用推论 72即可证明. ■

82 命题 设记号同定理 81. $[G : H] = [\mathcal{G} : \mathcal{H}]$.

2.11 直积

83 定义 (直积) 对于群 G 和 G',定义它们的直积为 $(G\times G', \cdot)$,其中 $(a, b)\cdot(a', b') = (aa', bb')$.

评注 可以证明，两个群的直积依然是一个群. 而对于一个给定的群 G，将它直积分解的含义是，找两个通常而言更简单的群 H 和 H'，使得 G 和 $H \times H'$ 同构. 另外，对于 $x \in G$ 和 $x' \in G'$，考虑如下四个映射通常是有用的：

$$i(x) = (x, 1), \quad i(x') = (1, x'), \quad p(x, x') = x, \quad p'(x, x') = x'.$$

84 命题 (循环群的分解) 设整数 r 和 s 互素. 一个阶为 rs 的循环群与一个阶为 r 的群和一个阶为 s 的循环群的直积同构.

证明 设 $\langle x\rangle$ 的阶为 rs，满足 $x^{rs} = 1$. 则 $\langle x^r\rangle$ 和 $\langle x^s\rangle$ 的阶分别为 s 和 r. 考虑 $y = (x^r, x^s)$，由于 $\gcd(r, s) = 1$，所以最小的满足 $y^k = 1$ 的 k 为 rs. 即 $\langle x\rangle$ 与 $\langle y\rangle$ 同构. ■

85 定理 (直积的同构) 设 H 和 K 是群 G 的子群，定义 $f : H \times K \to G$ 为 $f(h, k) = hk$. 记它的像集为 HK. 则

1. f 为单射当且仅当 $H \cap K = \{1\}$.

2. f 是 $H \times K$ 到 G 的同态当且仅当对任意 $h \in H$，$k \in K$，$hk = kh$.

3. 若 H 是 G 的正规子群，则 HK 是 G 的子群.

4. f 是 $H \times K$ 到 G 的同构当且仅当 $H \cap K = 1$，$HK = G$ 且 H 和 K 是 G 的正规子群.

评注 这一定理的动机在于一般而言，构造验证某个直积和另一个群同构的同构并不方便，这一定理给出了一个一般的映射，并给出了它是一个同构的充要条件.

证明 对于 [1.] 利用定义和投影即可证明. 而 [2.] 是显然的. [3.] 可利用 $h_1k_1h_2k_2 = h_1(k_1h_2k_1^{-1})k_1k_2$. 至于 [4.]，双射是显然的，而同态利用 [2.] 和 $H \cap K = 1$ 以及引理 61即可证明. ■

86 定义 (Klein 四元群) Klein 四元群是指由如下四个矩阵构成的群

$$\begin{pmatrix} \pm 1 & \\ & \pm 1 \end{pmatrix}$$

它是最小的非循环群.

评注 考虑一个向量 $x \in \mathbb{R}^2$，左乘一个 Klein 四元群里的矩阵对应着将 x 沿着 x 或 y 轴或关于原点翻转，或保持不变.

87 定理 (4 阶的群) 4 阶的群共有两个同构类，其一为 4 阶循环群 C_4 所处的同构类，其一为 Klein 四元群所处的同构类，$C_2 \times C_2$ 也属于这一同构类.

证明 设 $|G| = 4$. 若存在 $x \in G$，它的阶为 4，则 $\langle x \langle = G$，即 G 为 4 阶循环群.

对于另一情况：若任意非单位的 $x \in G$，阶都为 2. 考虑使用定理 85来证明，首先先构造处 H 和 K 并验证相关的条件. H 和 K 可以是 G 中两不同元素生成的循环子群. 则 $H \cap K = \{1\}$ 是自然成立的. 同时，利用它们的阶为 2，可知 $H = \{1, x\}$，$K = \{1, y\}$，不难推出 $HK = G$. 接下来只需证明它们都正规. 由于任意元素的阶都为 2，所以它们的逆就为本身. 所以 $aba^{-1}b^{-1} = (ab)(ab) = 1$，其中 a, b 为 G 中任意元素，所以 G 是 Abel 群，从而 G 的任意子群为正规子群. 所以另一同构类为 $C_2 \times C_2$ 所属的同构类. 关于 Klein 四元群和 $C_2 \times C_2$ 的同构的证明略. ■

88 例 设 G 包含一个阶为 5 和一个阶为 3 的正规子群 H 和 K，则 G 包含一个阶为 15 的元素.

