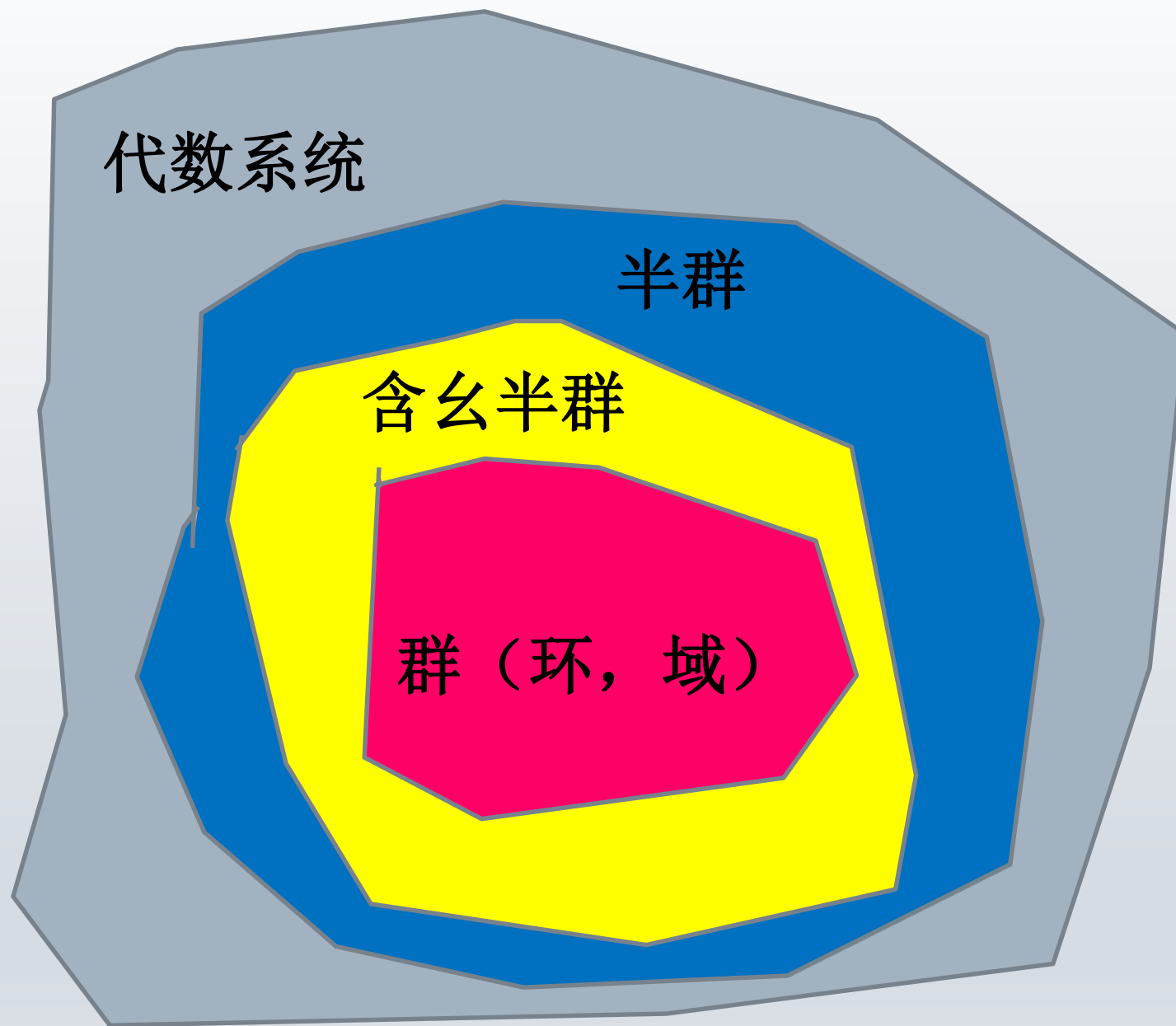


$\langle A, * \rangle$

群, 环, 域
格与布尔代数



§ 5.2 群的概念及其性质

5.2.1 群的基本概念

定义：

设 $\langle G, * \rangle$ 是一代数系统，如果满足以下几点：

- (1) 运算是可结合的；
- (2) 存在单位元 e ；
- (3) 对任意元素 a 都存在逆元 a^{-1} ；

则称 $\langle G, * \rangle$ 是一个群。 $|G|$ 表示群的阶，可以是有限也可以是无限

5.2.1 群的基本概念

例： $\langle \mathbf{R}, + \rangle$, $\langle \mathbf{R} - \{0\}, \times \rangle$, 构成群

(1) 运算是封闭的

(2) 运算是可结合的；

(3) 存在单位元 e ；

(4) 对任意元素 a 都存在逆元 a^{-1} ；

5.2.1 群的基本概念

例：下列系统能否构成群？

举例： $\langle M_n(R), + \rangle$ ，**n**是大于等于**1**的正整数。 \checkmark 是

举例： $\langle M_n(R), \bullet \rangle$ ，**n**是大于等于**1**的正整数。 \times 否

举例： $\langle P(S), \oplus \rangle$ ，**S**非空集合， \oplus 是集合的对称差。 \checkmark 是

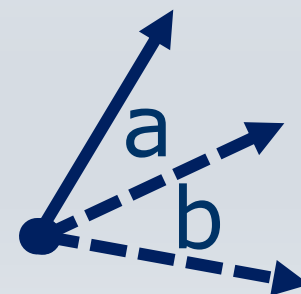
举例： $\langle P(S), \cap \rangle$ ， $\langle P(S), \cup \rangle$ \times 否

