第零章 预备知识

0.1 引言

经典代数(初等代数、高等代数或线性代数)的研究对象: 代数方程, 线性方程组; 线性关系、线性结构;

抽象代数(也称近世代数): 源于代数方程求根问题, 研究对象为各种代数系统, 如群、环、域、模等.

若干经典的代数问题

(1) **Fermat 大定理** $x^n+y^n=z^n\ (n\geq 3)$ 无正整数解;

来源: 业余数学家之王 Fermat 在阅读《算术》(丢番图著)所写的书边注记. 困扰了人们 300 多年的难题, 1995, A.Wiles 证明了定理的正确性.

(2) $n\geq 5$ 时, **一元 n 次方程没有一般的求根公式.**

天才数学家 (Abel, Galois), 抽象代数的诞生.

(3) **三大几何难题**: 能否仅用圆规直尺**倍立方体, 三等分任意角, 化圆为方**?

Gauss 关于正 n 边形可以作图问题的充要条件.

抽象代数在现代科学中的应用

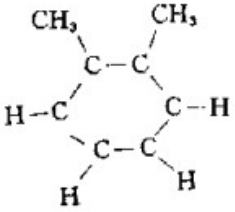
1. 计数问题

(1) 项链问题: n 种颜色的珠子串成有 m 颗珠子的项链, 本质上有多少种不同的方案? 考虑正多边形的顶点着色问题, 何谓本质不同?

(2) 分子结构的计数问题

在化学中研究由若干种元素可合成多少种不同物质的问题. 以此指导人们在大自然中寻找或人工合成这些物质.

例 2. 在一个苯环上结合 H 原子或 CH_3 原子团, 问可能形成多少种不同的化合物?

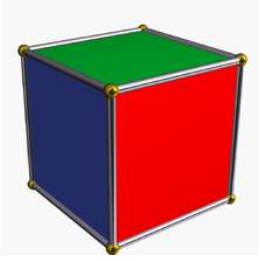


如果假定苯环上相邻 C 原子之间的键都是互相等价的, 则此问题就是两种颜色 6 颗珠子的项链问题.

(3) 正多面体着色问题

对一个正多面体的顶点或面用 n 种颜色着色, 问有多少种不同的着色方法?

例 3. 用 n 种颜色, 对正六面体的面着色, 问有多少种不同的着色方法?



(4) 图的构造与计数问题

例 4. 画出所有点数为 3 的互不同构的图.

(5) 开关线路的构造与计数问题

2. 数字通信的可靠性问题

例 5. 简单检错码—奇偶性检错码.

例 6. 简单纠错码——重复码.

设用 3 位二进制重复码表示 A, B 两个字母如下: A: 000 B: 111

则接收的一方对收到的信息码不管其中是否有错, 均可译码如下:

接收信息: 000 001 010 011 100 101 110 111

译 码: AAABABHB

目前, 抽象代数已经成为编码与纠错码等领域最重要的工具之一. 有兴趣的同学可以阅读冯克勤先生编著的《代数与通信》、《纠错码的代数理论》与《量子纠错码》等.

3. 几何作图问题

古代数学家们曾提出一个有趣的作图问题: 用圆规和直尺可作出哪些图形? 规定所用的直尺没有刻度和不能在其上作记号. 历史上, 有几个经典的几何作图问题曾经困扰人们很长时间, 它们是:

(1) 倍立方体向题 作一个立方体使其体积为一已知立方体体积的两倍.

(2) 三等分任意角问题 给定任意一个角, 将其三等分.

(3) 化圆化方问题 给定一个已知半径与圆心的圆, 作一个正方形使其面积等于已知圆的面积.

(4) 等分圆周问题. 等价于正多边形的尺规作图问题.

解决这些问题需要抽象代数中关于域扩张的一些理论.

4. 代数方程根式求解问题 一元 n 次方程求根导出的伽罗瓦理论.

5. 密码设计与分析

目前抽象代数已经成为诸多信息安全相关学科的重要数学基础: AES 算法 Rijndael、流密码、RSA 公钥体制、ElGamal 体制与 DSA 签名、椭圆曲线公钥体制、基于格的公钥体制等.

0.2 集合、关系与代数运算

1. 集合

集合 A 的**幂集合** $2^A, P(A)$

差集: $A-B:=\{x \mid x\in A \text{ 且 } x\notin B\}$, 也记为 $A\setminus B$.

对称差集: $A\oplus B:=(A-B)\cup(B-A)$.

有限集 $A=\{a_1,a_2,\ldots,a_n\}$ 的元素个数 n 称为集合 A 的**势**(大小, 长度), 记为 $|A|=n$ 或者 $\#A=n$.

可数集: 与自然数集 $\mathbb{N}=\mathbb{Z}^+=\{1,2,\cdots,n,\cdots\}$ 等势的无限集.

不可数集: 无限且不与 $\mathbb{N}$ 等势的集合.

笛卡尔积: 两个非空集合 A 与 B 的**笛卡尔积**, 或者 **Cartesian 积**规定为 $A\times B=\{(a,b)|a\in A,b\in B\}$, 类似地, 多个非空集合 $A_1,A_2,\cdots,A_n$ 的**笛卡尔积**规定为 $A_1\times A_2\times\cdots\times A_n=\{(a_1,a_2,\cdots,a_n)|a_i\in A_i,1\le i\le n\}$.

乘法原理: $1\le|A|,|B|\le\infty$时, $|A\times B|=|A|\bullet|B|$

两个集合的容斥原理: 设 A,B 都是非空的有限集, 则:

$$|A\cup B|=|A|+|B|-|A\cap B|,\quad |A\cup B|+|A\cap B|=|A|+|B|.$$

事实上, 在组合数学领域, 人们经常使用的有更一般的容斥原理.

定理 1 (容斥原理) 设 $A_1,A_2,\cdots,A_n$ 是集合 U 的有限子集合, 则:

$$\left|\bigcap_{i=1}^n A_i\right|=\sum_{i=1}^n|A_i|-\sum_{1\le i<j\le n}|A_i\cup A_j|+\sum_{1\le i<j<k\le n}|A_i\cup A_j\cup A_k|-\cdots+(-1)^{n-1}\left|\bigcup_{i=1}^n A_i\right|,$$

$$\left|\bigcup_{i=1}^n A_i\right|=\sum_{i=1}^n|A_i|-\sum_{1\le i<j\le n}|A_i\cap A_j|+\sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k|-\cdots+(-1)^{n-1}\left|\bigcap_{i=1}^n A_i\right|.$$

(用数学归纳法证明)

例 3. 求不大于 1000 并且可以被 3, 5, 7 其中一数整除的正整数的个数

解 令 $A_1=\{x|x\in\mathbb{N},x\le1000\text{ 且 }3|x\}$, $A_2=\{x|x\in\mathbb{N},x\le1000\text{ 且 }5|x\}$, $A_3=\{x|x\in\mathbb{N},x\le1000\text{ 且 }7|x\}$.

欲计算 $|A_1\cup A_2\cup A_3|$, 利用容斥原理, 可以先计算如下:

$$A_1=\left\lfloor\frac{1000}{3}\right\rfloor=333,A_2=\left\lfloor\frac{1000}{5}\right\rfloor=200,A_3=\left\lfloor\frac{1000}{7}\right\rfloor=142,$$

$$|A_1\cap A_2|=\left\lfloor\frac{1000}{15}\right\rfloor=66,|A_1\cap A_3|=\left\lfloor\frac{1000}{21}\right\rfloor=47,|A_2\cap A_3|=\left\lfloor\frac{1000}{35}\right\rfloor=28,\quad |A_1\cap A_2\cap A_3|=\left\lfloor\frac{1000}{105}\right\rfloor=9.$$

由容斥原理得:

$$|A_1\cup A_2\cup A_3|=(|A_1|+|A_2|+|A_3|)-(|A_1\cap A_2|+|A_1\cap A_3|+|A_2\cap A_3|)+|A_1\cap A_2\cap A_3|$$

$$=(333+200+142)-(66+47+28)+9=543.$$

2. 关系

设 A 是非空集合, $R\subseteq A\times A$, 则称 R 是 A 上的**二元关系**. 若 $(a,b)\in R$, 则称 a,b 有关系 R, 记为 aRb.

集合 A 上的二元关系 R 的表示方法: 集合法, 图, 矩阵表示

等价关系 非空集 A 上的二元关系"~"若满足:

(1) 自反性: $a\sim a,\forall a\in A$;

(2) 对称性: $a\sim b\Rightarrow b\sim a,\forall a,b\in A$;

(3) 传递性: $a\sim b,b\sim c\Rightarrow a\sim c\ \ \forall a,b,c\in A$

就称"~"是集合 A 上的**等价关系**.

记 $\bar{a}:=\{x\in A|x\sim a\}$, 称为 a 所在的**等价类**, 也记为 $[a]$. a 称为等价类 $\bar{a}$ 的一个**代表元**.

同余关系: 设 $n\in\mathbb{N}$, 规定 $\mathbb{Z}$ 上的一个二元关系如下:

$$a\equiv b(\mathrm{mod}\,n)\Leftrightarrow n|a-b,\forall a,b\in\mathbb{Z},$$ 称 a 与 b **模 n 同余.**

显然模 n 同余是整数集上的一个等价关系.

等价类的性质 设"~"是集合 A 上的等价关系, 则 $\bar{a}\cap\bar{b}=\varnothing$ 或 $\bar{a}$, $\forall a,b\in A$, 即任意两个等价类, 或不相交或重合.

由此可知若"~"是集合 A 上的等价关系, 则 A 上不同的等价类之并构成了 A 的一个**划分**!

设 $A\neq\varnothing,A_\alpha(\alpha\in I)\neq\varnothing,A_\alpha\subseteq A$ 满足

(1) $\bigcup\limits_{\alpha\in I}A_\alpha=A$; (2) $\forall\alpha\neq\beta\in I\Rightarrow A_\alpha\cap A_\beta=\varnothing$.