证明 由于 5 和 3 是素数，所以根据推论 70，H 和 K 是循环群，设生成它们的元素分别为 h 和 k. 根据 定理 85，HK 是 G 的子群且与 $H \times K$ 同构. 对任意的 $p \in \{0, \ldots, 4\}$ 和 $q \in \{0, 1, 2\}$，根据定理 79，存在 $n \in \mathbb{Z}$，成立 $n \equiv p \mod 5$，$n \equiv q \mod 3$，即 $HK = \langle (h, k) \rangle$. 同时 $(h, k)^n = 1$ 的最小正整数解为 15. 综上，HK 是 G 中的阶为 15 的循环子群. ■

2.12 商群

89 命题 设 N 是群 G 的正规子群，aN 和 bN 是 N 的陪集，则 $(aN)(bN)$ 也是 N 的陪集，且成立 $(aN)(bN) = (ab)N$.

证明 [18] 由于 N 是正规子群，所以根据定理 74，它的左陪集和右陪集相等，所以有

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)(NN) = (ab)N. \quad \blacksquare$$

评注 若 H 不是正规的，则存在 a 和 b，使 $(aH)(bH)$ 不是陪集. 证明如下：反证法，假设一定是左陪集. 取 $a = g, b = g^{-1}$，则由于 $1 \in (gH)(g^{-1}H)$，所以 $(gH)(g^{-1}H) = 1H = H$. 则对任意 $h \in H$，$ghg^{-1} = ghg^{-1}1 \in (gH)(g^{-1}H) = H$，即 H 正规，与已知矛盾. $\blacksquare$

90 引理 设 G 是一个群，Y 是一个定义了复合律的集合. 设 $\varphi : G \to Y$ 是一个有同态性质的满射. 则 Y 也是一个群且 φ 是一个同态.

91 定理 设 N 是群 G 的一个正规子群，记 $\bar{G}$ 是 N 的陪集全体. 则存在一个复合律，使得 $\bar{G}$ 构成一个群，且映射[19] $\pi : G \to \bar{G}$，$\bar{a} = \bar{a}$ 是一个满射同态且 $\ker \pi = N$.

证明 本节前述的命题与引理，分别定义了复合律并证明了 $\bar{G}$ 构成了一个群，所以仅需要再证明 $\ker \pi = N$ 即可，根据相关定义，这是显然的. $\blacksquare$

92 推论 设 N 是群 G 的正规子群，$\pi : G \to \bar{G}$ 为标准同态. 设 $a_1, \ldots, a_k \in G$ 满足 $a_1 \cdots a_k \in N$，则 $\bar{a}_1 \cdots \bar{a}_k = \bar{1}$.

证明 $p = a_1 \cdots a_k \in N$，则 $\bar{a}_1 \cdots \bar{a}_k = \pi(a_1 \cdots a_k) = \bar{p} = \bar{1}$. $\blacksquare$

93 定理 (群同构第一定理) 设 N 是满射群同态 $\varphi : G \to G'$ 的核，则商群 $\bar{G} = G/N$ 与 $\operatorname{im} \varphi = G'$ 同构. 即，设 $\pi : G \to \bar{G}$ 为标准映射，则存在唯一的同构 $\bar{\varphi} : \bar{G} \to G'$，成立 $\varphi = \bar{\varphi} \circ \pi$.

证明 首先注意，同态的核是一个正规子群，所以所说的商群是符合定义的. 根据命题 63，对于任意 $g' \in G'$，对应有唯一一个 N 的陪集，即 $\bar{G}$ 中的一个元素. 所以可以考虑定义 $\bar{\varphi}(\bar{g}) = \varphi(g)$，可以证明这是一个同构. $\blacksquare$

94 推论 设 N 和 H 分别是 $\varphi : G \to G'$ 的核和像，则 G/N 与 H 同构.

[18] 在此定义集合 $AB = \{x \mid a \in A, b \in B\}$.

[19] 称这一映射为标准映射（Canonical Map）

2.13 杂项

95 命题 [20]

1. 任意偶数阶的群必含有阶为 2 的元素.
2. 任意 21 阶群必含有阶为 3 的元素.

证明 根据命题 45，阶数大于 2 的元素个数为偶数，而阶数为 1 的元素仅有单位元，而因为群为偶数阶，所以必然必然存在阶为 2 的元素.

对于 21 阶群 G. G 的任意非单位的元素 x 的阶数为 $\{3,7,21\}$ 中的一个. 如果 x 的阶为 21，则 x^7 的阶为 3. 假设仅有阶为 7 的元素. 则取 $h\in G$，记 $H=\langle h\rangle$，同时取 G 中元素 $g\notin H$. 下证 $H,\dots,g^6H$ 不相交. 设 $g^ah^p=g^bh^q$，则 $g^{a-b}=h^{q-p}$. 由于 $g\notin H$，所以 $g^{a-b}=1$，即 $a\equiv b \mod 7$. 所以它们不相交. 因此 $[G:H]\geq 7$，所以 $|G|\geq 49$，矛盾. ■

96 定义 设 $a,b\in S\subset\mathbb{R}^k$，称 a 和 b 由一条 S 中的路径连接，若存在连续的映射 $X:[0,1]\to S$ 成立 $X(0)=a$，$X(1)=b$.

