第 6 章 基本概念

近世代数（抽象代数）研究的主要内容就是代数系统，即在一个非空集合上面定义一种满足一定条件的一种或一种以上的二元运算（也称代数运算）. 本书主要介绍群、环、域三个基本的代数系统. 在这一章中，主要介绍与三种代数系统密切相关的基础概念集合之间的映射、二元运算、带有二元运算集合之间的同态映射与同构映射以及等价关系.

§1 映射

在介绍映射的概念之前，首先大体回顾有关集合的表示符号与集合运算.

集合用字母 $A,B,C,D,\cdots$ 来表示. 元素一般用小写拉丁字母 $a,b,c,d,\cdots$ 来表示，我们记为 $A=\{a,b,c,d,\cdots\}$. 若 a 是集合 A 的一个元素，称为 a 属于 A，或 A 包含 a，记为 $a\in A$. 若 a 不是集合 A 的一个元素，称为 a 不属于 A，或 A 不包含 a，记为 $a\notin A$.

ϕ：空集，是任何集合的子集.

$B\subset A$： B 为 A 的**子集**，称为 B 属于 A.
$B\not\subset A$： B 不是 A 的子集，称为 B 不属于 A.
$A\bigcap B$：表示 B 和 A 的**交集.**
$A\bigcup B$：表示 A 和 B 的**并集.**

$\overline{A}$ ：表示 A 关于整体集合 I 的**补集.** 显然，$\overline{A}=I-A$.

$2^A=\{B\mid B\subseteq A\}$ 表示 A 的所有子集组成的集合，叫做 A 的**幂集.**

定义 1 设 $A_1,A_2,\cdots,A_n$ 是 n 个集合. 一切从 $A_1,A_2,\cdots,A_n$ 里顺序取出的元素组 $(a_1,a_2,\cdots,a_n)$，$a_i\in A_i$ 所做成的集合叫做**集合 $A_1,A_2,\cdots,A_n$ 的加氏积**，记为 $A_1\times A_2\times\cdots\times A_n$.

下面给出映射的一般性定义.

定义 2 设 A,B 是两个给定的集合，如果有一个规则 ϕ，对于 A 的任意元素 $a\in A$，都能得到一个唯一的 $b\in B$ 与 a 对应，那么 ϕ 是 A 到 B 的一个映射. 记为

$$\phi : A \to B$$

A 叫做映射 ϕ 的定义域，B 叫做 ϕ 的值域，b 说是 a 在 ϕ 作用下的象，记作 $b = \phi(a)$，并用符号

$$\phi : a \mapsto b$$

表示，a 说是 b 的一个原象.

例 1　　I_A：　$a \mapsto a$，　$\forall a \in A$

是 A 到 A 的一个映射，叫做 A 上的**恒等映射.**

例 2　　设 $A = \{x, y, z\}$，　$B = \{a, b, c, d\}$.

$$\varphi：\ A \mapsto B$$

$$x \mapsto a$$
$$x \mapsto b$$
$$y \mapsto c$$
$$z \mapsto d$$

x 的象不唯一，故 φ 不是 A 到 B 的映射.

定义 3　A 到 B 的两个映射 ϕ 和 φ 相等当且仅当，对任意的 $a \in A$，都有 $\phi(a) = \varphi(a)$.

从定义 3 中可以得到一判断映射不相等的简单方法，即存在 $a \in A$，使得 $\phi(a) \neq \varphi(a)$.

定义 4　ϕ 为集合 A 到集合 B 的映射．如果对于集合 B 中的每一个元素 b，在集合 A 中都能找到原象 a，使 $b = \phi(a)$，则称 ϕ 为集合 A 到集合 B 的**满射.** 如果对于任意

$$a_1 \neq a_2 \Rightarrow \phi(a_1) \neq \phi(a_2)，$$

称 ϕ 为集合 A 到集合 B 的**单射.** 如果 ϕ 即为单射又为满射，则称 ϕ 为集合 A 到集合 B 的一一**映射.**

由单射的定义知，ϕ 为单射的另等价一定义（逆否命题）是

$$\phi(a_1) = \phi(a_2) \Rightarrow a_1 = a_2 .$$

另外，由一一映射的定义易得结论有限集合与它的真子集之间不可能存在一一映射.

定义 5 若有三个集合 $A,B,C,$

$$\phi: A \to B, \qquad \varphi: B \to C$$

由 ϕ,φ 确定的 A 到 C 的映射

$$\eta: a \mapsto \varphi(\phi(a)), \quad \forall a \in A.$$

叫做映射 ϕ,φ 的**合成**，记为 $\eta = \varphi \circ \phi$.