则称 $\{A_\alpha(\alpha\in I)\}$ 是 A 上的一个**划分**或者**分类.**

集合 A 上的等价关系与划分之间: A 上的一个等价关系 $\Leftrightarrow$ A 的一个划分, 每一类视为一个等价类.

例 6. 模 n 同余关系将整数划分为 n 类: $\bar{0},\bar{1},\bar{2},\cdots,\overline{n-1}$.

3. 运算

二元运算 非空集合 A 上的一个 ***n* 元运算**, 是指从 A^n 到 A 的一个映射:

$$\circ:A^n\to A,\ (a_1,a_2,\ldots,a_n)\mapsto\circ(a_1,a_2,\ldots,a_n),\forall(a_1,a_2,\ldots,a_n)\in A^n.$$

特别地, $n=2$ 时得到二元运算, 且通常将映射称为运算符号, 写在中间, 即将 $\circ(a_1,a_2)$ 记为 $a_1\circ a_2$.

如: 整数集

$(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Z},-)$, $(\mathbb{Z},\circ):a\circ b:=ab-a-b,\forall a,b\in\mathbb{Z}.$

$\mathrm{GL}(n,\mathbb{R})=\{A\in\mathbb{R}^{n\times n}|\det A\neq0\}$ 对矩阵的乘法运算.

代数系统 设 $S\neq\varnothing$, 若 S 中定义了一种运算(或多种运算), 则称 S 是一个代数系统(Algebraic System).

0.3 数论基础

1. 数学归纳法

第一数学归纳法 设 $P(n)$ 是一个关于自然数 n 的命题，如果 $P(0)$ 为真，且

假设 $P(n)$ 为真时可以证得 $P(n+1)$ 为真.

那么对所有自然数 n，$P(n)$ 均为真.

良序性质 自然数集的任一非空子集 S 必有一个最小元，即存在某 $m\in S$ 使得 $m<a,\forall a\in S$.

第二数学归纳法 设 $P(n)$ 是关于自然数 n 的命题，如果 $P(0)$ 为真，且

假设对小于 n 的自然数 k 均有 $P(k)$ 为真时，可以证得 $P(n+1)$ 为真.

那么对所有自然数 n，$P(n)$ 均为真.

2. 整数的整除理论

算术基本定理 大于 1 的整数 a 可以写成有限多个素数的乘积 $a=p_1p_2\cdots p_r$，且这些素因子按大小顺序排列后，写法只有一种.

a 的**标准分解式**：$a=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$，其中 $e_1,e_2,\cdots,e_n$ 均为正整数，素数 $p_1,p_2,\cdots p_r$ 互异.

3. 同余式和同余方程

模 n 同余 设 $a,b\in\mathbb{Z},n\in\mathbb{Z}_{>0}$，规定 $a\equiv b\pmod n\Leftrightarrow n\mid(a-b)$，简记 $a\equiv b$. 同余是整数集上的等价关系.

同余的简单性质 设 $a,b,c,d,u,v\in\mathbb{Z},n\in\mathbb{Z}_{>0}$，则

(1) $a\equiv b,c\equiv d\Rightarrow ua+vc\equiv ub+vd$，特别地，$a+c\equiv b+d,ac\equiv bd$；

(2) $ac\equiv bc,(c,n)=1\Rightarrow a\equiv b$；

(3) $a\equiv b\pmod n,m\mid n\Rightarrow a\equiv b\pmod m$；

(4) $a\equiv b\pmod n\Rightarrow(a,n)=(b,n)$；

(5) $ad\equiv bd\pmod{dn}\Rightarrow a\equiv b\pmod n$.

整数模 n 的剩余类所成集 $\mathbb{Z}_n=\mathbb{Z}/(n)=\{\bar0,\bar1,\bar2,\cdots,\overline{n-1}\}$，每个剩余类中取一个代表元所成集称为整数模 n 的一个完全剩余代表系. 关于模 n 的加法作成 n 阶加法循环群，关于模 n 的加法与乘法作成环.

一次同余方程 $ax\equiv b\pmod n$，解 $c,d\in\mathbb{Z}$ 视为相同的 $\Leftrightarrow c\equiv d\pmod n$.

定理 1 设 $(\alpha, n)=1$, 则 $ax\equiv b(\mathrm{mod}\, n)$ 有唯一解.

证明 由 $(\alpha, n)=1$ 用辗转相除法求得整数 u, v 使得 $ua+vn=1$, 于是 $bua+bvn=b\Rightarrow a(bu)\equiv b(\mathrm{mod}\, n)$, 故 $x=bu$ 是一个解.

如果 y 也是解, 则 $ax\equiv b(\mathrm{mod}\, n), ay\equiv b(\mathrm{mod}\, n)\Rightarrow ax\equiv ay(\mathrm{mod}\, n)$, 由 $(\alpha, n)=1$ 知 $x\equiv y(\mathrm{mod}\, n)$.■

定理 2 (孙子定理, 中国剩余定理) 设 $a_i\in\mathbb{Z}, n_i\,(1\le i\le r)$ 两两互素, 则 $x\equiv a_i(\mathrm{mod}\, n_i)(1\le i\le r)$ 有唯一解.

4. 欧拉函数和欧拉-费马定理

欧拉函数 $\varphi(n)$ 定义为整数 0, 1, 2, ..., $n-1$ 中与 n 互素整数的个数.

例 1.(1) $\varphi(7)=6, \varphi(7^2)=49-7=7\cdot 6, \varphi(7^3)=7^3-7^2=7^2\cdot 6$;

(2) $\varphi(7\cdot 5)=7\cdot 5-7-5+1=(7-1)(5-1)$.

欧拉函数的性质: (1) $\varphi(p^m)=p^m\left(1-\frac{1}{p}\right)=p^{m-1}(p-1)$, 其中 p 为素数, m 为正整数.

(2) 整数 m, n 互素 $\Rightarrow\varphi(mn)=\varphi(m)\varphi(n)$.

(3) 正整数 n 的标准分解式为 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}\Rightarrow\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)$.

证明 (2) 考虑映射 $\sigma:\{0,1,2,\cdots,mn-1\}\to\{0,1,2,\cdots,m-1\}\times\{0,1,2,\cdots,n-1\}$, $x\mapsto(x\,\mathrm{mod}\, m, x\,\mathrm{mod}\, n)$, 由中国剩余定理知其为单射, 再比较元素个数知其亦为满射. 不仅如此,

$$(x, mn)=1\Rightarrow(x\,\mathrm{mod}\, m, m)=1=(x\,\mathrm{mod}\, n, n),$$

反之, 若 $(x\,\mathrm{mod}\, m, m)=1=(x\,\mathrm{mod}\, n, n)\Rightarrow(x, m)=1=(x, n)$, 再由 m, n 互素知 $(x, mn)=1$, 这表明如上映射也可以视为是从 A_{mn} 到 $A_m\times A_n$ 的双射, 这里 $A_m=\{x\in\{0,1,2,\cdots,m-1\}\,|\,(x, m)=1\}$, 比较元素个数即得.

(3) 反复利用(2), 或者利用容斥原理与(1).

欧拉-费马定理 (1) $a\in\mathbb{Z}, n\in\mathbb{Z}_{>0}, (a, n)=1\Rightarrow a^{\varphi(n)}\equiv 1(\mathrm{mod}\, n)$;

(2) 特别地, $a\in\mathbb{Z}, p$ 是素数 $\Rightarrow a^p\equiv a(\mathrm{mod}\, p)$.

证明概要 (1) 模 n 的剩余类中, 与 n 互素的剩余类有 $\varphi(n)$ 个, 记其构成的集合为 H_n, 规定 H_n 中的乘法为模 n 乘, 验证其对乘法运算封闭, 结合律与幺元, 于是 H_n 构成一个 $\varphi(n)$ 阶群, 此时元 $\bar{a}\in H_n$ 的阶整除群 H_n 的阶 $\varphi(n)$, 故有 $\overline{a^{\varphi(n)}}=\bar{a}^{\varphi(n)}=\bar{1}$, 即 $a^{\varphi(n)}\equiv 1(\mathrm{mod}\, n)$.

(2) 令 $n=p$, 由 $\varphi(p)=p-1$ 知, 若 $(p, a)=1$, 由(1)有 $a^{p-1}\equiv 1(\mathrm{mod}\, p)$, 于是 $a^p\equiv a(\mathrm{mod}\, p)$;

若 $(p,a)\neq 1$，由 p 是素数知 $p\mid a$，此时 $p\mid a^p$，于是 $a^p\equiv 0\equiv a(\mathrm{mod}\,p)$.■

0.4 偏序集与 Zorn 引理

1. 偏序集

非空集合 S 上的**偏序**"<": 自反性、反对称性与传递性.

全序: 任意两个元均可比较的偏序集;

链: 偏序集 S 的一个全序子集

例 1. (1) 非空集合的幂集关于集合的包含关系作成偏序集，但一般来说不是全序集;

(2) 自然数集关于数的大小关系作成全序集;

(3) 自然数系关于整数的整除关系作成偏序集.

偏序集 S 的极小元，极大元. 未必存在，也可能存在多个.

下界，上界.

最小元，最大元，未必存在，但如果存在则一定唯一.

2. 选择公理和良序原理

策梅洛(Zermelo)1904 年提出的选择公理 设 $T=\{A_\alpha\}_{\alpha\in I}$ 是由一些非空集合 $A_\alpha(\alpha\in I)$ 构成的非空集，则存在一个 T 上的函数 f 使得 $f(A_\alpha)\in A_\alpha$，f 称为 T 上的一个选择函数.

选择函数的存在作为公理提出来意味着存在某种规律使得可以从每个 $A_\alpha(\alpha\in I)$ 中同时地挑出一个元素. 选择公理是不能证明的.

良序集: 每个非空子集都有最小元的偏序集. 具有良序的集合称为良序集.

良序集都是全序集，自然数集合按通常的小于等于作成良序集.

Zermelo 应用选择公理证明了著名的**良序原理**: 每个集合都存在一个良序.

