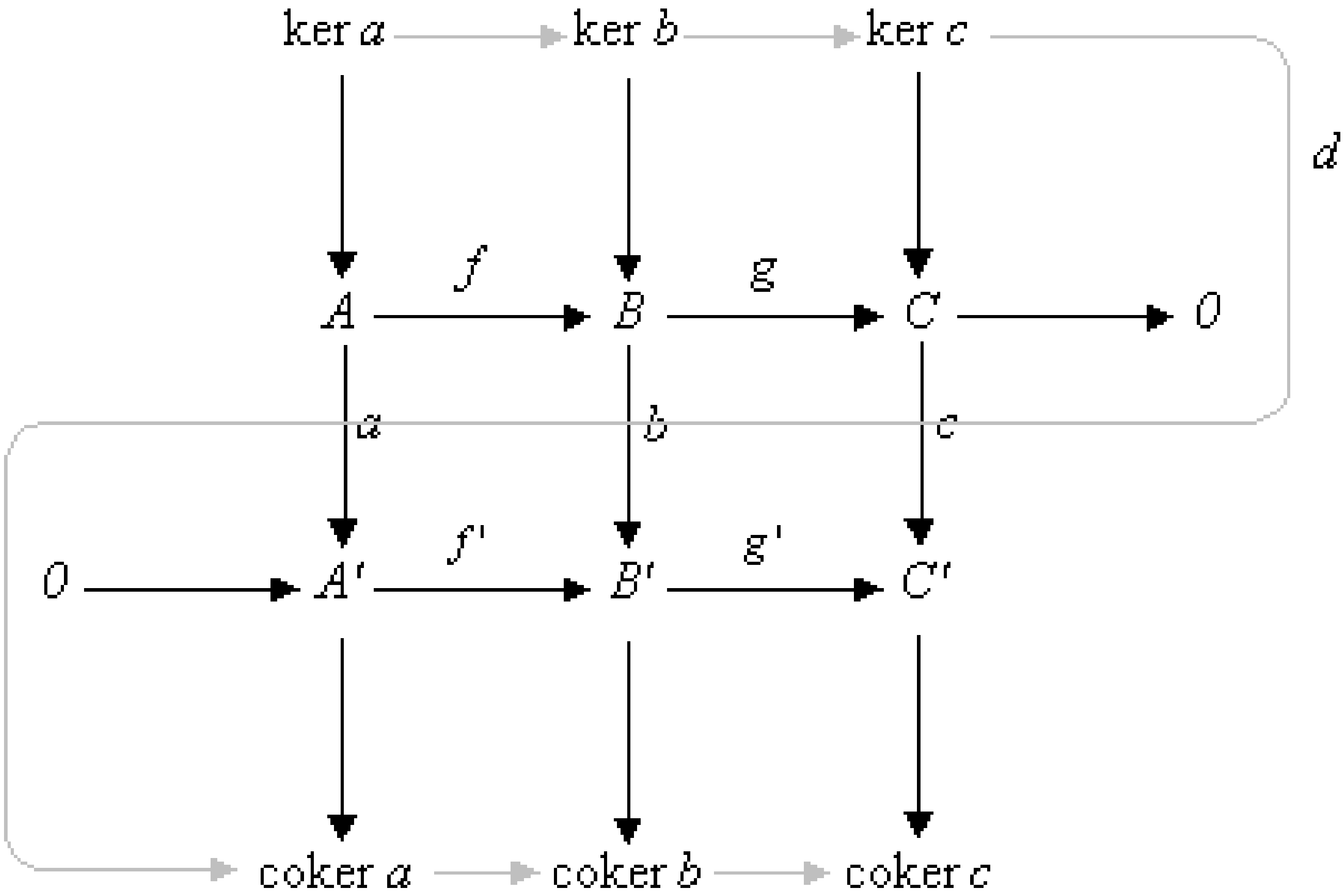

Abstract Algebra

Abstract Algebra

作者：Peknt
组织：清疏大学
时间：March 26, 2024
版本：1.1
作者联系方式：QQ2499032096

晚上不要听歌，不要在群里聊天，有时间就要学习

前言

参考书

- 近世代数引论，冯克勤，李尚志，章璞
- 近世代数 300 题，冯克勤，章璞
- 伽罗瓦理论—天才的激情，章璞
- *Abstract Algebra*,Dummit,Foote