定理 1 设

$$\phi: A \to B, \varphi: B \to C, \eta: C \to D,$$

则有

1) $\eta \circ (\varphi \circ \phi) = (\eta \circ \varphi) \circ \phi,$

2) $I_B \circ \phi = \phi, \quad \phi \circ I_A = \phi$.

证明 1）按照映射相等的定义，易见合成映射 $\eta \circ (\varphi \circ \phi)$ 与 $(\eta \circ \varphi) \circ \phi$ 的定义域和值域相同，下面我们需证对任意的 $a \in A$

$$[\eta \circ (\varphi \circ \phi)](a) = [(\eta \circ \varphi) \circ \phi](a)$$

成立.

根据映射合成定义，对于任意的 $a \in A$ 我们有以下等式

$$[\eta \circ (\varphi \circ \phi)](a) = \eta[(\varphi \circ \phi)(a)] = \eta[\varphi(\phi(a))] = (\eta \circ \varphi)(\phi(a)) = [(\eta \circ \varphi) \circ \phi](a).$$

2）$I_B \circ \phi$ 与 ϕ 的定义域均为 A，值域均为 B . 并且对任意的 $a \in A$ 有

$$(I_B \circ \phi)(a) = I_B(\phi(a)) = \phi(a),$$

即 $I_B \circ \phi = \phi$. 同理可证 $\phi \circ I_A = \phi$.

定理 1 中的 1）说明了映射的合成满足结合律.

定义 6 设 $\phi: A \to B$. 若存在 $\varphi: B \to A$，使 $\varphi \circ \phi = I_A$，则说 ϕ 是左可逆映射，φ 叫做 ϕ 的左逆映射. 同样，若 $\phi \circ \varphi = I_B$，则说 ϕ 是右可逆，φ 叫做 ϕ 的右逆映射. 当 ϕ 是双侧可逆时，称 ϕ 是可逆映射.

下面定理提供了判断一个映射为左可逆或右可逆的充要条件.

定理 2　给定映射 $\phi: A \to B$.

（1）ϕ 是左可逆的充要条件为 ϕ 是单射；

（2）ϕ 是右可逆的充要条件为 ϕ 是满射.

证明　（1）必要性：设 ϕ 是左可逆，即存在 $\varphi: B \to A$，使 $\varphi \circ \phi = I_A$.

希望证明，当 $\phi(a_1) = \phi(a_2)$ 时，有 $a_1 = a_2$. 因为

$$a_1 = I_A(a_1) = (\varphi \circ \phi)(a_1) = \varphi(\phi(a_1)) = \varphi(\phi(a_2))$$

$$= (\varphi \circ \phi)(a_2) = I_A(a_2) = a_2 ,$$

即 ϕ 是单射.

充分性：设 ϕ 是 A 到 B 的单射，希望找到 $\varphi_1: B \to A$，使 $\varphi_1 \circ \phi = I_A$. 取定一个 $a_1 \in A$. 定义 φ_1 如下

$$\varphi_1(b) = \begin{cases} a, & \exists a \in A, \phi(a) = b, \\ a_1, & b \notin \phi(A). \end{cases}$$

则任意的 $b \in B, \varphi_1(b)$ 唯一确定，并且对任意的 $a \in A$ 有

$$(\varphi_1 \circ \phi)(a) = \varphi_1(\phi(a)) = \varphi_1(b) = a ,$$

即 $\varphi_1 \circ \phi = I_A$.

（2）必要性：设 ϕ 是右可逆，即存在 $\eta: B \to A$，使 $\phi \circ \eta = I_B$. 下证 ϕ 为满射. 由

$$b = I_B(b) = (\phi \circ \eta)(b) = \phi(\eta(b))$$

知，对于任意 $b \in B$，存在 $\eta(b) \in A$，使 $\phi(\eta(b)) = b$，故 ϕ 是满射.