反之，从良序原理也可推出选择公理.

良序原理的重要性: 数学归纳法原理可以推广到良序集上去，从而得到超限归纳法原理.

设 S 是良序集，对任一 $a\in S$，规定 $S(a):=\{x\in S\mid x<a\}$，称为 a 的**前段**. 规定最小元的前段为空集.

超限归纳法原理 设 S 是一个良序集，$A\subseteq S$. 如果对任一 S 中的元 a，都可以由 $S(a)\subseteq A$ 证得 $a\in A$，则 $A=S$.

3. Zorn 引理

下面的描述的 Zorn 引理与前面讨论的选择公理与良序定理都是等价的, 选择公理作为公理是不能证明的, 但是可以证明如上原理或公理是等价的, 其证明属于集合论范畴, 我们在此不予以证明.在抽象代数课程中, 选择公理与 Zorn 引理使用起来更为便捷一些.

Zorn 引理 如果偏序集 S 的每个链都有上界, 则 S 有一个极大元.

应用 证明数域上任一线性空间基的存在性.

定义 设 V 是数域 F 上的一个线性空间(以后简称 V 为 $F-$ 空间), A 是 V 的一个子集.

(1) 如果 A 的任一有限子集均线性无关, 称**子集 A 线性无关**. 如果存在 A 的某个有限子集线性相关, 称**子集 A 线性相关**.

(2) 如果 V 中任一元都可以写成 A 中有限多个元的 $F-$ 线性组合, 称 **A 生成 V**, 即 $\forall v\in V$, 存在有限多个元 $\alpha_1,\cdots,\alpha_n\in A$ 及 $c_1,\cdots,c_n\in F$ 使得 $v=c_1\alpha_1+\cdots+c_n\alpha_n$.

(3) 如果 A 线性无关且生成 V, 则称 A 是 **V 的一组基**.

定理 设 V 是一个 $F-$ 空间, 则 V 有一组基.

证明 V 的所有线性无关子集构成的集合 S 按包含关系作成偏序集. 设 $T=\{A_\alpha\mid\alpha\in I\}$ 是 S 的一个链,下面证明其并集 $A=\bigcup_{\alpha\in I}A_\alpha$ 线性无关:

设 $A_1=\{a_1,\cdots,a_r\}$ 是 A 的一个有限子集, 于是每一个 a_i 必包含在某一个 $A_{\alpha_i}\ (\alpha_i\in I)$ 内, 由 T 是链知 $A_{\alpha_1},\cdots,A_{\alpha_r}$ 包含在某一个 $A_\alpha\ (\alpha\in I)$ 中, 于是 $A_1\subseteq A_\alpha$ 线性无关(线性无关集 A_α 的子集 A_1 也线性无关). 由线性无关集的定义(1)知 A 线性无关, 于是 $A\in S$. 这表明 S 满足 Zorn 引理的条件, 于是由 Zorn 引理知 S 有一个极大元 M.

下证 M 生成 V.

反证. 设 $\beta\in V$ 不能表成 M 中任一有限子集的线性组合, 令 $B=M\bigcup\{\beta\}$, 则 B 线性无关:

任取 B 的一个有限向量组 B_1.

如果 B_1 不包含 β, 则 B_1 也是 M 的一个有限向量组, 由 M 线性无关知其子集 B_1 也线性无关.

若 B_1 包含 β, 不妨设 $B_1=\{\alpha_1,\cdots,\alpha_r,\beta\}$, 其中 $\{\alpha_1,\cdots,\alpha_r\}\subseteq M$ 线性无关, 若 B_1 线性相关, 则 $\beta\in V$ 是 M 的有限子集 $\{\alpha_1,\cdots,\alpha_r\}$ 的线性组合, 矛盾!

所以 B_1 线性无关.

由于 B 的任一有限向量组 B_1 均线性无关, 所以 B 线性无关.

于是 $B\in S$, 但显然 $B=M\bigcup\{\beta\}$ 真包含 M, 这与 M 是 S 的极大元矛盾!

又由 M 的构造过程知 ***M* 线性无关**, 所以 M 是 V 的一组基.

例 2. 实数域可视为有理数域上的无穷维线性空间, 虽然基存在, 但是要写出一组基出来是很困难的.

习题

1. 设 p 是素数, 利用 $\mathbb{Z}_p^* \coloneqq \mathbb{Z}_p - \{\overline{0}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ 是一个 $p-1$ 阶循环群这一事实, 证明 Wilson 定理:

$$(p-1)! \equiv -1 \pmod{p}.$$

2. 用反证法证明有无穷多个模 6 余 1 的素数.

3. 解同余方程: (1) $29x \equiv 27 \pmod{31}$; (2) $30x \equiv 9 \pmod{33}$.

4. 解同余方程组 $\begin{cases} x \equiv 3 \pmod{5}, \\ 2x \equiv 4 \pmod{6}, \\ 3x \equiv 1 \pmod{7}. \end{cases}$

5. 将正整数 n 写成十进制 $n = a_1 a_2 \cdots a_r, 1 \le a_1 \le 9, 0 \le a_i \le 9, i = 2, 3, \cdots, r$, 证明:

(1) $n \equiv 0 \pmod{9} \Leftrightarrow \sum\limits_{1 \le i \le r} a_i \equiv 0 \pmod{9}$; (2) $n \equiv 0 \pmod{11} \Leftrightarrow \sum\limits_{1 \le i \le r} (-1)^i a_i \equiv 0 \pmod{11}$.

请利用 $13 \mid 1001$ 这一事实给出整数是否整除 13 的简单判别法吗, 请说明判别法的原理.

第一章 群论基础

1.1 群的直积

参阅韩士安教材 2.4 节，《代数学引论》2.8 节

1. 两个群的外直积与内直积

外直积：设 G_1, G_2 都是群，则 $G_1 \times G_2 = \{(a_1, a_2) | a_1 \in G_1, a_2 \in G_2\}$ 对如下按分量进行的乘法成群：

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2), \forall (a_1, a_2), (b_1, b_2) \in G_1 \times G_2,$$

称为 G_1, G_2 的**外直积**，该群仍记为 $G_1 \times G_2$.

单位元： $(1_1, 1_2)$，其中 $1_1, 1_2$ 分别是 G_1, G_2 的单位元；

逆元： $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$，按分量在每个群里边分别求逆；

元素的阶： $o(a_1, a_2) = [o(a_1), o(a_2)]$ 是分量阶的最小公倍数，当某分量的阶无穷时，元素的阶也无穷.

如果 G_1, G_2 都是交换群，也记为 $G_1 \oplus G_2$，称 $G_1 \oplus G_2$ 为 G_1, G_2 的**外直和**.

利用外直积与集合笛卡尔积的定义直接验证易知下面的定理成立，请读者自己完成证明.

定理 1(外直积的性质). 设有群的外直积 $G = G_1 \times G_2$，$H_1 = \{(g_1, 1_2) | g_1 \in G_1\}, H_2 = \{(1_1, g_2) | g_2 \in G_2\}$，则

(1) G 有限 $\Leftrightarrow G_1, G_2$ 均有限，此时 $|G| = |G_1||G_2|$； 笛卡尔乘积的定义

(2) G 交换 $\Leftrightarrow G_1, G_2$ 均交换； 直接验证

(3) $G_1 \times G_2 \cong G_2 \times G_1$； 验证 $\sigma: (g_1, g_2) \mapsto (g_2, g_1)$ 是双射保持运算

(4) $H_i \lhd G$，$H_i \cong G_i, i = 1, 2$； 直接验证

(5) $G = H_1 H_2$，且 $h_1 h_2 = h_2 h_1, \forall h_1 \in H_1, h_2 \in H_2$； 直接验证

(6) $H_1 \cap H_2 = 1$，其中 $1 = (1_1, 1_2)$ 是 G 的乘法单位元； 显然

(7) 每一个 $g \in G$ 可唯一写成 $g = h_1 h_2$ 的形式，其中 $h_1 \in H_1, h_2 \in H_2$. 直接验证

例 2 (1) $\mathbb{Z}_2 \times \mathbb{Z}_2$ (也写成 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$)是 4 阶交换群，非单位元的阶都是 2，与 Klein 四元群同构，与 S_4 的如下子群同构：$H = \{(1), (12), (34), (12)(34)\}$；

(2) $\mathbb{Z}_3\times\mathbb{Z}_7$(也写成$\mathbb{Z}_3\oplus\mathbb{Z}_7$)是 21 阶交换群, $(\bar{1},\bar{1})$的阶为 21, 故$\mathbb{Z}_3\times\mathbb{Z}_7$为 21 阶循环群.

更一般地, 如果正整数 m 与 n 互素, 则$\mathbb{Z}_m\oplus\mathbb{Z}_n$是 mn 阶循环群, $(\bar{1},\bar{1})$是其生成元.

定理 1 表明, 如果有群的外直积$G=G_1\times G_2$, 那么由外直积的性质(4)(5)(6)知其子群H_1,H_2满足

(1) $H_1\lhd G,H_2\lhd G$; (2) $G=H_1H_2$; (3) $H_1\cap H_2=1$;

这可以类比于一个$F-$空间 V 是其子空间直和的两个要求: $V=V_1+V_2$且$V_1\cap V_2=O$. 基于此, 我们给出群的内直积的概念.

内直积: 如果群 G 的子群H_1,H_2满足

(1) $H_1\lhd G,H_2\lhd G$; (2) $G=H_1H_2$; (3) $H_1\cap H_2=1$;

就称 G 是G_1,G_2的**内直积**, 记为$G=G_1\dot{\times}G_2$.

例 3 设有群的外直积$G=G_1\times G_2$, $H_1=\{(h_1,1_2)|h_1\in G_1\},H_2=\{(1_1,h_2)|h_2\in G_2\}$, 那么由外直积的性质(4)(5)(6)知$H_1,H_2$满足内直积的 3 个定义条件, 故$G=H_1\dot{\times}H_2$.