参考资料

- 南开大学徐彬斌抽象代数讲义
- 上海交通大学章璞课程 PPT
- 南开大学凯淼淼抽象代数 note

目录

第 1 章 群论

1.1 群的概念

定义 1.1 (群)

设 G 是带有二元运算 $\cdot$ 的非空集合。如果 $(G,\cdot)$ 具有下述三条性质：

(G1) 结合律：$(a\cdot b)\cdot c=a\cdot(b\cdot c),\forall a,b,c\in G$

(G2) 存在单位元：存在 $e\in G$，使得 $e\cdot a=a\cdot e=a,\forall a\in G$

(G3) 每个元均有逆元：对任意 $a\in G$，存在 $b\in G$，使得 $a\cdot b=b\cdot a=e$

则称 $(G,\cdot)$ 是一个群 (Group)

♣

注 开始时，我们用 $(G,\cdot)$ 表示一个群，以后当二元运算不言自明时，我们就简单地称 G 是群。如果不引起混乱，今后我们常将运算符号 $\cdot$ 省略不写。例如将 $a\cdot b$ 简写成 ab

例题 1.1 我们称集合 A 到自身的一个双射为 A 上的一个置换，集合 A 上的所有置换记为 $S(A)$，可知 $S(A)$ 关于映射的复合构成群。

定义 1.2 (半群和含幺半群)

如果 $(G,\cdot)$ 满足 $(G1)$，则称 G 是半群 (semigroup)。

如果 $(G,\cdot)$ 满足 $(G1)$ 和 $(G2)$，则称 G 是含幺半群 (monoid)。

♣

定义 1.3 (阿贝尔群)

设 $(G,\cdot)$ 是群。若 $ab=ba,\forall a,b\in G$，则称 $(G,\cdot)$ 为交换群，又称为阿贝尔群，或 Abel 群。

♣

命题 1.1

(1) 存在半群 S，S 中有左幺元，但没有右幺元。

(2) 若一个半群 S 中既有左幺元，又有右幺元，S 是否一定为含幺半群？

♠

解 (1) 考虑 $S=\{\begin{pmatrix} a & b\\ 0 & 0\end{pmatrix}\mid a,b\in R\}$ 关于矩阵乘法构成的半群，则易见其有无穷多左幺元 $\begin{pmatrix} 1 & c\\ 0 & 0\end{pmatrix}$ 其中 $c\in R$，而容易验证其没有右幺元。

(2) 设 S 有左幺元 e_1，右幺元 e_2，则有 $e_1=e_1\cdot e_2=e_2$，从而左右幺元相等，故有唯一元素为左幺元和右幺元，从而为含幺半群。

命题 1.2

(1) 存在含幺半群 S 及 $a\in S$，a 存在左逆元，但不存在右逆元。

(2) 若含幺半群 S 中元素既有左逆元，又有右逆元，则 a 一定是可逆元。

♠

解 (1) 记 $M(N)$ 为 N 的所有变换组成的含幺半群，其中元素 f 定义为

$$f(n)=n+1,\forall n\in N$$

考虑 $g_k(n)=\begin{cases} n-1,n\geq 1\\ k,n=0\end{cases}$ 从而对任意 $k\in N$ 有 $g_kf(n)=n$，从而 g_k 为左逆元，故有无穷多左逆元。但是若存在右逆元 h，则 $f(h(0))=0$，即 $h(0)+1=0$，即 $h(0)=-1$，矛盾，所以不存在。(2) 设 $ba=ac=e$，则有 $b=be=b(ac)=(ba)c=ec=c$，得证

性质 [群的简单性质]

(1)G 的单位元是唯一的（用 e 表示 G 的单位元）

证　设 e 和 $e^{'}$ 都是 G 的单位元，则 $e = ee^{'} = e$

(2)G 中任意元 a 的逆元是唯一的（今后用 a^{-1} 表示 a 的逆元）

证　设 b 和 c 都是 a 的逆元，则 $c = ec = (ba)c = b(ac) = be = b$

(3) 穿脱原理：$(ab)^{-1} = b^{-1}a^{-1}, \forall a, b \in G$，以及 $(a^{-1})^{-1} = a, \forall a \in G$

证　由 $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$ 以及

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$

知 $(ab)^{-1} = b^{-1}a^{-1}$，类似可证 $(a^{-1})^{-1} = a$

(4) 左消去律：即，由 $ab = ac$ 可推出 $b = c$。右消去律：即，由 $ba = ca$ 可推出 $b = c$

证 由 $ab = ac$ 知 $a^{-1}(ab) = a^{-1}(ac)$，由此即得 $(a^{-1}a)b = (a^{-1}a)c$，即 $eb = ec$，即 $b = c$。同理，可证右消去律。