充分性：设 ϕ 是满射，则对于每一 $b \in B$，存在一个 $a \in A$，使 $\phi(a) = b$. 一般情形，这样的 a 不只一个，但是，我们只取定一个，作 $\varphi_2: b \mapsto a,$ 这是 B 到 A 的一个映射，并且对任

意$b \in B$有，

$$(\phi \circ \varphi_2)(b) = \phi(\varphi_2(b)) = \phi(a) = b.$$

即$\phi \circ \varphi_2 = I_B$．故$\phi$是右可逆．

推论　$\phi : A \to B$，则ϕ是可逆映射的充要条件为ϕ是双射．

当ϕ是双射，则ϕ既有左逆映射φ，又有右逆映射η，φ与η有何关系呢？下面定理说明两者相等．

定理 3　设$\phi : A \to B$，且$\varphi \circ \phi = I_A, \phi \circ \eta = I_B$，则$\varphi = \eta$．

证明　由定理 1，

$$\varphi = \varphi \circ I_B = \varphi \circ (\phi \circ \eta) = (\varphi \circ \phi) \circ \eta = I_A \circ \eta = \eta .$$

定义 6　一个A到A的映射叫做A的一个**变换**.

习惯上，一个A到A的满射，单射或一一映射叫做A的一个**满射变换，单射变换，一一变换**.

最后再通过几个例子熟悉以下映射的有关内容．

例 3　设$A = Z, B = \{2n \mid n \in Z\}$（所有偶数的集合），$\forall n \in Z$　定义

$$\varphi_1 : \ n \mapsto 2n$$

$$\varphi_2 : \ n \mapsto 4n$$

$$\varphi_3 : \ n \mapsto n，\text{当} 2 \mid n$$

$$n \mapsto n+1 \ ，\text{当} 2 \nmid n$$

$$\varphi_4 : \ n \mapsto |n|, \ \text{当} 2 \mid n$$

$$n \mapsto |n+1| \ \ \text{当} 2 \nmid n$$

这四个法则都符合映射的定义，都是整数集Z到偶数集B的映射．

φ_1是双射．φ_2是单射，但不是满射．φ_3是满射，但不是单射．φ_4既不是满射，又不是单射．

例 4　设$A = \{a, b, c\}$，　$B = \{1, 2, 3, 4\}$.

$$f：1\mapsto a,\quad 2\mapsto b,\quad 3\mapsto c,\quad 4\mapsto a$$

$$g：a\mapsto 1,\quad b\mapsto 2,\quad c\mapsto 3$$

易见 $f\circ g=I_A$，但 $g\circ f\neq I_B$，故 g 是左可逆映射，f 是其左逆映射，但不是其右逆映射.

§2 代数运算

代数系就是研究带有代数运算（或者称为二元运算）的集合的特性．有了代数运算，才可以研究集合关于代数运算的结构．因此代数运算是代数系重要组成部分．在这一节我们将利用映射来定义代数运算的概念，并简单介绍与代数运算有关的几个运算规律，如结合律、交换律、分配律等.

定义 1 A, B, C 为三个集合．我们把一个从 $A\times B$ 到 C 的映射叫做一个从 $A\times B$ 到 C 的**代数运算，记为**$\circ$，对于任意 $\circ$：$(a,b)\mapsto c$，记为 $a\circ b=c$.

例 1 $A=${所有整数}，$B=${所有不等于零的整数}，$D=${所有有理数}.

$$\circ:\ (a,b)\mapsto \frac{a}{b}=a\circ b$$

是从 $A\times B$ 到 D 的代数运算，其中 $A\times B$ 是 A 与 B 的加氏积.

如果 $\circ$ 是 $A\times A$ 到 A 的代数运算，我们就说，集合 A 对于代数运算 $\circ$ 来说是封闭的，也说 $\circ$ 是 A 的代数运算或**二元运算.**

例 2 $A=Z^+=${正整数集合}，对于 A 上的普通除法不是 A 上的二元运算.

例 3 对任意的 $a, b\in R$ 规定

$$a\circ b=\max(a,b)$$
$$a\cdot b=\min(a,b)$$

都是实数集 R 上的二元运算.

例 4 证明 Z_m 的加法与乘法运算为二元运算.

$$+:\ \ \overline{a}+\overline{b}\mapsto\overline{a+b}$$

$$\times:\ \ \overline{a}\times\overline{b}\mapsto\overline{ab}$$

证明 若 $\overline{a}=\overline{a'},\overline{b}=\overline{b'}$，则

$$\overline{a'}+\overline{b'}=\overline{a'+b'}=\overline{a+b}=\overline{a}+\overline{b},$$

故“＋”为 $Z_m\times Z_m$ 到 Z_m 的映射，从而加法运算为二元运算.

同理，

$$\overline{a'}\times\overline{b'}=\overline{a'b'}=\overline{ab}=\overline{a}\times\overline{b},$$

故“×”为 $Z_m\times Z_m$ 到 Z_m 的映射，从而乘法运算为二元运算.