5.2.1 群的基本概念

例：假设 $R = \{0, 60, 120, 180, 240, 300\}$ 表示平面几何上图形绕形心顺时针旋转的角度集合。

$*$ 是定义在 R 上的运算。定义如下：对任意的 $a, b \in R$ ， $a * b$ 表示图形顺时针旋转 a 角度，再顺时针旋转 b 角度得到的总旋转度数。并规定旋转 360 度等于原来的状态，即该运算是模 360 的。

整个运算可以用运算表表示。



5. 2. 1 群的基本概念

*	0	60	120	180	240	300
0	0	60	120	180	240	300
60	60	120	180	240	300	0
120	120	180	240	300	0	60
180	180	240	300	0	60	120
240	240	300	0	60	120	180
300	300	0	60	120	180	240

5.2.1 群的基本概念

设 $\langle R, * \rangle$ 是一代数系统，满足以下几点：

- (1) 运算 $*$ “顺时针旋转的角度”是封闭的
- (2) 运算 $*$ “顺时针旋转的角度”是可结合的
- (3) 存在单位元 $e=0$;
- (4) 对任意元素 a 都存在逆元 a^{-1} ;

*	0	60	120	180	240	300
0	0	60	120	180	240	300
60	60	120	180	240	300	0
120	120	180	240	300	0	60
180	180	240	300	0	60	120
240	240	300	0	60	120	180
300	300	0	60	120	180	240

$0*0=0$; $60*300=0$;

$120*240=0$; $180*180=0$

$0^{-1}=0$; $60^{-1}=300$; $120^{-1}=240$; $180^{-1}=180$

$\langle G, * \rangle$ 是一个群。 **$|G|=6$** ，六阶群

5.2.1 群的基本概念

例：**A**是非空集合， $F = \{f \mid f : A \rightarrow A\}$, 双射集

运算“ \circ ”是函数的复合运算，

则 $\langle F, \circ \rangle$ 是群

5.2.1 群的基本概念

例1： $A=\{1,2,3\}$

解： 双射的个数 **3!**， $F=\{f_1, f_2, f_3, f_4, f_5, f_6\}$,

$$\begin{aligned} f_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \\ f_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ f_5 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{aligned}$$

5.2.1 群的基本概念

\circ	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

$$f_2 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_6$$

$$f_3 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5$$

$$f_4 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

5.2.1 群的基本概念

\circ	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

(1) 运算是可结合的;

(2) 存在单位元 e ; $\mathbf{f1=I_A}$

(3) 对任意元素 a 都存在逆元 a^{-1} ;

f_1, f_2, f_3, f_4 自身为逆元, f_5, f_6 互为逆元

5.2.1 群的基本概念

一个群如果运算满足交换律，则称该群为交换群，或Abel群（阿贝尔）。

$$\forall a, b \in G \text{ 有 } \mathbf{a * b = b * a}$$



尼尔斯·亨利克·阿贝尔(**N.H.Abel**)**1802**年**8**月**5**日出生在挪威一个名叫芬德的小村庄。有七个兄弟姐妹，阿贝尔在家里排行第二。他父亲是村子里的穷牧师，母亲安妮是一个非常美丽的女人，她遗传给阿贝尔惊人的漂亮容貌。

勒让德、拉普拉斯、傅立叶、泊松、柯西。

5.2.1 群的基本概念

例 $\langle \mathbf{Z}_5, +_5 \rangle$ 是可交换群。 $\langle \mathbf{Z}_m, +_m \rangle$ 也是可交换群

$$(1) \forall [i], [j], [k] \in \mathbf{Z}_5$$

$$([i] +_5 [j]) +_5 [k] =$$
$$[i] +_5 ([j] +_5 [k]) =$$
$$[(i+j+k) \bmod 5]$$

$$(2) e = [0]$$

$$(3) \forall [i] \in \mathbf{Z}_5$$

$$[i]^{-1} = [-i] = [5-i]$$

$$(4) \forall [i], [j] \in \mathbf{Z}_5$$

$$[i] +_5 [j] = [j] +_5 [i] = [(i+j) \bmod 5]$$

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]



陪集, 拉格朗日定理

环, 域

正规子群

子群与元素周期

置换群

循环群

群

半群、独异点

代数系统

群小结 (1)

1、 $\langle G, * \rangle$ 是一代数系统，如果满足以下几点：

(1) 运算是可结合的；

(2) 存在单位元 e ；

(3) 对任意元素 a 都存在逆元 a^{-1} ；

则称 $\langle G, * \rangle$ 是一个群。 $|G|$ 表示群的阶，可以是有限也可以是无限

2、交换群，或**Abel**群（阿贝尔）一类特殊的群