定义 1.4 (有限群的群表)

考虑一个有限群 $G = \{a_1, \cdots, a_n\}$ 我们将 G 中元素两两相乘的结果列出（(i, j) 位置上为 a_ia_j）

a_1a_1	a_1a_2	$\cdots$	a_1a_n
a_2a_1	a_2a_2	$\cdots$	a_2a_n
$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_na_1	a_na_2	$\cdots$	a_na_n

♣

命题 1.3

一个有限群 G 交换当且仅当相应的群表对称

♠

在一个半群 G 中，一个元 $e_l \in G$ 称为 G 的左幺元，如果 $e_lg = g, \forall g \in G$

设半群 G 有左幺元 e_l，称元 $a \in G$(相对于 e_l) 有左逆元，如果存在 $a_l^{-1} \in G$ 使得 $a_l^{-1}a = e_l$，将 a_l^{-1} 称为 a 的左逆元

命题 1.4 (群的单边定义)

设 G 是半群，则 G 是群当且仅当 G 有左幺元，且任一元均有左逆元

♠

证明　必要性显然，只需证明充分性。

先证 g 的左逆元有性质 $gg_l^{-1} = e_l$, 有

$$\begin{aligned} gg_l^{-1} &= e_l(gg_l^{-1}) \\ &= ((g_l^{-1})_l^{-1}g_l^{-1})gg_l^{-1} \\ &= (g_l^{-1})_l^{-1}(g_l^{-1}g)g_l^{-1} \\ &= (g_l^{-1})_l^{-1}e_lg_l^{-1} \\ &= (g_l^{-1})_l^{-1}g_l^{-1} \\ &= e_l \end{aligned}$$

现在证明 e_l 也是 G 的右幺元，从而 e_l 是 G 的单位元。对任一元 g，由 $gg_l^{-1} = e_l$ 知

$$ge_l = g(g_l^{-1}g) = (gg_l^{-1})g = e_lg = g$$

即，e_l 也是 G 的右幺元。

最后，由性质 $gg_l^{-1} = e_l$ 知 g 的左逆元 g_l^{-1} 也是 g 的逆元。根据定义，G 是群。

命题 1.5

(1) 上述命题改为右幺元和右逆元也成立。

(2) 若改为一左一右，则命题不再成立。

命题 1.6 (有限半群成群的充要条件)

设 $(G,\cdot)$ 是有限半群，则 $(G,\cdot)$ 是群当且仅当 $(G,\cdot)$ 满足左消去律和右消去律。

证明 必要性显然，只需证明充分性。

设 $(G,\cdot)$ 是满足左消去律和右消去律的有限半群。取 $a \in G$，考虑 G 的子集 $Ga := \{ga \mid g \in G\}$，用 $|Ga|$ 表示 Ga 中元素的个数。由右消去律知，$|Ga| = |G|$。因为 G 是有限集合，所以 $Ga = G$。于是存在 $e \in G$ 使得 $ea = a$。

下证 e 是 G 的左单位元。对任意 $x \in G$，由左消去律知 $aG = G$，故存在 $y \in G$ 使得 $x = ay$。于是

$$ex = e(ay) = (ea)y = ay = x$$

则 e 是 G 的左单位元

再证任意元 $x \in G$ 均有左逆元，由 $Gx = G$ 知存在 $y \in G$ 使得

$$yx = e$$

即，x 有左逆元 y

根据群的单边定义，$(G,\cdot)$ 是群。

命题 1.7 (含幺半群生成群)

设 S 是含幺半群，记 $U(S)$ 为 S 中可逆元全体，则 $U(S)$ 构成群。

1.2 子群与陪集

定义 1.5 (子群)

设 $(G,\cdot)$ 是群，H 是 G 的非空子集。如果 $\cdot$ 也是 H 的二元运算，并且 $(H,\cdot)$ 也是一个群，则称 H 为群 G 的子群 (subgroup)，记为 $H \leq G$。此外，若 $H \neq G$，则称 H 为 G 的真子群，记为 $H < G$

显然，$G \leq G, \{e\} \leq G$，它们叫做 G 的平凡子群。

注 我们可以由子群定义得到，若 H 为 G 的一个子群，K 为 H 的一个子群，则 K 为 G 的一个子群。若 H 和 K 为 G 的子群，且 $K \subset H$，则 K 为 H 的子群。