定义 2 如果$\circ$是 A 的代数运算，对于任意 $a,b,c\in A$，如果 $(a,b)\circ c=a\circ(b,c)$，则称代数运算$\circ$适合**结合律**，记 $a\circ b\circ c=(a\circ b)\circ c=a\circ(b\circ c)$．如果结合律不成立，符号 $a\circ b\circ c$ 是没有意义的.

从更一般的情况看，在 A 中任取 n 个元 $a_1,a_2,\cdots a_n$，π_i 和 π_j 是任意两种不改变 $a_1,a_2,\cdots a_n$ 的先后顺序加括号的方法，如果

$$\pi_i(a_1\circ a_2\circ\cdots\circ a_n)=\pi_j(a_1\circ a_2\circ\cdots\circ a_n),$$

则用 $a_1\circ a_2\circ\cdots\circ a_n$ 来表示这个唯一结果.

下面我们证明一个定理并以此说明结合律的作用.

定理 1 假如一个集合 A 的代数运算$\circ$适合结合律，那么对于 A 的任意 $n(n\geq 2)$ 个元 $a_1,a_2,\cdots a_n$ 来说，所有的 $\pi_i(a_1\circ a_2\circ\cdots\circ a_n)$ 都相等，因此符号 $a_1\circ a_2\circ\cdots\circ a_n$ 就总有意义.

证明 用数学归纳法．已知 $n\leq 3$ 时，定理成立．假设元素个数 $\leq n-1$ 时，定理成立．对于 n 个元 $a_1,a_2,\cdots a_n$ 来说，只需证

$$\pi(a_1\circ a_2\circ\cdots\circ a_n)=a_1\circ(a_2\circ a_3\circ\cdots\circ a_n) \qquad (1)$$

成立． $\pi(a_1\circ a_2\circ\cdots\circ a_n)$ 是由加括号所的结果，这个结果的最后一步总是对两个元进行运算 $\pi(a_1\circ a_2\circ\cdots\circ a_n)=b_1\circ b_2$，这里 b_1 表示前面 i 个元经加括号所的结果，b_2 是后 $n-i$ 个元经加括号所得的结果．因为 i 和 $n-i$ 都小于 $n-1$，由归纳法得

$$b_1 = a_1 \circ a_2 \circ \cdots \circ a_i, \quad b_2 = a_{i+1} \circ \cdots \circ a_n$$

$$\pi(a_1 \circ a_2 \circ \cdots \circ a_n) = (a_1 \circ a_2 \circ \cdots \circ a_i) \circ (a_{i+1} \circ a_{i+2} \circ \cdots \circ a_n)$$

当$i = 1$，则(1)成立；若$i \geq 2$，那么

$$\begin{aligned}
&\pi(a_1 \circ a_2 \circ \cdots \circ a_n) \\
&= [a_1 \circ (a_2 \circ \cdots \circ a_i)] \circ (a_{i+1} \circ \cdots \circ a_n) \\
&= a_1 \circ [(a_2 \circ \cdots \circ a_i) \circ (a_{i+1} \circ \cdots \circ a_n)] \\
&= a_1 \circ (a_2 \circ a_3 \circ \cdots \circ a_n)
\end{aligned}$$

定理得证.

由以上定理可看出，若结合律成立，我们就能随时应用$a_1 \circ a_2 \circ \cdots \circ a_n$这一符号，结合律的重要性也就在此.

定义 3 $\circ$为$A \times A$到D的代数运算，如果$a \circ b = b \circ a$，则说代数运算$\circ$适合交换律.

定理 2 假如一个集合A的代数运算$\circ$同时适合结合律和交换律，那么$a_1 \circ a_2 \circ \cdots \circ a_n$中元素次序可以任意交换.

证明 利用归纳法. 已知当只看一个或两个元素时，定理成立.

设当元的个数$\leq n-1$时，定理成立. 在此假设下，我们证明若将a_i的次序颠倒一下，做成$a_{i1} \circ a_{i2} \circ \cdots \circ a_{in}$（此处的$i1, i2, \cdots, in$是$1,2,\cdots,n$的一个排列），则

$$a_{i1} \circ a_{i2} \circ \cdots \circ a_{in} = a_1 \circ a_2 \circ \cdots \circ a_n$$