类似于向量空间的直和, 内直积的定义条件(2)(3)也可以替换为一般元素表示为乘积的唯一性, 或单位元表示为乘积的唯一性, 或群阶与子群阶的关系, 即我们有下面的内直积刻画定理.

定理 4(内直积的刻画) 设G_1,G_2是群 G 的正规子群, 则如下条件彼此等价:

(1) G 是G_1,G_2的内直积$G=G_1\dot{\times}G_2$, 即$G=G_1G_2$且$G_1\cap G_2=1$;

(2) 每一个$g\in G$可唯一写成$g=g_1g_2$的形式, 其中$g_1\in G_1,g_2\in G_2$;

(3) $G=G_1G_2$且 G 的单位元 1 可唯一写成G_1,G_2中元的乘积, 即

$$g_1\in G_1,g_2\in G_2\text{ 使得 }1=g_1g_2\text{, 则 }g_1=g_2=1;$$

(4) $G=G_1G_2$且$|G|=|G_1|\bullet|G_2|$;

(5) $G_1\cap G_2=1$且$|G|=|G_1|\bullet|G_2|$.

证明 $(1)\Rightarrow(2)$ 任取$g\in G$, 由$G=G_1\dot{\times}G_2$知存在$g_1\in G_1,g_2\in G_2$使得$g=g_1g_2$. 下证唯一性:

设$h_1\in G_1,h_2\in G_2$使得$g=h_1h_2$, 则$g_1g_2=h_1h_2$, 于是$h_1^{-1}g_1=h_2g_2^{-1}\in G_1\cap G_2=1$, 所以$h_1^{-1}g_1=h_2g_2^{-1}=1$, 由此立得$g_1=h_1,g_2=h_2$.

$(2)\Rightarrow(3)$ 显然.

$(3)\Rightarrow(1)$ 任取 $a\in G_1\cap G_2$，则 $1=1\cdot 1=a\cdot a^{-1}$，由条件(3)知元 $a=1$，所以 $G_1\cap G_2=1$，故 $G=G_1\dot{\times}G_2$.■

引理 5 设群 G 的两个正规子群 G_1,G_2 满足 $G_1\cap G_2=1$，则 $xy=yx,\forall x\in G_1,y\in G_2$.

特别地，如果 $G=G_1\dot{\times}G_2$，则 $xy=yx,\forall x\in G_1,y\in G_2$.

证明 由 $G_1\lhd G$ 知 $xyx^{-1}y^{-1}=x\left(yx^{-1}y^{-1}\right)\in G_1$，由 $G_2\lhd G$ 知 $xyx^{-1}y^{-1}=\left(xyx^{-1}\right)y^{-1}\in G_2$，所以 $xyx^{-1}y^{-1}\in G_1\cap G_2=1$，于是 $xy=yx$.■

下面的定理给出了内直积与外直积的关系.

定理 6 (1) 设有群的外直积 $G=G_1\times G_2$，$H_1=\left\{(g_1,1_2)\middle|g_1\in G_1\right\},H_2=\left\{(1_1,g_2)\middle|g_2\in G_2\right\}$，则 $G=H_1\dot{\times}H_2$；

(2) 设 $G=H_1\dot{\times}H_2$ 是内直积，则 $G\cong H_1\times H_2$.

证明 (1) 由外直积的性质(4)(5)(6)即得.

也可由外直积的性质(4)知 H_1,H_2 都是 G 的正规子群，由(7)知每一个 $g\in G$ 可唯一写成 $g=g_1g_2$ 的形式，其中 $g_1\in H_1,g_2\in H_2$，由定理 2 知 G 是 H_1,H_2 的内直积.

(2) 由内直积的刻画定理 2(3)知，任一 $g\in G$ 可唯一写成 $g=h_1h_2$，其中 $h_1\in H_1,h_2\in H_2$，规定映射

$$\sigma:G\to H_1\times H_2,g=h_1h_2\mapsto(h_1,h_2),$$

由分解的唯一性知映射良定.

显然 σ 单. 任取 $(h_1,h_2)\in H_1\times H_2$，由映射定义知 $\sigma(h_1h_2)=(h_1,h_2)$，于是映射 σ 满.

映射保持乘法运算：由 $G=H_1\dot{\times}H_2$ 知，任取 $x=x_1x_2,y=y_1y_2\in G$，其中 $x_1,y_1\in H_1,x_2,y_2\in H_2$，由引理 3 知 H_1 与 H_2 中元可换，故

$$\sigma(xy)=\sigma(x_1x_2y_1y_2)=\sigma(x_1y_1x_2y_2)=\sigma((x_1y_1)(x_2y_2))=(x_1y_1,x_2y_2)=(x_1,x_2)(y_1,y_2)=\sigma(x)\sigma(y).$$

综上，σ 是同构，故 $G\cong H_1\times H_2$.■

2. 多个群的外直积与内直积

我们先将两个群的外直积推广到 s 个群的情形.

设 $G_1,\ldots,G_s$ 都是群，则 $G_1\times\cdots\times G_s=\left\{(a_1,\ldots,a_s)\middle|a_i\in G_i,1\le i\le s\right\}$ 对按分量进行的乘法成群：

$$(a_1,\ldots,a_s)(b_1,\ldots,b_s)=(a_1b_1,\ldots,a_sb_s),\forall(a_1,\ldots,a_s),(b_1,\ldots,b_s)\in G_1\times\cdots\times G_s,$$

称为 $G_1,\ldots,G_s$ 的**外直积**，该群仍记为 $G_1\times\cdots\times G_s$.

单位元： $(1_1,\cdots,1_s)$，其中 1_i 是 G_i 的单位元；

逆元： $(a_1,\cdots,a_s)^{-1}=(a_1^{-1},\cdots,a_s^{-1})$，按分量在每个群里边分别求逆；

元素的阶： $o((a_1,\cdots,a_s))=[o(a_1),\cdots,o(a_s)]$ 是各分量阶的最小公倍数，当某分量的阶无穷时，元素的阶也无穷.

如果 $G_1,\cdots,G_s$ 都是交换群，外直积也记为 $G_1\oplus\cdots\oplus G_s$，称其为群 $G_1,\cdots,G_s$ 的**外直和**.

定理 7(外直积的性质) 设有群的外直积 $G=G_1\times\cdots\times G_s$，令 $H_i=\{(1_1,\ldots,1_{i-1},h_i,1_{i+1},\ldots,1_s)\mid h_i\in G_i\}$ 是第 j $(j\neq i)$ 个分量为 $1_j\in G_j$ 的 G 中元所成子群，则

(1) G 有限 $\Leftrightarrow G_1,\cdots,G_s$ 均有限，此时 $|G|=|G_1|\bullet\cdots\bullet|G_s|$；

(2) G 交换 $\Leftrightarrow G_1,\cdots,G_s$ 均交换；

(3) 如果 π 是集合 $\{1,2,\ldots,n\}$ 上的一个置换，则 $G_1\times\cdots\times G_s\cong G_{\pi(1)}\times\cdots\times G_{\pi(s)}$.

(4) $H_i\lhd G$，$H_i\cong G_i,1\le i\le s$；

(5) $G=H_1H_2\cdots H_s$，$xy=yx,\forall x\in H_i,y\in H_j,\forall i\neq j$；

(6) $H_i\bigcap(H_1\cdots H_{i-1}H_{i+1}\cdots H_s)=1,1\le i\le s$；

(7) 每一个 $g\in G$ 可唯一写成 $g=g_1g_2\cdots g_s$ 的形式，其中 $g_i\in H_i,1\le i\le s$.

如上定理直接验证即可，请读者自己给出证明.

我们再将两个正规子群的内直积推广到多个正规子群的情形.

如果群 G 的子群 $H_1,\cdots,H_s$ 满足

(1) $H_i\lhd G,1\le i\le s$； (2) $G=H_1\bullet\cdots\bullet H_s$； (2) $H_i\bigcap H_1\cdots H_{i-1}H_{i+1}\cdots H_s=1$；

则称 G 是 $H_1,\cdots,H_s$ 的**内直积**，记为 $G=H_1\dot\times\cdots\dot\times H_s$. 如果 $G_1,\ldots,G_s$ 都是交换群，也记为 $G_1\oplus\cdots\oplus G_s$，称其为 $H_1,\cdots,H_s$ 的**外直和**.

定理 3 刻画了何时一个群是两个正规子群的内直和，如下定理对其进行了推广，刻画了何时一个群是

多个正规子群的内直和.

定理 8(内直积的刻画) 设群 G 的正规子群 $G_1,\cdots,G_s$ 使得 $G=G_1G_2\cdots G_s$，则如下条件彼此等价:

(1) $G=G_1\dot{\times}\cdots\dot{\times}G_s$，即 $G_i\cap\left(G_1\cdots G_{i-1}G_{i+1}\cdots G_s\right)=1,\forall i$;

(2) 每一个 $g\in G$ 可唯一写成 $g=g_1g_2\cdots g_s$ 的形式，其中 $g_i\in G_i,1\le i\le s$;

(3) 单位元 $1\in G$ 可唯一写成 $G_1,\cdots,G_s$ 中元的乘积，即

$$1=g_1\cdots g_s,\ \text{其中}\ g_i\in G_i,1\le i\le s\Rightarrow 1=g_1=\cdots=g_s.$$

证明 $(1)\Rightarrow(2)$ $i\ne j$ 时 G_i 与 G_j 中的元可换: $G_i\cap G_j\subseteq G_i\cap\left(G_1\cdots G_{i-1}G_{i+1}\cdots G_s\right)=1$，由引理 3 知

$$xy=yx,\forall x\in G_i,y\in G_j.$$

如果 $g_i,h_i\in G_i\left(1\le i\le s\right)$ 使得 $g=g_1g_2\cdots g_s=h_1h_2\cdots h_s$，则由 $i\ne j$ 时 G_i 与 G_j 中的元可换知

$$h_1^{-1}g_1=h_2\cdots h_sg_s^{-1}\cdots g_2^{-1}=\left(h_2g_2^{-1}\right)\cdots\left(h_sg_s^{-1}\right)\in G_1\cap\left(G_2\cdots G_s\right)=1,$$

所以 $h_1^{-1}g_1=\left(h_2g_2^{-1}\right)\cdots\left(h_sg_s^{-1}\right)=1$，故 $g_1=h_1$ 且 $\left(h_2g_2^{-1}\right)\cdots\left(h_sg_s^{-1}\right)=1$. 此时

$$\left(h_2g_2^{-1}\right)=\left[\left(h_3g_3^{-1}\right)\cdots\left(h_sg_s^{-1}\right)\right]^{-1}=\left(g_sh_s^{-1}\right)\cdots\left(g_3h_3^{-1}\right)=\left(g_3h_3^{-1}\right)\cdots\left(g_sh_s^{-1}\right)\in G_2\cap\left(G_1G_3\cdots G_s\right)=1,$$

所以 $h_2g_2^{-1}=\left(g_3h_3^{-1}\right)\cdots\left(g_sh_s^{-1}\right)=1$，故 $g_2=h_2$ 且 $\left(g_3h_3^{-1}\right)\cdots\left(g_sh_s^{-1}\right)=1$. 如此继续，最后得到 $g_i=h_i,1\le i\le s$.