命题 1.8

设 $H \leq G$，则 H 的单位元与 G 的单位元相同，H 的元在 H 中的逆元与它在 G 中的逆元相同。

例题 1.2 记 $n \in \mathbb{N}^*$，我们考虑 $\mathbb{R}$ 上的 n 阶可逆方阵的集合 $GL(n,\mathbb{R})$，该集合关于矩阵乘法构成群，我们一般称为**一般线性群 (General Linear Group)**。该群及其子群是李理论的研究对象的一部分。以下是 $GL(n,\mathbb{R})$ 的一些子群：

1. 特殊线性群 (Special Linear Group):

$$SL(n,\mathbb{R}) := \{A \in GLn, \mathbb{R} \mid \det A = 1\}$$

2. 正交变换群 (Orthogonal Group):

$$O(n) := \{A \in GL(n,\mathbb{R}) \mid AA^T = I_n\}$$

3. 不定正交变换群 (Indefine Orthogonal Group): 设 $p, q \in \mathbb{N}^*$，满足 $p+q=n$，记

$$I_{p,q} = \begin{bmatrix} I_p & \\ & -I_q \end{bmatrix}$$

我们记

$$O(p,q) := \{A \in GL(n,\mathbb{R}) \mid AI_{p,q}A^T = I_{p,q}\}$$

4. 辛变换群 (Symplectic Group): 设 $n = 2k$ 为偶数

$$Sp(2k) := \{A \in GL(n,\mathbb{R}) \mid A \begin{bmatrix} O_k & I_k \\ -I_k & O_k \end{bmatrix} A^T = \begin{bmatrix} O_k & I_k \\ -I_k & O_k \end{bmatrix}\}$$

从定义我们可以看出，后面的几个群都是保持 $\mathbb{R}^n$ 上某些双线性型的矩阵构成的群。这些双线性型通常与几何结构相关，对应的保持这些双线性型的群代表了此类几何结构局部的对称性，例如

O(n)	欧氏几何
O(n-1,1)	双曲几何
O(n-2,2)	Anti-de Sitter 几何
O(p,q)	伪黎曼几何
Sp_{2k}	辛几何

定义 1.6

设 G 为一个群，我们称以下 G 的子集为 G 的中心：

$$Z(G) := \{a \in G \mid \forall b \in G, ab = ba\}$$

♣

命题 1.9

设 G 为一个群，则 $Z(G)$ 为 G 的一个子群。

♠

定理 1.1 (子群的判定法则)

群 G 的非空子集 H 是 G 的子群当且仅当若 $a, b \in H$，则 $ab^{-1} \in H$

♡

证明 只要证明充分性。

因为 H 非空，故可取到 $h \in H$, 由题设有 $e = hh^{-1} \in H$。

设 $a \in H$，则由题设 $a^{-1} = ea^{-1} \in H$

设 $a, b \in H$，上面已经证明 $b^{-1} \in H$，则 $ab = a(b^{-1})^{-1} \in H$

命题 1.10

记 $\{H_\alpha\}_{\alpha \in I}$ 为 G 中任意一族子群（I 为指标集合），则

$$\bigcap_{\alpha \in I} H_\alpha$$

为 G 的子群。

♠

证明 记

$$H = \bigcap_{\alpha \in I} H_\alpha$$

由于对任意 α，H_α 为子群，因此有 $e \in H_\alpha$ 对任意 α 成立。因此，由 H 的定义有 $e \in H$，H 非空。

进一步任取 $a, b \in H$，对任意 α，有

$$a, b \in H_\alpha$$

因为 H_α 是 G 的子群，所以 $ab^{-1} \in H_\alpha$，所以 $ab^{-1} \in H$，由子群判定法则知 H 是 G 的一个子群。

例题 1.3 考虑整数 $\mathbb{Z}$ 的子群。记 $k \in \mathbb{N}^*$,$m_1, m_2, \cdots, m_k$ 为 k 个两两不同的正整数，则有

$$m_1\mathbb{Z} \cap m_2\mathbb{Z} \cap \cdots \cap m_k\mathbb{Z} = lcm(m_1, m_2, \cdots, m_k)\mathbb{Z}$$

如果我们取无穷多个两两不同的整数，则有

$$\bigcap_{k \in \mathbb{N}} m_k\mathbb{Z} = \{0\}$$

命题 1.11

两个子群的并集不一定是子群。

设 G 为群，A, B 为 G 的子群，$a \in G$，今后记

$$aA = \{ax \mid x \in A\}, Aa = \{xa \mid x \in A\}$$
$$A^{-1} = \{a^{-1} \mid a \in A\}, AB = \{ab \mid a \in A, b \in B\}$$