[20] 习题 2.M.2

3 向量空间

3.1 $\mathbb{R}^n$ 的子空间

3.2 域

97 定义 (域) 设集合 F 定义了如下被称作加法和乘法的复合律

$$F \times F \to^{+} F \quad 和 \quad F \times F \to^{\times} F.$$

称 F 为域若它满足如下性质

1. 加法使 F 构成了一个 Abel 群 F^{+}，记其单位元为 0.
2. 乘法满足交换律，且乘法使 F 的非零元素全体构成了一个 Abel 群 $F^{\times}$，记其单位元为 1.
3. 满足分配律：$a(b+c) = ab + ac$.

评注 [2.] 需要单独说明满足交换律，只要是为了处理与 0 相乘的情况. 另外可以证明：

1. $0 \neq 1$.
2. $0a = a0 = 0$.
3. 乘法满足结合律，1 是 F 全体[21]的乘法单位元.

98 定义 (子域) 设 F 为域，称 $L \subset F$ 为其子域，若它对加减乘除封闭且包含乘法单位元.

评注 可以证明 $0 = 1 - 1$ 成立，从而 $0 \in L$.

99 定理 设 p 为素数，则任意非零的模 p 同余类有逆元，因此 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 为一个阶为 p 的域.

评注 这一定理声称 $\mathbb{F}_p^{\times}$ 是一个群. 如果它结论成立的话，那么我们可以知道 $|\mathbb{F}_p^{\times}| = p-1$ 为一有限数，所以它的任意元素 $\bar{a}$ 的阶也是一个有限数，设为 r. 即有 $\bar{a}^r = 1$，从而它的逆元为 $\bar{a}^{r-1}$.

[21]定义中仅说是非零子集的单位元.

证明 首先可以证明 $\mathbb{F}_p^\times$ 有消去律，即若 $\bar{a}\bar{b}=0$，则 $\bar{a}=0$ 或 $\bar{b}=0$；若 $\bar{a}\neq -$ 且 $\bar{a}\bar{b}=\bar{a}\bar{c}$，则 $\bar{b}=\bar{c}$. 接下来只需要对于 $\bar{1},\bar{a},\bar{a}^2,\dots$ 以及 $\mathbb{F}_p^\times$ 施鸽巢原理以及消去律即可. ■

100 定义 (特征[22]) 定一个域 F 的特征为它的乘法单位元 1 作为加法群中元素时的阶数，若其阶数为无穷，则定义特征为零.

101 引理 域的特征或为零，或为一个素数.

证明 设特征为 $m\neq 0$. 记乘法单位元为 $\bar{1}$，$\bar{n}$ 为 n 个 $\bar{1}$ 相加的结果. $\bar{1}$ 在加法意义下生成的子群 $\langle\bar{1}+\rangle=\{\bar{0},\bar{1},\dots,\overline{m-1}\}$. 若 m 不为素数，则 $m=rs$，其中 $r,s\neq 1$. 即成立

$$\bar{0}=\bar{m}=\overline{rs}=\sum_1^{rs}\bar{1}=\left(\sum_1^{r}\bar{1}\right)=\left(\sum_1^{s}\bar{1}\right)=\bar{r}\bar{s}.$$

而 $\bar{r},\bar{s}\in F^\times$ 但 $\bar{0}\notin F^\times$，同时 $F^\times$ 是一个群，矛盾. ■

102 定理 (乘法群的结构) 设 p 为素数. 则 $\mathbb{F}_p^\times$ 是 $p-1$ 阶循环群.

评注 证明见之后的内容.

103 推论 (Fermat) 设 p 为素数，则对任意 $a\in\mathbb{Z}$，成立 $a^p\equiv a \mod p$.

104 推论 (Wilson) 设 p 为素数，则 $(p-1)!\equiv -1 \mod p$.

证明 考虑 $\mathbb{F}_p^\times=\{1,2,\dots,p-1\}$，根据定理 102它是 $p-1$ 阶循环群，所以

$$(p-1)!=\prod_{k=0}^{p-2}(p-1)^k=(p-1)^{(p-2)(p-1)/2}\equiv p-1\equiv -1 \mod p.$$

105 定义 (原根) 能生成 $\mathbb{F}_p^\times$ 的数被称作模 p 的原根.

[22]Characteristic