$(2)\Rightarrow(3)$ 显然.

$(3)\Rightarrow(1)$ 任取 $a\in G_i\cap\left(G_1\cdots G_{i-1}G_{i+1}\cdots G_s\right)$，不妨设 $a=a_1\cdots a_{i-1}a_{i+1}\cdots a_s$，其中 $a_j\in G_j$，则

$$1=\left(a_1\cdots a_{i-1}\right)^{-1}a\left(a_{i+1}\cdots a_s\right)^{-1},$$

由 $G_1,\cdots,G_s$ 都是群 G 的正规子群知 $G_1\cdots G_{i-1}\lhd G,G_{i+1}\cdots G_s\lhd G$，于是

$$\left(a_1\cdots a_{i-1}\right)^{-1}\in G_1\cdots G_{i-1},a\in G_i,\left(a_{i+1}\cdots a_s\right)^{-1}\in G_{i+1}\cdots G_s,$$

由单位元的分解唯一知 $a=1$，所以 $G_i\cap\left(G_1\cdots G_{i-1}G_{i+1}\cdots G_s\right)=1,\forall i$，即(1)成立.■

完全类似于定理 4，如下定理 7 刻画了一般情形下外直积与内直积的关系，其证明完全类似于定理 4，请读者完成证明.

定理 9 (1) 设群的外直积 $G=G_1\times\cdots\times G_s$，$H_i=\left\{\left(1_1,\ldots,1_{i-1},h_i,1_{i+1},\ldots,1_s\right)\middle|h_i\in G_i\right\}$ 是第 j 个分量为 $1\in G_j$ 的 G 中元所成子群，则 $G=H_1\dot{\times}\cdots\dot{\times}H_s$;

(2) 设 $G=H_1\dot{\times}\cdots\dot{\times}H_s$ 是内直积, 则 $G\cong H_1\times\cdots\times H_s$.

约定 在后续节次的讨论中, 我们不再严格区分外直接与内直积, 而是将它们统称为直积, 统一采用记号 $G=G_1\times\cdots\times G_s$, 如果涉及的群是加法群, 也采用记号 $G=G_1\oplus\cdots\oplus G_s$, 请读者根据上下文来判断是内直积或者外直积.

例 10 $\mathbb{Z}_{12}$ 是正规子群 $\langle\bar{3}\rangle=\{\bar{0},\bar{3},\bar{6},\bar{9}\},\langle\bar{4}\rangle=\{\bar{0},\bar{4},\bar{8}\}$ 的内直积, 注意到 $\langle\bar{3}\rangle\cong\mathbb{Z}_4,\langle\bar{4}\rangle\cong\mathbb{Z}_3$, 故

$$\mathbb{Z}_{12}\cong\mathbb{Z}_4\times\mathbb{Z}_3\cong\mathbb{Z}_3\times\mathbb{Z}_4.$$

但是 $\mathbb{Z}_{12}$ 与 $\mathbb{Z}_2\times\mathbb{Z}_6$ 不同构: 前者有 12 阶元, 后者只有 1, 2, 3, 6 阶元.

注记 上例中 $\mathbb{Z}_3,\mathbb{Z}_4,\mathbb{Z}_2,\mathbb{Z}_6$ 并不是 $\mathbb{Z}_{12}$ 的正规子群, 所以这里的直积都是外直积.

习题 1.1

1. (1) 设 H,K 是群 G 的有限子群, 证明: $|HK|=\dfrac{|H||K|}{|H\cap K|}$.

(2) 利用(1)证明定理 2 中的条件(4)(5)与(1)等价.

提示: 构造从 H 在 HK 中的左陪集所成集到 $H\cap K$ 在 K 中的左陪集所成集之间的一个双射.

2. 设 H,K 是有限群 G 的子群, 则

(1) $\big[\langle H,K\rangle:H\big]\geq\big[K:H\cap K\big]$;　　(2) $\big[G:H\big]\big[G:K\big]\geq\big[G:H\cap K\big]$;

(3) 若 $\big[G:H\big],\big[G:K\big]$ 互素, 则 $\big[G:H\big]\big[G:K\big]=\big[G:H\cap K\big]$, 且 $G=HK$.

3. 求 $\mathbb{Z}_6\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{12}$ 中 3 阶元的个数.

4. 设 H 与 K 都是群, 证明:

(1) $\mathbf{Z}(H\times K)=\mathbf{Z}(H)\times\mathbf{Z}(K)$, 其中 $\mathbf{Z}(G)=\{g\in G|gx=xg\}$ 表示群 G 的中心.

(2) H 的正规子群也是群的直积 $H\times K$ 的正规子群.

5. 设 G 是群,记 $\mathrm{Aut}\,G:=\{\sigma|\sigma$ 是群 G 的自同构$\}$, 即

$$\sigma\in\mathrm{Aut}\,G\Leftrightarrow\sigma\text{ 是 }G\text{ 上的双射且}\sigma(ab)=\sigma(a)\sigma(b),\forall a,b\in G.$$

证明: (1) $\mathrm{Aut}\,G$ 关于映射的合成: $\sigma\tau(g)=\tau(\sigma(g)),\forall g\in G,\sigma,\tau\in\mathrm{Aut}\,G$ 做成群, 称为群 G 的**自同构群**.

(2) 证明群 G 的任一自同构均保持单位元, 逆元与元素的阶.

6. 设循环群 $G=\langle a\rangle$ 是循环群. 证明:

(1) 若 $\sigma \in \operatorname{Aut} G$，则 $G=\langle \sigma(a) \rangle$；

(2) $|\operatorname{Aut} G|=\begin{cases}2, & \text{若 } G \text{ 是无限循环群,} \\ \varphi(n), & \text{若 } G \text{ 是 } n \text{ 阶循环群}\end{cases}$，特别地 $\operatorname{Aut} G$ 是一个交换群;

(3) 证明: $\operatorname{Aut} \mathbb{Z}_8$ 与 Klein 四元群同构.

7. 设 G 是群，$a, g \in G$，称 gag^{-1} 为 a 在 g 之下的**共轭**. 类似地若 H 是 G 的子群，规定 H 在 g 之下的**共轭**为 $gHg^{-1}=\left\{ghg^{-1} \middle| h \in H\right\}$，显然 gHg^{-1} 是 G 的子群. 若 $a, g, h \in G, H \leq G$，证明

(1) $o\left(gag^{-1}\right)=o(a),\left|gHg^{-1}\right|=|H|$.

(2) $H \lhd G \Leftrightarrow xhx^{-1} \in H, \forall x \in G, h \in H$.

8. **内自同构与内自同构群** 设 G 是群，对任一 $g \in G$，规定映射

$$\sigma_g : G \to G, x \mapsto gxg^{-1}, \forall x \in G,$$

证明: (1) σ_g 是 G 的一个自同构，称为由元素 g 导出的群 G 的**内自同构**.

(2) 记群 G 的全体内自同构所成集为 $\operatorname{Inn} G$，即 $\operatorname{Inn} G \coloneqq \left\{\sigma_g \in \operatorname{Aut} G \middle| g \in G\right\}$，证明: $\operatorname{Inn} G \lhd \operatorname{Aut} G$. 称 $\operatorname{Inn} G$ 是群 G 的**内自同构群**.

(3) 证明: $\operatorname{Inn} G \cong G/\mathbf{Z}(G)$.

9. 称群 G 的子群 N 为 G 的**特征子群**，如果 $\varphi(N) \leq N, \forall \varphi \in \operatorname{Aut}(G)$，记为 $N \operatorname{char} G$. 此时正规子群也可以定义为: 称群 G 的子群 N 为 G 的**正规子群**，如果满足 $\varphi(N) \leq N, \forall \varphi \in \operatorname{Inn}(G)$. 证明:

(1) $N \operatorname{char} G \Leftrightarrow \varphi(N)=N, \forall \varphi \in \operatorname{Aut}(G)$;

(2) $K \operatorname{char} N, N \lhd G \Rightarrow K \lhd G$;

(3) $K \operatorname{char} N, N \operatorname{char} G \Rightarrow K \operatorname{char} G$;

(4) 请针对二面体群 D_8，说明存在 4 阶子群 $N \lhd D_8$，2 阶子群 $K \lhd N$，但是 $K \lhd D_8$ 不成立，即正规子群没有传递关系.

1.2 群的系列同构定理与对应定理

当我们考虑从一个数学对象(比如群)到另一个同一类型数学对象的映射时，我们通常更关注那些“保持对象结构”的映射. 如果两个群之间的映射 $\varphi: G \to H$ 保持乘法运算，即 $\varphi(xy)=\varphi(x)\varphi(y), \forall x, y \in G$，就称 φ 是从群 G 到群 H 的一个**群同态**. 进而，如果群同态 φ 是单射、满射或双射，则称 φ 为**单同态**、**满同态**

或**同构**.