假设$i1, i2, \cdots, in$中ik等于n，那么由于结合律，交换律及归纳法假定，可得

$$\begin{aligned}
a_{i1} \circ a_{i2} \circ \cdots \circ a_{in} &= (a_{i1} \circ a_{i2} \circ \cdots \circ a_{ik-1}) \circ \left[a_n \circ \left(a_{ik+1} \circ \cdots \circ a_{in}\right)\right] \\
&= \left(a_{i1} \circ a_{i2} \circ \cdots \circ a_{ik-1}\right) \circ [(a_{ik+1} \circ \cdots \circ a_{in}) \circ a_n] \\
&= [(a_{i1} \circ a_{i2} \circ \cdots \circ a_{ik-1}) \circ (a_{ik+1} \circ \cdots \circ a_{in})] \circ a_n \\
&= (a_1 \circ a_2 \circ \cdots \circ a_{n-1}) \circ a_n
\end{aligned}$$

$$= a_1 \circ a_2 \circ \cdots \circ a_n .$$

我们已知的许多代数运算都是满足交换律的，但也有例外，如 n 阶矩阵及线性变换的乘法．总之交换律是一个很重要的性质．

最后我们来看一个涉及到两个运算的规律，第一分配律与第二分配律．

定义 4 定义了以下这两个代数运算 $\otimes$ 和 $\oplus$：

（1）$\otimes$ 是一个 $B \times A$ 到 A 的代数运算．

（2）$\oplus$ 是一个 A 的代数运算．

如果对于任意 $b \in B$ 和 $a_1, a_2 \in A$，下式总成立

$$b \otimes (a_1 \oplus a_2) = (b \otimes a_1) \oplus (b \otimes a_2) ,$$

则称代数运算 $\otimes$ 和 $\oplus$ 适合**第一分配律.**

一般地，第一分配律不一定成立．

定理 3 假如 $\oplus$ 适合结合律，而且 $\otimes$ 和 $\oplus$ 适合第一分配律，那么对于 B 的任意 b，A 的任意 $a_1, a_2, \cdots a_n$ 来说，

$$b \otimes (a_1 \oplus a_2 \oplus \cdots \oplus a_n) = (b \otimes a_1) \oplus (b \otimes a_2) \oplus \cdots \oplus (b \otimes a_n) .$$

此定理同样可用归纳法证明，此处略去，留作习题．以上所讨论的为第一分配律，第二分配律与其完全类似．

定义 5 定义了以下这两个代数运算 $\otimes$ 和 $\oplus$：

（1）$\otimes$ 是一个 $B \times A$ 到 A 的代数运算。

（2）$\oplus$ 是一个 A 的代数运算。

如果对于任意 $b \in B$ 和 $a_1, a_2 \in A$，下式总成立

$$(a_1 \oplus a_2) \otimes b = (a_1 \otimes b) \oplus (a_2 \otimes b) ,$$

则称代数运算 $\otimes$ 和 $\oplus$ 适合**第二分配律.**

同样，我们有定理 4．

定理 4 假如 $\oplus$ 适合结合律，而且 $\otimes$ 和 $\oplus$ 适合第二分配律，那么对于 B 中的任意元素 b，A 中的任意元素 $a_1, a_2, \cdots a_n$ 来说，

$$(a_1 \oplus a_2 \oplus \cdots \oplus a_n) \otimes b = (a_1 \otimes b) \oplus (a_2 \otimes b) \oplus \cdots \oplus (a_n \otimes b)$$

分配律的重要性在于它将两种运算联系到了一起．

§3 带有运算集合之间的同态映射与同构映射

上节我们讨论了集合 A 上的代数运算，它是定义 $A\times A$ 到 A 的特殊的映射．在本节中讨论与代数运算有联系的两种映射，同态映射与同构映射．

定义 1 给定两个带有运算的集合 A, B，$\circ$ 为 A 的代数运算，$\bullet$ 为 B 的代数运算，并且有一个 A 到 B 的映射 ϕ，对于 A 中任意两个元 a_1, a_2 下式总成立

$$\phi(a_1 \circ a_2) = \phi(a_1) \bullet \phi(a_2), \tag{1}$$

则称 ϕ 为 A 到 B 的**同态映射**.

习惯上，如果 A 到 B 的映射 ϕ 满足(1)，我们称 ϕ 能够保持 A 的代数运算.

例 1 设 $G=(Z,+), G'=(R^*,\circ)$，令

$$\varphi:\ n \mapsto \begin{cases} 1, & \text{当} 2 \mid n \text{时}, \\ -1, & \text{当} 2 \nmid n. \end{cases}$$

则 φ 是 G 到 G' 的一个映射．并且对于任意 $m,n\in Z$，有

$$\varphi(m+n) = \varphi(m) \circ \varphi(n),$$

即 φ 是 G 到 G' 的一个同态映射.