容易验证子集的乘积和逆也有性质：

1. 结合律：$(AB)C = A(BC)$
2. 穿脱原理：$(AB)^{-1} = B^{-1}A^{-1}$，特别地有 $(A^{-1})^{-1} = A$

如果 $H \leq G$，则有 $H^{-1} = H, HH = H$
则子群的判定定理可以重新表述为：
群 G 的非空子集 H 是 G 的子群当且仅当 $HH^{-1} \subset H$，当且仅当 $HH^{-1} = H$

定理 1.2 (两个子群的乘积称为子群的充要条件)

设 $(G, \cdot)$ 是群，$A \leq G, B \leq G$，则 $AB \leq G$ 当且仅当 $AB = BA$

证明 必要性：设 $AB \leq G$，则 $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$
充分性：设 $AB = BA$，则

$$\begin{aligned}(AB)(AB)^{-1} &= (AB)(B^{-1}A^{-1}) = (AB)(BA) = A(BB)A \\ &= ABA = BAA = BA \\ &= AB\end{aligned}$$

则有 $AB \leq G$

定义 1.7 (元素的阶)

设群 G 以及 $a \in G$，考虑子群 $< a >= \{a^n \mid n \in \mathbb{Z}\}$，则考虑该子群的阶，并将其称为 a 的阶。

定义 1.8 (生成子群、有限生成群)

设 S 是群 G 中的一个非空子集，令 $S^{-1} = \{a^{-1} \mid a \in S\}$，记

$$< S >= \{x_1 \cdots x_m \mid m \in \mathbb{N}, x_1, \cdots, x_m \in S \cup S^{-1}\}$$

不难看到 S 为子群，称为 S 生成的子群。若存在 S 使得 $< S >= G$，则称 S 为 G 的一个生成组，如果 G 有一个生成组，则称 G 为有限生成群。

命题 1.12 (生成子群的等价刻画)

群 G 中非空子集 S 生成的子群 $< S >$ 是 G 中包含 S 的子群的交，也是 G 中包含 S 的最小子群。

证明 因为 $S \subset H \leq G$，所以 $S \cup S^{-1} \subset H$，所以 $< S > \subset \bigcap\limits_{S \subset H \leq G} H$。又有 $< S > \leq G$，所以 $\bigcap\limits_{S \subset H \leq G} H \subset < S >$，所以两者相等。

定义 1.9 (陪集)

设 G 为一个群。任取 G 的一个子群 H，以及 $a \in G$，我们定义 H 关于 a 的左陪集为

$$aH := \{ab \in G \mid b \in H\}$$

H 关于 a 的右陪集为

$$Ha := \{ba \in G \mid b \in H\}$$

♣

命题 1.13

设 G 为一个群。任取 G 的一个子群 H 和一个元素 $a \in G$，我们有

1. $aH = H$ 当且仅当 $a \in H$
2. aH 为一个子群当且仅当 $a \in H$
3. 若 $a \notin H$，则 $aH \cap H = \varnothing$

♠

证明

1. 必要性：因为 $aH = H$，所以 $e \in aH$，所以 $a = ae \in aH = H$。
   充分性：当 $a \in H$ 时，由子群运算的封闭性有 $aH \subset H$，又有任意 $b \in H$，有 $b = eb = (aa^{-1})b = a(a^{-1}b) \in aH$，所以有 $H \subset aH$，综上
2. 必要性：因为 aH 为一个子群，所以 $e \in aH$, 所以 $e = aa^{-1} \in aH$，即 $a^{-1} \in H$，则 $a \in H$
   充分性：若 $a \in H$，由 (1) 有 $aH = H$，则 aH 为一个子群。
3. 假设 $aH \cap H \neq \varnothing$，则存在 $b \in H, b \in aH$，则存在 $c \in H, b = ac$，由运算封闭性，$a \in H$，矛盾，则 $aH \cap H = \varnothing$

推论 1.1

设 $H \leq G, a, b \in G$，则 $aH \cap bH = \varnothing$，或者 $aH = bH$。$aH = bH$ 当且仅当 $a^{-1}b \in H$

