判天地之美，析万物之理
—庄子

Cogito,ergo sum.
吾思故吾在
—René Descartes
—[法]笛卡尔

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

第二章 群论

November 20, 2006

wujunanhuiwuhu@gmail.com

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§1 群的概念

群的第一定义

定义 (第一定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G$;

群的第一定义

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义 (第一定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义 (第一定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) 封闭性: $\forall a, b \in G, ab \in G$;

(2) 结合律: $\forall a, b, c \in G, a(bc) = (ab)c$;

(3) $\forall a, b \in G$,方程

$$ax = b, \quad ya = b$$

都在G中有解,

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义 (第一定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

(3) $\forall a, b \in G,$*方程*

$$ax = b, \quad ya = b$$

都在G中有解,

*则称G关于该代数运算成为**群**.*

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

群的第二定义

定义（第二定义）

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

群的第二定义

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义 (第二定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G$;

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c$;

(3) *单位元:* $\exists e \in G, \ni \forall a \in G, ea = ae = a$;

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义 (第二定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

(3) *单位元:* $\exists e \in G, \ni \forall a \in G, ea = ae = a;$

(4) *逆元:* $\forall a \in G, \exists a^{-1} \in G, \ni aa^{-1} = a^{-1}a = e,$

群的第二定义

定义 (第二定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

(3) *单位元:* $\exists e \in G, \ni \forall a \in G, ea = ae = a;$

(4) *逆元:* $\forall a \in G, \exists a^{-1} \in G, \ni aa^{-1} = a^{-1}a = e,$

则称G关于该代数运算成为群.

群的第三定义

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义 (第三定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

群的第三定义

定义 (第三定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

(3) *左单位元:* $\exists e \in G, \ni \forall a \in G, ea = a;$

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义（第三定义）

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

(3) *左单位元:* $\exists e \in G, \ni \forall a \in G, ea = a;$

(4) *左逆元:* $\forall a \in G, \exists a^{-1} \in G, \ni a^{-1}a = e,$

群的第三定义

定义 (第三定义)

设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) *封闭性:* $\forall a, b \in G, ab \in G;$

(2) *结合律:* $\forall a, b, c \in G, a(bc) = (ab)c;$

(3) *左单位元:* $\exists e \in G, \ni \forall a \in G, ea = a;$

(4) *左逆元:* $\forall a \in G, \exists a^{-1} \in G, \ni a^{-1}a = e,$

*则称G关于该代数运算成为**群**.*

三个定义的等价性

这里给出了群的三个定义,实际上,这三个定义是等价的.

第二章 群论

群的概念

单位元逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

这里给出了群的三个定义,实际上,这三个定义是等价的.

第一定义⇒第二定义: 由$ax=a, ya=a$分别得解e_r, e_l.对$\forall b\in G, \exists c, d\in G \ni ac=b, da=b$,于是$e_lb=(e_la)c=ac=b, be_r=d(ae_r)=da=b$,所以$e_l=e_le_r=e_r\overset{\text{def}}{=}e$,且$\forall b\in G, eb=be=e$.再由$ax=e, ya=e$分别得解$a_r, a_l$,于是$a_l=a_le=a_l(aa_r)=(a_la)a_r=ea_r=a_r\overset{\text{def}}{=}a^{-1}$.

三个定义的等价性

这里给出了群的三个定义,实际上,这三个定义是等价的.

第一定义⇒第二定义: 由$ax = a, ya = a$分别得解e_r, e_l.对$\forall b \in G, \exists c, d \in G \ni ac = b, da = b$,于是$e_l b = (e_l a)c = ac = b, be_r = d(ae_r) = da = b$,所以$e_l = e_l e_r = e_r \overset{\text{def}}{=} e$,且$\forall b \in G, eb = be = e$.再由$ax = e, ya = e$分别得解$a_r, a_l$,于是$a_l = a_l e = a_l(aa_r) = (a_l a)a_r = ea_r = a_r \overset{\text{def}}{=} a^{-1}$.

第二定义⇒第三定义是自动的.

三个定义的等价性

这里给出了群的三个定义,实际上,这三个定义是等价的.

第一定义$\Rightarrow$第二定义: 由$ax=a, ya=a$分别得解e_r, e_l.对$\forall b\in G, \exists c, d\in G\ni ac=b, da=b$,于是$e_lb=(e_la)c=ac=b, be_r=d(ae_r)=da=b$,所以$e_l=e_le_r=e_r\overset{\text{def}}{=}e$,且$\forall b\in G, eb=be=e$.再由$ax=e, ya=e$分别得解$a_r, a_l$,于是$a_l=a_le=a_l(aa_r)=(a_la)a_r=ea_r=a_r\overset{\text{def}}{=}a^{-1}$.

第二定义$\Rightarrow$第三定义是自动的.