例 2 对于 $(Z,+)$ 考虑映射

$$\varphi:\ n \mapsto 2n, \quad \forall n \in Z.$$

因对任意的 $m,n\in Z$，有

$$\varphi(m+n) = 2(n+m) = 2n+2m = \varphi(n)+\varphi(m)$$

故 φ 是 $(Z,+)$ 到 $(Z,+)$ 的一个同态映射，但 φ 不是 $(Z,\cdot)$ 到 $(Z,\cdot)$ 的同态映射，因为不能保证

$$\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n).$$

另外，A 到 B 的同态映射 ϕ 如果同时也是一个满射，我们叫做**同态满射.**

定义 2 A 到 B 的同态映射 ϕ，若

（1）ϕ是一个满射，称ϕ为A到B的**同态满射**，称A与B同态，记为$A\sim B$；

（2）ϕ是一个一一映射，称ϕ为A到B的**同构映射**．称A与B同构，记为$A\cong B$．

同构映射不仅反映了两个集合之间的元素是一一对应的，而且它们的运算结构是完全相同．

若对于代数运算$\circ$与$\bullet$来说，A和B同构．那么，对于代数运算$\circ$与$\bullet$来说，A和B两个集合，抽象来看没有什么区别（只有命名上的不同）．若一个集合有一个与这个集合的代数运算有关的性质，那么另一个集合有一个完全类似的性质．

定义 3 对于同一个A上的运算$\circ$来说，若存在一个A到A间的同构映射，称这个影射为A的**自同构映射**．

例 3 给出一个自同构的例子．

对于从R到R的映射$\phi: x\mapsto x^m$，$m\in N$且为奇数．对任意$x,y\in R$有

$$\phi(xy)=(xy)^m=x^m y^m=\phi(x)\phi(y)$$

ϕ是一个同态映射，显然ϕ是一个一一映射，所以ϕ是R的自同构映射．

最后我们再通过几个例子，以便熟悉同态、同构的概念．

例 4 设映射ϕ将整数集合$(Z,+)$映到模n剩余类集合$(Z_n,+)$，

$$\phi:\ Z\to Z_n$$

$$a\mapsto \overline{a}$$

证明：$(Z,+)\sim(Z_n,+)$．

证明 只要证明ϕ为满同态．任意$a,b\in Z$有

$$\phi(a+b)=\overline{a+b}=\overline{a}+\overline{b}=\phi(a)+\phi(b),$$

ϕ为同态映射．

又因为任意$\overline{b}\in Z_n$，存在$b\in Z$，使$\phi(b)=\overline{b}$，所以ϕ为满射．但是若$a\equiv b(\mathrm{mod}\, n)$，则$\phi(a)=\phi(b)$，所以$\phi$不为单射，从而$\phi$为满同态映射．

例 5 设模p的原根为g，模p的简化剩余类集合Z_p^*上的二元运算定义为模p乘法．定义Z_p^*到$(Z_{p-1},+)$的映射f

$$f:\ Z_p^* \to (Z_{p-1},+)$$

$$a \mapsto \gamma_p(a)$$

证明：f 为同构映射.

证明 f 显然为映射，且

(1) $f(ab)=\gamma(ab)=\gamma(a)+\gamma(b)=f(a)+f(b)$. 因此 f 为同态影射；

(2) 任意 $x\in(Z_{p-1},+)$，存在 $a=g^x(\mathrm{mod}\ p)$，使 $f(a)=x$，故 f 为满射；

（3）若 $x\equiv y(\mathrm{mod}\ p-1),$ 则

$$a=g^x\equiv g^y=b(\mathrm{mod}\ p),$$

即 $f(a)=x, f(b)=y$，即 f 为单射. 因此， f 为同构映射.

§4 等价关系与分类

在前面数论的学习中知道，给定一个模 n 剩余类，实际上是给定了整数的一个分类. 对于一般的集合有时也要对其进行分类. 集合的分类与等价关系的概念有密切关系. 首先我们来看一下二元关系的概念.

定义 1 $A\times B$ 的子集 R 叫做 A,B 间的一个二元关系. 当 $(a,b)\in R$ 时，说 a 与 b 具有关系 R，记为 aRb；当 $(a,b)\notin R$ 时，说 a 与 b 不具有关系 R，记为 $aR'b$.

下面我们主要讨论 A 上的二元关系.

定义 2 A 是一个集合， $A\times A$ 为加氏积， $A\times A$ 的任何一个子集合 R，称为集合 A 上的一个二元关系.