♡

证明 若 $a^{-1}b \in H$，则存在 $h \in H$，使得 $a^{-1}b = h$，即 $b = ah$，则 $bH \subset aH$，又有 $a = bh^{-1}$，则 $aH \subset bH$，则 $aH = bH$。若 $a^{-1}b \notin H$，易得 $aH \cap bH = \varnothing$

定义 1.10 (陪集确定的等价关系)

设 $H \leq G$，则由

$$aRb = a^{-1}b \in H$$

所确定的 G 中的关系为等价关系，且 a 所在的等价类恰是以 a 为代表元的 H 的左陪集 aH。

♣

定义 1.11

设 G 为一个群。任给 G 的子群 H，我们记 G 对 H 的左陪集空间为如下集合:

$$G/H := \{aH \mid a \in G\}$$

类似地，我们记 G 对 H 的右陪集空间为:

$$H\backslash G := \{Ha \mid a \in G\}$$

♣

命题 1.14

设 G 为一个群。任给 G 的子群 H，定义双射:

$$\phi : G/H \to H\backslash G$$
$$aH \to Ha^{-1}$$

♠

证明

1. 先说明 ϕ 是良定义的，若有 $aH = bH$，则有 $a^{-1}b \in H$，则 $a^{-1}(b^{-1})^{-1} \in H$，则 $Ha^{-1} = Hb^{-1}$，则 ϕ 是良定的。
2. 再构造 φ，
$$\varphi : H\backslash G \to G/H$$
$$Ha \to a^{-1}H$$
可以说明 φ 也是良定的。
3. 有 $(\varphi \circ \phi)(aH) = \varphi(\phi(aH)) = \varphi(Ha^{-1}) = aH, (\phi \circ \varphi)(Ha) = \phi(\varphi(Ha)) = \phi(a^{-1}H) = Ha$ 因此 ϕ 是双射。

推论 1.2

设 G 是一个群。任给 G 的一个子群 H，则 H 的左陪集空间和右陪集空间等势：
$$|G/H| = |H\backslash G|$$
♡

定义 1.12 (指数)

设 G 为一个群。任给 G 的一个子群 H，则定义 H 在 G 中的指数为：
$$[G : H] := |G/H| = |H\backslash G|$$
♣

引理 1.1

任取有限群 G 的一个子群 H 和一个元素 a，我们有 $|H| = a\,|H|$
♡

定理 1.3 (Lagrange 定理)

设 G 是一个有限群，H 为 G 的一个子群，则有
$$|G| = [G : H]\,|H|$$
♡

证明 考虑 G 中由 H 的左陪集给出的分划，设 $k = [G : H]$，设 $a_1, a_2, \cdots, a_k \in G$，满足
$$G = a_1H \cup a_2H \cup \cdots \cup a_kH$$
因此
$$|G| = |a_1H| + |a_2H| + \cdots + |a_kH| = [G : H]\,|H|$$

推论 1.3

设 G 为一个有限群，任取 G 的子群 H，我们有 H 的阶整除 G 的阶，即
$$|H| \mid |G|$$
特别地，任取 $a \in G$，则有
$$o(a) = |< a >| \mid |G|$$
♡

推论 1.4

若群 G 的阶为素数 p，则 G 为一个循环群。
♡

推论 1.5

设 G 为一个有限群，H 为 G 的子群，K 为 H 的子群，则有
$$[G : K] = [G : H][H : K]$$
♡

证明 $[G:K]=\frac{|G|}{|K|}=\frac{[G:H]|H|}{|K|}=[G:H][H:K]$

定理 1.4 (两个子群的积集的阶)

设 G 是群，A 和 B 是 G 的子群，则 $|AB|=\frac{|A||B|}{|A\cap B|}$ ♡

证明 考虑映射 $\pi: A\times B\to AB, (a,b)\to ab$，显然 π 是满射。

设 $a\in A, b\in B$，则 $ab\in AB$，考虑集合 $\pi^{-1}(ab)=\{(x,y)\in A\times B \mid xy=ab\}$。从而有 $a^{-1}x=by^{-1}$，则 $h=a^{-1}x=by^{-1}\in A\cap B$，所以 $(x,y)=(ah,h^{-1}b)$。故

$$\pi^{-1}(ab)=\{(ah,h^{-1}b)\mid h\in A\cap B\}$$

所以 $\left|\pi^{-1}(ab)\right|=|A\cap B|$

因此 $|AB|\,|A\cap B|=|A|\,|B|$

1.3 正规子群

1.4 商群

第 2 章 环论

第 3 章 模论

第 4 章 域论

第 5 章 Galois 理论