如果 $\varphi: G \to H$ 是单同态, 我们可以将 G 等同于其在 H 中的像 $\varphi(G)$, 即, 将 G 视为 H 的一个子群, 也称 G 经由 φ 嵌入 H.

设 N 是群 G 的正规子群, 定义 $\pi: G \to G/N$ 为 $\pi(g) := gN, \forall g \in G$, 则由 N 正规知

$$\pi(gh) = ghN = gN \cdot hN = \pi(g)\pi(h), \forall g, h \in G,$$

即 π 是群同态, 称为 G 到 G/N 的**自然(Canonical)同态**, 显然 π 是满同态.

同构定理 A 也称为同态基本定理.

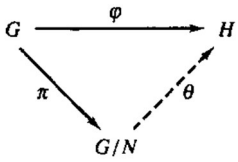
同构定理 A 设 $\varphi: G \to H$ 是群同态, 则

(1) 同态核 $\ker\varphi = \{g \in G \mid \varphi(g) = 1\}$ 是 G 的正规子群;

(2) 同态像 $\mathrm{Im}\varphi = \{\varphi(g) \mid g \in G\}$ 是 H 的子群;

(3) $G/\ker\varphi \cong \mathrm{Im}\varphi$.

(3) 存在唯一的同构 $\theta: G/\ker\varphi \to \mathrm{Im}\varphi$ 使得 $\theta\pi = \varphi$, 即如右图表是交换的.



特别地, 若 φ 是满的群同态, 则 $G/\ker\varphi \cong H$.

证明 (1)(2)直接验证即可.

(3) 如果群同构 $\theta: G/\ker\varphi \to \mathrm{Im}\varphi$ 使得 $\theta\pi = \varphi$, 则对任一 $g \in G$, 有

$$\varphi(g) = (\theta\pi)(g) = \theta(\pi(g)) = \theta(g\ker\varphi),$$

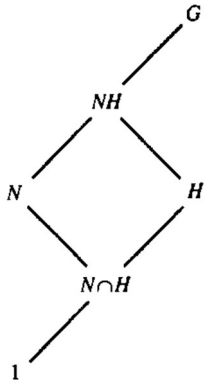
即必须规定 $\theta(g\ker\varphi) := \varphi(g)$, 这就表明了 θ 的唯一性. 再直接验证映射

$$\theta: G/\ker\varphi \to \mathrm{Im}\varphi, \theta(g\ker\varphi) := \varphi(g), \forall g\ker\varphi \in G/\ker\varphi.$$

良定、单、满且保持乘法, 即 θ 确实是同构, 这也表明了同构 θ 的存在性.■

同构定理 B 设 G 是群, $H \le G, N \lhd G$. 则

(1) $N \lhd HN \le G$; (2) $H \cap N \lhd S$; (3) $HN/N \cong H/(H \cap N)$.



如上也称为同构定理、**钻石定理**或平行四边形定理.

证明 (1)(2)直接验证即可.

(3) 规定映射 $\tau: H \to HN/N, h \mapsto hN, \forall h \in H$, 直接验证 τ 是满同态, 再证明 $\ker\tau = H \cap N$, 由同构定理 A 即得.■

例 1. 全体 2 阶可逆复矩阵关于矩阵的乘法构成一个群, 称为**一般 2 级复线性群**, 记为$\mathrm{GL}_2(\mathbb{C})$, 其中行列式为 1 的所有 2 阶复矩构成$\mathrm{GL}_2(\mathbb{C})$的子群, 称为**2 级特殊复线性子群**, 记为$\mathrm{SL}_2(\mathbb{C})$. 规定

$$\mathrm{PGL}_2(\mathbb{C}):=\mathrm{GL}_2(\mathbb{C})/\mathbf{Z}(\mathrm{GL}_2(\mathbb{C})),\quad \mathrm{PSL}_2(\mathbb{C}):=\mathrm{SL}_2(\mathbb{C})/\mathbf{Z}(\mathrm{SL}_2(\mathbb{C})).$$

分别称为**一般射影线性群**与**特殊射影线性群**.

由高等代数知识知道, $\mathrm{GL}_2(\mathbb{C})$的中心恰由 2 阶可逆数量阵构成, 即$\mathbf{Z}(\mathrm{GL}_2(\mathbb{C}))=\{aI_2\mid a\in\mathbb{C}^*\}$, 其中$\mathbb{C}^*$是非零复数构成的乘法群. 其子群$\mathrm{SL}_2(\mathbb{C})$的中心

$$\mathbf{Z}(\mathrm{SL}_2(\mathbb{C}))=\left\{\begin{pmatrix}a&0\\0&a\end{pmatrix}\middle|\,a\in\mathbb{C}^*\text{ 且 }a^2=1\right\}=\{\pm I_2\}=\mathrm{SL}_2(\mathbb{C})\cap\mathbf{Z}(\mathrm{GL}_2(\mathbb{C})),$$

此时$\mathrm{GL}_2(\mathbb{C})=\mathrm{SL}_2(\mathbb{C})\mathbf{Z}(\mathrm{GL}_2(\mathbb{C}))$: 任取$A\in\mathrm{GL}_2(\mathbb{C})$, 设$c:=\sqrt{\det A}\in\mathbb{C}$, 则$A=\sqrt{\det A}I_2\cdot\frac{1}{\sqrt{\det A}}A\in SN$, 即$\mathrm{GL}_2(\mathbb{C})\subseteq\mathrm{SL}_2(\mathbb{C})\mathbf{Z}(\mathrm{GL}_2(\mathbb{C}))$, 反包含关系是显然的.

由同构定理 B 知

$$\mathrm{PGL}_2(\mathbb{C})=\mathrm{GL}_2(\mathbb{C})/\mathbf{Z}(\mathrm{GL}_2(\mathbb{C}))=\mathrm{SL}_2(\mathbb{C})\mathbf{Z}(\mathrm{GL}_2(\mathbb{C}))/\mathbf{Z}(\mathrm{GL}_2(\mathbb{C}))$$

$$\cong\mathrm{SL}_2(\mathbb{C})/(\mathrm{SL}_2(\mathbb{C})\cap\mathbf{Z}(\mathrm{GL}_2(\mathbb{C})))=\mathrm{SL}_2(\mathbb{C})/\mathbf{Z}(\mathrm{SL}_2(\mathbb{C}))=\mathrm{PSL}_2(\mathbb{C}).\blacksquare$$

如果将复数域换为p^n元有限域$\mathbb{F}_{p^n}$, 将 2 阶矩阵换为n阶矩阵, 将相应的群分别记为

$$\mathrm{GL}_n(p^n),\mathrm{SL}_n(p^n),\mathrm{PGL}_n(p^n),\mathrm{PSL}_n(p^n),$$

请读者分别计算这些群的阶.

同构定理 C 设N是群G的正规子群. 则

(1) 若$N\le K\le G$, 则$K/N\le G/N$; 进而, 若$K\lhd G$, 则$K/N\lhd G/N$, 且$(G/N)/(K/N)\cong G/K$;

(2) G/N的子群均形如K/N, 其中K满足$N\le K\le G$; 进而, G/N的正规子群均形如K/N, 其中K满足$N\le K\lhd G$.

证明 (1) 显然$K/N=\{kN\mid k\in K\}\le G/N$. 直接验证知$K\lhd G$时, $K/N\lhd G/N$:

任取$kN\in K/N, gN\in G/N$, 其中$k\in K, g\in G$, 有

$$(gN)kN(gN)^{-1}=gkg^{-1}N\in K/N\left(\because K\lhd G\Rightarrow gkg^{-1}\in K\right).$$

规定映射$\tau:G/N\to G/K, gN\mapsto gK, \forall g\in G$. 验证映射良定, 是群的满同态, 再验证同态核是K/N, 由同构定理 A 即得.

(2) 设 $\overline{H}$ 是 G/N 的子群, 令 $K:=\left\{k\in G\middle| kN\in\overline{H}\right\}$, 由 $nN=N\in\overline{H},\forall n\in N$ 知 $N\subseteq K$.

设 $a,b\in K$, 则 $aN,bN\in\overline{H}$, 于是 $a^{-1}bN=\left(aN\right)^{-1}\left(bN\right)\in\overline{H}$, 故 $a^{-1}b\in K$, 于是 $K\leq G$. 由 K 的定义知 $K/N\leq\overline{H}$. 另一方面, 任取 $gN\in\overline{H}$, 其中 $g\in G$, 由 K 的定义知 $g\in K$, 于是有 $gN\in K/N$, 即 $\overline{H}\leq K/N$. 所以 $\overline{H}=K/N$, 即 G/N 的子群均形如, 其中 K 满足 $N\leq K\leq G$.

反之, 若 K 满足 $N\leq K\leq G$, 由 $N\lhd G$ 知 $N\lhd K$, 于是有商群 K/N, 显然 K/N 是 G/N 的子群.

进而, 如果 $\overline{H}=K/N\lhd G/N$, 其中 $K\leq G$, 下面来证明 $K\lhd G$:

任取 $k\in K,g\in G$, 由 $K/N\lhd G/N$ 知 $gkg^{-1}N=\left(gN\right)\left(kN\right)\left(gN\right)^{-1}\in K/N$, 故 $gkg^{-1}\in K$, $K\lhd G$.■

对应定理(格定理) 设 N 是群 G 的正规子群. 令

$$\mathcal{G}=\left\{A\middle| N\leq A\leq G\right\},\mathcal{N}=\left\{G/N\text{的子群集}\right\},$$

则存在双射 $\phi:\mathcal{G}\to\mathcal{N}$ 使得 $\phi\left(A\right)=A/N,\forall A\in\mathcal{G}$. 或者等价地如下映射是双射:

$$\phi:\mathcal{G}\to\mathcal{N},A\mapsto A/N,\forall A\in\mathcal{G}.$$

进而, 对任一 $A\in\mathcal{G}$, 有 $A\lhd G\Leftrightarrow A/N\lhd G/N\Leftrightarrow\phi\left(A\right)\lhd G/N$.