例 1 $A=R$，这里 R 表示实数.

$$R_1=\{(a,b)\,|\,(a,b)\in R\times R, a=b\},$$

$$R_2=\{(a,b)\,|\,(a,b)\in R\times R, a\le b\},$$

$$R_3 = \{(a,b) \mid (a,b) \in R \times R, a^2 + b^2 = 1\}.$$

容易看出，

$$aR_1b \Leftrightarrow a = b,$$

故 R_1 是 R 上元素的相等关系.

$$aR_2b \Leftrightarrow a \le b,$$

故 R_2 是 R 上元素的小于等于关系. aR_3b 当且仅当 (a,b) 在单位圆上.

等价关系是一种特殊的二元关系，我们用“~”来表示.

定义 3 若 $R \subseteq A \times A$，且 R 满足如下条件：

1) 自反性：$(a,a) \in R$；

2) 对称性：$(a,b) \in R$，则 $(b,a) \in R$；

3) 传递性：$(a,b) \in R$，$(b,c) \in R$，则 $(a,c) \in R$；

那么我们称 R 为一个**等价关系.**

如果 R 为一个等价关系，若 $(a,b) \in R$，则称 a 与 b 等价，记为 $a \sim b$.

若已知 R 是 A 上的一个等价关系，$x \in A$，则

$$\overline{x} = \{y \mid y \in A, (x,y) \in R\}$$

称为由 x 决定的**等价类.**

性质 R 是 A 上的一个等价关系，任 $x, y \in A$，有

$$\overline{x} = \overline{y} \text{ 或者 } \overline{x} \cap \overline{y} = \phi.$$

该性质的证明留作习题.

定义 4 如果 $\{B_i, i \in I\}$ 为一个 A 的子集的集合，满足下列两个条件：

（1） $A = \bigcup_{i \in I} B_i$

（2） $B_i \bigcap B_j = \Phi$

$\{B_i, i \in I\}$ 叫做集合 A 的一个分类.

分类与等价关系之间存在以下结论.

定理 给定集合 A 的一个分类决定 A 的一个等价关系；反之给定集合 A 的一个等价关系~决定 A 的一个分类.

证明 （1）给定集合 A 的的一个分类 $\{B_i, i \in I\}$，下面我们利用这个分类定义一个等价关系. $a \sim b$，当且仅当 $a,b \in B_i$，其中 B_i 为 A 的分类中的某个子集.

下证~为一个等价关系.

a) 显然~为 A 上的一个二元关系.

b) $a \sim a$.

c) 若 $a \sim b$，那么 $b \sim a$.

d) $a \sim b,\quad b \sim c \Rightarrow a \sim c$.

（2）给定集合 A 的一个~等价关系，下面我们利用等价关系定义 A 的一个分类 $\{B_i, i \in I\}$.

由等价关系~得到一个等价类的集合 $\{\overline{a}, a \in A\}$，下证 $\{\overline{a}, a \in A\}$ 为 A 的一个分类

a) $A = \bigcup_{a \in A} \overline{a}$

b) 由等价类的性质知任 $a,b \in A$，　$\overline{a} = \overline{b}$ 或 $\overline{a} \cap \overline{b} = \phi$，即 A 的不同得等价类为两两不相交的子集. 定理得证.

例 2 同余关系是一种等价关系. 即给定模 m，关于模 m 同余关系“$\equiv$”满足等价关系的三个条件.

证明 由第 2 章第 1 节知同余关系为等价关系.

根据同余关系，将整数集合 Z 划分为 m 个集合 $Z_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}$ 称为模 m 剩余类集合.

例 3　p 为大于 2 的素数，按照 $p^{\alpha} \| n, \alpha = 1,2\cdots$，将整数集合分为无穷多类.

习题

1．设 $A = \bigcup_{i=1}^{\infty} A_i$，证明存在 A_i 的子集 B_i，$i = 1,2,\cdots$，使 $A = \bigcup_{i=1}^{\infty} B_i$，并对任意 $i \neq j$，均有 $B_i \bigcap B_j = \phi$.

2．ϕ,φ,η 均为 z 到 z 的映射 ϕ,φ,η

$$\phi: k \mapsto ak$$

$$\varphi: k \mapsto ak+1$$

$$\eta: k \mapsto ak+2$$

计算 $\phi\circ\varphi,\varphi\circ\eta,\phi\circ\eta\circ\varphi$，并找出 ϕ,φ,η 共同的左逆映射.

3．设 f 是 A 到 B 的映射，$S\subseteq A$，$T\subseteq B$，证明：

（1）$f(f^{-1}(T))=T\bigcap f(A)$；

（2）$f(S\bigcap f^{-1}(T))=f(S)\bigcap T$

4．设 φ 是双射，且 $\varphi\psi$ 有意义，证明：ψ 是单射的充分必要条件是 $\varphi\psi$ 是单射；ψ 是满射的充分必要条件是 $\varphi\psi$ 是满射.

5．$A=\{$所有实数$\}$，并定义了两个运算$\circ,\bullet$

$$a\circ b=a+2b$$
$$a\bullet b=a-b$$

验证这两个代数运算是否满足结合律、交换律？

6．设 φ 是单射，且 $\varphi\psi$ 和 $\varphi\psi'$ 都有意义，证明：$\varphi\psi=\varphi\psi'\Leftrightarrow\psi=\psi'$.

7．设 $A=\{a,b,c\}$，试构造 A 上的二元运算.

8．设 R_1,R_2 是 A 的两个等价关系，$R_1\cap R_2$ 是不是 A 的二元关系？是不是等价关系？为什么？$R_1\cup R_2$ 是不是 A 的二元关系？

9．设 R_1,R_2 是 A 的两个二元关系，规定

$$R_1\circ R_2=\{(a,b)\mid\exists x\in A:(a,x)\in R_1,(x,b)\in R_2\}$$

证明：“$\circ$”是 A 的一切二元关系所成集合 B 的一个二元运算.

10．设 $G=(R^*,\times)$，R^* 为一切非零实数集合，下述规则 f，哪些是 G 到 G 的同态映射？

1）$x \mapsto |x|$，　　2）$x \mapsto 2x$，　　3）$x \mapsto x^2$，

4）$x \mapsto \frac{1}{x}$，　　5）$x \mapsto -x$，　　6）$x \mapsto -\frac{1}{x}$.

11．假定 A 和 A' 对代数运算$\circ$和$\bar{\circ}$来说同态，A' 和 B 对代数运算$\bar{\circ}$和$*$来说同态，证明：A 和 B 对代数运算$\circ$和$*$来说同态.

12．假定对于 A 的代数运算$\circ$和$\oplus$，B 的代数运算$\bullet$和$\otimes$，A 到 B 的同态满射 ϕ，则

a) 若$\circ$适合结合律，$\bullet$也适合结合律；

b) 若$\circ$适合交换律，$\bullet$也适合交换律；

c) 若$\circ$对$\oplus$适合第一分配律，$\bullet$对$\otimes$也适合第一分配律；若$\circ$对$\oplus$适合第二分配律，$\bullet$对$\otimes$也适合第二分配律.

13．$G=(Z,+), G'=\{C^*,\circ)$，令

$$f：\ n \mapsto i^n \qquad （i 是 C 的虚数单位），$$

则 f 是G到G'的一个同态映射.

14．证明：$f:a \mapsto a^k$，$(k, p-1)=1$为 Z_p^* 上的自同构映射.

15．设 $B=\{1,-1\}$，B 对于数的乘法封闭。对于 $(Z_2,+)$ 与 $(B,\cdot)$，证明：映射 $\varphi：\bar{0} \mapsto 1, \bar{1} \mapsto -1$ 为同构映射.

16．设 $A=\{$所有有理数$\}$，A 的代数运算式普通加法．$A'=\{$所有不为零的有理数$\}$，A' 得代数运算为普通乘法．证明：A 与 A' 间不存在同构映射。（先确定 0 的像）.

17．任意 $(x,y),(x',y') \in R \times R$，令

$$(x,y) \sim (x',y') \Leftrightarrow x-x\text{和}y-y \text{ 都是整数.}$$

证明：~是一个等价关系.

18．假如一个关系 R 具有对称性和传递性，那么它也具有自反性．推论方法是：因为 R 具有对称性，$aRb \Rightarrow bRa$；因为 R 具有传递性，$aRb, bRa \Rightarrow aRa$ 这个推论方法有什么错误？

19．$(F)_n$ 表示数域 F 上全部 n 阶方阵的集合，f 是 $(F)_n$ 到 $\{0,1,2,\cdots,n\}$ 上的满射

$$f:(a_{ij}) \mapsto 秩(a_{ij}),$$

求 f 决定的等价关系，定义等价类.

２０．设 F 是一个数域

$$V_4=\{a_1,a_2,a_3,a_4 \mid a_i \in F\}, M_2(F)=\{\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \mid a_i \in F\},$$

证明：$(V_4,+) \cong (M_2(F),+)$．（其中左、右端中的“+”分别是向量加法和矩阵乘法）.