证明 由同构定理 C 知映射 ϕ 良定且为满射. 下证 ϕ 单. 设 $N\leq H,K\leq G$ 使得 $H/N=K/N$. 任取 $h\in H$, 则 $hN\in H/N=K/N=\left\{kN\middle| k\in K\right\}$, 故存在 $k\in K$ 使得 $h\in kN\subseteq K$, 即 $H\subseteq K$.

同理可证 $K\subseteq H$, 所以 $H=K$. 综上, ϕ 是双射.

再结合同构定理 C 知对任一 $A\in\mathcal{G}$ 有: $A\lhd G\Leftrightarrow A/N\lhd G/N\Leftrightarrow\phi\left(A\right)\lhd G/N$.■

推论 2 设群的满同态 $\pi:G\to H$ 的核 $N=\ker\pi$, 则 $A\leftrightarrow\pi\left(A\right)$ 是 G 的包含 N 的子群与 H 的子群之间的双射, 也是 G 的包含 N 的正规子群与 H 的正规子群之间的双射.

习题 1.2

1. 设 G 是群, 令 $G'=\left\langle aba^{-1}b^{-1}\middle| a,b\in G\right\rangle$ 是群 G 所有形如 $\left[a,b\right]:=aba^{-1}b^{-1}$ 的换位子生成的子群, 称为群 G 的**换位子群**, 或称为 G 的**导群**. 证明:

(1) $G'\lhd G$;

(2) 设 N 是 G 的正规子群, 则 G/N 是 Abel 群 $\Leftrightarrow G'\leq N$;

2. 设 A 是 Abel 群，$\varphi: G \to A$ 是群同态，则 $G' \le \ker\varphi$；

3. 包含导群的子群一定正规，即如果有子群关系 $G' \le H \le G$，则 $H \lhd G$.

4. 设 $\varphi: G \to K$ 是从有限群 G 到群 K 的一个群同态，$H \le G$. 证明:

(1) $\left|\varphi(G):\varphi(H)\right|$ 整除 $\left|G:H\right|$；　　(2) $\left|\varphi(H)\right|$ 整除 $\left|H\right|$.

5. 设 $N \lhd G$，满同态 $\varphi: G \to H$ 满足 $N \cap \ker\varphi = 1$. 设 $x \in N$，证明：$\varphi\left(\mathbf{C}_G(x)\right) = \mathbf{C}_H\left(\varphi(x)\right)$.

6. 设 $H \le G$. 证明 $\mathbf{N}_G(H)/\mathbf{C}_G(H)$ 与 $\mathrm{Aut}(H)$ 的某个子群同构. 该结论称为“N/C 定理”.

7. 设 G 有两个正规子群 M 与 N，证明：$G/(M \cap N)$ 与 $(G/M)\times(G/N)$ 的某个子群同构.

8. 如果群 G 使得 $G/\mathbf{Z}(G)$ 循环，证明 G 是交换群.

1.3 有限交换群的构造定理

约定：本节 G 总是表一个有限群，p 是一个素数.

1. p -元素、p -群与 Sylow p -子群

定义 1 如果元素 $a \in G$ 的阶 $o(a)$ 是素数 p 的方幂，则称 a 为 **$p-$元素**；如果 a 的阶 $o(a)$ 与 p 互素，则称 a 为 **$p'-$元素**. 约定 G 的单位元 1 既是 $p-$元素，也是 $p'-$元素.

如果群 G 的元均为 $p-$元素，称 G 为 **$p-$群**，如果群 G 的元均为 $p'-$元素，称 G 为 **$p'-$群**.

群 G 的极大 $p-$子群 S 称为 G 的 **Sylow $p-$子群**，即如果 G 的 $p-$子群 P 使得 $S \le P \le G$，则 $S = P$.

在一个有限群中，可能有些元既不是 $p-$元素，也不是 $p'-$元素.

例 1 (1) 在 36 阶加法循环群 $\mathbb{Z}_{36} = \{\bar{0}, \bar{1}, \cdots, \overline{35}\}$ 中，由于元素阶均整除群阶 36，它的 $2-$元素可以是 1、2 或 4 阶元，即唯一 4 阶子群中的 4 个元 $\bar{0}, \bar{9}, \overline{18}, \overline{27}$，这些元构成的 4 阶子群 $\langle\bar{9}\rangle$ 是 $\mathbb{Z}_{36}$ 的 Sylow $2-$子群；它的 $3-$元素可以是 1、3 或 9 阶元，即唯一 9 阶子群中的 9 个元 $\bar{0}, \bar{4}, \bar{8}, \overline{12}, \overline{16}, \overline{20}, \overline{24}, \overline{28}, \overline{32}$，这些元构成的 9 阶子群 $\langle\bar{4}\rangle$ 是 $\mathbb{Z}_{36}$ 的 Sylow $3-$子群.

$\mathbb{Z}_{36} - \{\langle 4\rangle \cup \langle 9\rangle\}$ 中的元素既不是 $2-$元素，也不是 $3-$元素. $\mathbb{Z}_{36}$ 是一个 $5'-$群，也是 $7'-$群，$13'-$群.

(2) $\mathbb{Z}_9$ 的 Sylow $3-$子群就是 $\mathbb{Z}_9$ 自身，Sylow $2-$子群是单位子群，它的所有元素都是 $3-$元素. ■

如下引理讨论了在一个有限交换群当中，$p-$元素，$p'-$元素，$p-$子群与 Sylow $p-$子群的基本性质.

引理 2 设 A 是有限交换群, p 是素数，则

(1) $p-$元素的乘积与逆仍然是 $p-$元素，$p'-$元素的乘积与逆仍然是 $p'-$元素;

(2) $p-$子群的乘积仍为 $p-$子群;

(3) 令 $S_p=\{a\in A|a\text{ 是 }p-\text{元素}\}$，则 S_p 是 A 唯一的 Sylow $p-$子群.

证明 (1) 任取 $p-$元素 $a,b\in A$，则 $o(a),o(b)$ 均为 p 的方幂，由 A 交换知

$$(ab)^{o(a)o(b)}=a^{o(a)o(b)}b^{o(a)o(b)}=1,$$

所以 $o(ab)$ 整除 $o(a)o(b)$，也是 p 的方幂，故 ab 是 $p-$元素.

任取 $p'-$元素 $a,b\in A$，则 $o(a),o(b)$ 均与 p 互素，同上知 $o(ab)$ 整除 $o(a)o(b)$，故 $o(ab)$ 与 p 互素，即 ab 是 $p'-$元素.

由 $o(a^{-1})=o(a)$ 知，$p-$元素的逆仍为 $p-$元素，$p'-$元素的逆仍为 $p'-$元素.

(2) 设 P_1,P_2 都是 $p-$子群，由 A 交换知其乘积 P_1P_2 仍为子群，P_1P_2 中元形如 p_1p_2，其中 $p_1\in P_1,p_2\in P_2$ 都是 A 的 $p-$元素，由(1)知 p_1p_2 也是 $p-$元素，所以 P_1P_2 仍然是 A 的 $p-$子群.

(3) 显然 $1\in S_p$，故 S_p 非空. 由(1)知 S_p 对乘积与求逆封闭，故 S_p 是 A 的子群，再由定义知 S_p 的元素均为 $p-$元素，故 S_p 是 A 的 $p-$子群.

G 的任一 $p-$子群 A 中的元均为 $p-$元素，含于 $S_p=\{a\in A|a\text{ 是 }p-\text{元素}\}$，所以 $P\le S_p$.

综上，S_p 是 A 唯一的极大 $p-$子群，即 A 唯一的 Sylow $p-$子群.■

下面的 Cauchu 引理表明，任一有限群总是含有整除群阶的素数阶元与素数阶循环子群.

引理 3(Cauchy) (1) 设素数 p 整除有限交换群 A 的群阶 $\Rightarrow A$ 有 p 阶元.

(2) 设素数 p 整除群 G 的群阶 $\Rightarrow G$ 有 p 阶元.

证明 (1) 对群阶 $n:=|A|$ 用数学归纳法. 由题设知 $|A|\ge 2$.

如果 $|A|=2$，此时 $p=2$，2 阶群 A 循环，有 2 阶元，结论为真.

下设 A 的阶大于 2，且命题对阶小于 $|A|$ 的交换群均为真.

任取非单位元 $a\in A$. 如果 $p|o(a)$，设 $o(a)=pk,k\in\mathbb{Z}_{>0}$，则 $o(a^k)=p$，命题为真.

否则$(p,o(a))=1$. 此时商群$A/\langle a\rangle$的阶小于$|A|$, 由$p\|A|=|A/\langle a\rangle|\cdot o(a)$与$(p,o(a))=1$知$p\|A/\langle a\rangle|$, 对$A/\langle a\rangle$用归纳假设知其存在某$p$阶元$b\langle a\rangle$, 其中$b\in A$.

设$o(b)=s$, 则$(b\langle a\rangle)^s=b^s\langle a\rangle=\langle a\rangle$, 由$o(b\langle a\rangle)=p$知$p|s$, 设$s=pk,k\in\mathbb{Z}_{>0}$, 则$o(b^k)=p$.

(2) 对群G的阶用数学归纳法. 群阶为2时命题显然为真. 如果G是交换群, 由(1)即得.

下设G不是交换群, 则其中心$\mathbf{Z}(G)$是G的真子群. 如果$p\|\mathbf{Z}(G)|$, 由(1)知$\mathbf{Z}(G)$中有p阶元从而命题为真. 如果$p\nmid|\mathbf{Z}(G)|$, 设$x_1,\cdots,x_s$是群G的长度大于1的全部互异共轭类, 则有类方程:

$$|G|=|\mathbf{Z}(G)|+\sum_{1\le i\le s}|G:\mathbf{C}_G(x_i)|,$$

由$p\|G|$与$p\nmid|\mathbf{Z}(G)|$知存在某$|G:\mathbf{C}_G(x_i)|$不被p整除, 于是$p\|\mathbf{C}_G(x_i)|$, 对$\mathbf{C}_G(x_i)$用归纳法即得.■

利用Cauchy引理有下面的推论, 它表明$p-$群与一个群的Sylow $p-$子群的阶总是素数的方幂.

推论 4 (1) *有限$p-$群的阶为p的方幂*; (2) *有限群的Sylow $p-$子群的阶为p的方幂*.

证明 (1) 设P是有限$p-$群, 素数q整除$|P|$, 则由Cauchy引理知P有一个q阶元, 由P是$p-$群知其元素均为p的方幂, 于是由p,q均为素数知$q=p$, 故p是$|P|$唯一的素因子, 所以$|P|$是p的方幂.

(2) 由(1)即得.■

下面的定理表明, 有限交换群恰为其全部非单位 Sylow $p-$子群的之积. 这就使得研究一般的有限交换群可以归结为讨论有限交换的$p-$群.

定理 5 *A是有限交换群$\Rightarrow A=\times_{p\in\pi}S_p$. 其中$\pi$是$|A|$的全部素因子所成集, $S_p=\{a\in A|a$是$p-$元素$\}$.*

证明 (1) 由引理1(3)知S_p是A唯一的Sylow $p-$子群, 由A交换知任一子群均正规, 故$S_p\lhd A$;

(2) 任取素数$p\in\pi$, 由$p'-$元素的乘积仍为$p'-$元素知$\prod_{q\ne p,q\in\pi}S_q$中元素均为$p'-$元素, 而$S_p$中元为$p-$元素, 所以$S_p\cap\prod_{q\ne p}S_q=1$.

(3) 任取$a\in A$, 设$o(a)=n=p_1^{e_1}\cdots p_s^{e_s}$, 则$(n/p_1^{e_1},\cdots,n/p_s^{e_s})=1$, 于是存在整数$u_1,\ldots,u_s$使得

$$u_1\cdot n/p_1^{e_1}+\cdots+u_s\cdot n/p_s^{e_s}=1,$$

此时$a=a^1=\left(a^{n/p_1^{e_1}}\right)^{u_1}\cdots\left(a^{n/p_s^{e_s}}\right)^{u_s}$, 注意到$a^{n/p_i^{e_i}}$是$p_i-$元素, 属于$a^{n/p_i^{e_i}}\in S_{p_i}$, 故$\left(a^{n/p_i^{e_i}}\right)^{u_i}\in S_{p_i}$. 再注意到$p_i\in\pi$, 故$a\in\times_{p\in\pi}S_p$.

综合(1)(2)(3), 由内直积定义知 $A=\underset{p\in\pi}{\times}S_p$.■

注记 由于是交换群的分解, 如果将群运算用加号来表示, 这里的内直积就是内直和.

为了研究有限交换 $p-$ 群, 我们需要下面的两个引理. 不过引理本身也是非常有意义的结论.

引理 6 设有限交换 $p-$ 群 $A\neq 1$, 则: A 循环 $\Leftrightarrow$ A 有唯一的 p 阶子群.

证明 "$\Rightarrow$" 显然.

"$\Leftarrow$" 对 A 的阶用归纳法. A 的阶为 p 时结论显然成立, 下设 $|A|=p^n>p$ 且 A 具有唯一的 p 阶子群 P.

由 A 交换知映射 $\sigma:A\to A, a\mapsto a^p, \forall a\in A$ 是群同态, 显然 $\ker\sigma=P$. 由同构定理 A 知 $A/P\cong\sigma(A)$, 于是 $|A:\sigma(A)|=p$. 由 $|A|>p$ 知 $\sigma(A)\neq 1$, 由 P 是 A 唯一的 p 阶子群知 P 也是 $p-$ 群 $\sigma(A)$ 唯一的 p 阶子群, 由归纳假设知 $\sigma(A)$ 是 p^{n-1} 阶循环群.

设 $\sigma(A)=\langle b\rangle$, 任取 b 在 σ 下的一个原像 a, 则 $b=\sigma(a)=a^p$, 此时 $o(a)=p^n$, 故 A 循环.■

引理 6 用 p 阶子群刻画了循环交换 $p-$ 群, 引理 7 给出了有限交换 $p-$ 群有直积分解的一个充分条件.

引理 7 设 a 是有限交换 $p-$ 群 A 的最高阶元, 则存在子群 B 使得 $A=\langle a\rangle\times B$.

证明 由推论 3 知群阶 $|A|$ 为素数方幂 $p^n(n\geq 2)$, 对群阶用归纳法. 设最高阶元 a 的阶为 $p^m(m\leq n)$.

如果 A 循环, 则 a 是 A 的生成元, 令 $B=1$ 即可. 下设 A 不循环.

由 A 不循环与定理 5 知 A 至少有两个 p 阶子群, 设 P 是不含于 $\langle a\rangle$ 的一个 p 阶子群, 则 $\langle a\rangle\cap P=1$.

此时 $(aP)^{p^{m-1}}=a^{p^{m-1}}P\neq P$, 否则 $1\neq a^{p^{m-1}}\in P$ 从而导出矛盾! 而 $(aP)^{p^m}=a^{p^m}P=P$, 故 aP 是 A/P 的 p^m 阶元, 又显然 $o(gP)|o(g)$, 故 aP 是 A/P 的的最高阶元. 对 A/P 用归纳假设知存在 A/P 的某个子群 B/P 使得

$$A/P=(\langle a\rangle P/P)\times B/P,\ \text{其中}\ P\leq B\leq A.$$

由 $P\leq B$ 知 $A=\langle a\rangle PB=\langle a\rangle B$. 由直积 $(\langle a\rangle P/P)\times B/P$ 知 $\langle a\rangle\cap B\leq P$, 再由 P 不含于 $\langle a\rangle$ 知 $\langle a\rangle\cap P=1$, 故 $\langle a\rangle\cap B=\langle a\rangle\cap(\langle a\rangle\cap B)\leq\langle a\rangle\cap P=1$, 所以 $A=\langle a\rangle\times B$. ■

现在我们就可以证明如下有限交换 $p-$ 群的结构定理了.

定理 8 有限交换 $p-$ 群 A 可以分解为循环子群的直积 $A=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle$, 且直积因子的个数 s 及阶 $p_1^{e_1}\geq\cdots\geq p_s^{e_s}$ 由 A 唯一确定, 称为 A 的**型不变量**. 元素 $a_1,\cdots,a_s$ 称为 A 的一组**基**.

证明 重复应用引理 7 即得分解的存在性.

为证明唯一性, 引入 A 的如下两个子群

$$\Omega_1(A)=\{a\in A\mid a^p=1\},\quad \mho_1(A)=\{a^p\mid a\in A\},$$

直接验证知二者均为 A 的全不变子群, 分别是群同态 $\eta: a\mapsto a^p$ 的核与像. 且有

$$\Omega_1(A)=\langle a_1^{p^{e_1-1}}\rangle\times\cdots\times\langle a_1^{p^{e_s-1}}\rangle,\ \mho_1(A)=\langle a_1^p\rangle\times\cdots\times\langle a_s^p\rangle.$$

于是有 $|\Omega_1(A)|=p^s$, 给定 A 则 $\Omega_1(A)$ 唯一确定, 进而阶 $|\Omega_1(A)|=p^s$ 唯一确定, 这表明 s 与分解无关是唯一确定的.

给定 A, 则 $\mho_1(A)$ 唯一确定, 对 $\mho_1(A)$ 用归纳假设知 $a_1^p,\cdots,a_s^p$ 的阶 $p_1^{e_1-1}\geq\cdots\geq p_s^{e_s-1}$ 唯一确定, 进而知 $p_1^{e_1}\geq\cdots\geq p_s^{e_s}$ 也是由 A 唯一确定, 与分解无关.■

1.3 小 结

1. 定义 $p-$, $p'-$ 元素与 $p-$, $p'-$ 群, 子群, Sylow $p-$ 子群, $\mathbb{Z}_{36}$ 的 Sylow $2-$ 子群与 Sylow $3-$ 子群.

2. 有限 Abel 群: $p-$ 元素, $p-$ 子群的简单性质, 有唯一的 Sylow $p-$ 子群恰由全部 $p-$ 元素构成.

3. 阶被素数 p 整除的有限群必有 p 阶元的 Cauchy 引理; $p-$ 群、 $p-$ 子群与 Sylow $p-$ 子群的阶均为 p 的方幂.

4. **定理 4** 有限交换群 A 是其 Sylow $p-$ 子群的直积.

5. 有限交换 $p-$ 群 $A\neq 1$ 循环的刻画: 循环 $\Leftrightarrow$ 唯一的 p 阶子群.

6. 最高阶元导出有限交换 $p-$ 群 A 的直积分解: 设 a 是 A 的最高阶元, 则存在子群 $B\leq A$ 使得 $A=\langle a\rangle\times B$.

7. **有限 Abel p-群 A 的结构定理** A 可以分解为循环子群的直积.

习题 1.3

1. 设 G 是有限群, $N\triangleleft G$. 证明: G 是 $p-$ 群 $\Leftrightarrow N, G/N$ 都是 $p-$ 群.

2. 设 G 是群, $H\leq C\triangleleft G$ 且 C 是循环群, 证明 $H\triangleleft G$.

3. 设 G 是有限群, 规定群 G 的方指数 $\exp(G)$ 是使得 $a^{\exp(G)}=1,\forall a\in G$ 的最小正整数.

   (1) 如果 G 是交换群, 证明 G 中存在阶为 $\exp(G)$ 的元素;

   (2) 如果 G 是交换群, 证明: G 是循环群 $\Leftrightarrow|G|=\exp(G)$.

4. 设交换 $p-$ 群 G 的型不变量为 (p^4,p^3), 问 G 包含有多少个 p 阶子群? 多少个 p^2 阶子群?

5. 证明任一有限交换群 G 均可表为如下形状 $G=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle$, 其中 $o(a_i)\mid o(a_{i+1}),1\leq i\leq s-1$. 叙述并证明这种分解式的唯一性定理.