第三定义$\Rightarrow$第二定义: 由条件,$\forall a\in G, \exists a^{-1}\in G\ni a^{-1}a=e$,可知$\exists a'\in G\ni a'a^{-1}=e$,于是$aa^{-1}=e(aa^{-1})=(a'a^{-1})(aa^{-1})=a'((a^{-1}a)a^{-1})=a'a^{-1}=e$(即左逆元也为右逆元),所以$a=ea=(aa^{-1})a=a(a^{-1}a)=ae$(即左单位元也为右单位元).故对$\forall a, b\in G$,方程$ax=b, ya=b$分别有解$a^{-1}b, ba^{-1}$.

两个推论

定义

设G为群.

1. G中使$\forall a \in G$,均有$ea = ae = a$的元素e叫做G的单位元;

两个推论

定义

设G为群.

1. G中使$\forall a\in G$,均有$ea=ae=a$的元素e叫做G的单位元;
2. G中使$\forall a\in G$, 均有$ea=a$的元素e叫做G的左单位元;
3. G中使$\forall a\in G$, 均有$ae=a$的元素e叫做G的右单位元;

两个推论

定义

设G为群.

1 G中使$\forall a \in G$,均有$ea = ae = a$的元素e叫做G的单位元;
2 G中使$\forall a \in G$, 均有$ea = a$的元素e叫做G的左单位元;
3 G中使$\forall a \in G$, 均有$ae = a$的元素e叫做G的右单位元;
4 对$a \in G$,使$a'a = aa' = e$的元素a'叫做G的逆元,记为a^{-1};

第二章 群论
群的概念
单位元 逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义

设G为群.

1. G中使$\forall a \in G$,均有$ea = ae = a$的元素e叫做G的单位元;
2. G中使$\forall a \in G$, 均有$ea = a$的元素e叫做G的左单位元;
3. G中使$\forall a \in G$, 均有$ae = a$的元素e叫做G的右单位元;
4. 对$a \in G$,使$a'a = aa' = e$的元素a'叫做G的逆元,记为a^{-1};
5. 对$a \in G$,使$a'a = e$的元素a'叫做G的左逆元;
6. 对$a \in G$,使$aa' = e$的元素a'叫做G的右逆元.

第二章 群论
群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义

设G为群.

1. G中使$\forall a\in G$,均有$ea=ae=a$的元素e叫做G的单位元;
2. G中使$\forall a\in G$, 均有$ea=a$的元素e叫做G的左单位元;
3. G中使$\forall a\in G$, 均有$ae=a$的元素e叫做G的右单位元;
4. 对$a\in G$,使$a'a=aa'=e$的元素a'叫做G的逆元,记为a^{-1};
5. 对$a\in G$,使$a'a=e$的元素a'叫做G的左逆元;
6. 对$a\in G$,使$aa'=e$的元素a'叫做G的右逆元.

推论

群G的单位元是惟一的.

两个推论

定义

设G为群.

1. G中使$\forall a \in G$,均有$ea = ae = a$的元素e叫做G的单位元;
2. G中使$\forall a \in G$, 均有$ea = a$的元素e叫做G的左单位元;
3. G中使$\forall a \in G$, 均有$ae = a$的元素e叫做G的右单位元;
4. 对$a \in G$,使$a'a = aa' = e$的元素a'叫做G的逆元,记为a^{-1};
5. 对$a \in G$,使$a'a = e$的元素a'叫做G的左逆元;
6. 对$a \in G$,使$aa' = e$的元素a'叫做G的右逆元.

推论

群G的单位元是惟一的.

推论

设G为群,$a \in G$.a的逆元是惟一的.

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义

元素个数有限的群叫做有限群, 有限群G的元素个数称为这个群的阶,简记为$|G|$. 不是有限群的群叫做无限群.

几个概念

定义

元素个数有限的群叫做有限群, 有限群G的元素个数称为这个群的阶,简记为$|G|$. 不是有限群的群叫做无限群.

定义

设G为群,如果对$\forall a, b \in G$均有$ab = ba$,则称G为交换群(或$Abel$群).

几点说明

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

注

1 如果非空集合G上的二元运算满足群定义中的第一、二两个条件，则称G为半群.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

几点说明

注

1. 如果非空集合G上的二元运算满足群定义中的第一、二两个条件, 则称G为半群.
2. 将第三定义中的左改成右,可得群的又一等价定义.

几点说明

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

注

1. 如果非空集合G上的二元运算满足群定义中的第一、二两个条件, 则称G为半群.
2. 将第三定义中的左改成右,可得群的又一等价定义.
3. 将第三定义中的一个左改为右,不能得出群的定义.见

$$\begin{array}{c|cc} \circ & e & a \\ \hline e & e & a \\ a & e & a \end{array} \quad \text{或} \quad \begin{array}{c|cc} \circ & e & a \\ \hline e & e & e \\ a & a & a \end{array}.$$

几点说明

注

1 如果非空集合G上的二元运算满足群定义中的第一、二两个条件，则称G为半群.

2 将第三定义中的左改成右,可得群的又一等价定义.

3 将第三定义中的一个左改为右,不能得出群的定义.见

$$\begin{array}{c|cc} \circ & e & a \\ \hline e & e & a \\ a & e & a \end{array} \quad \text{或} \quad \begin{array}{c|cc} \circ & e & a \\ \hline e & e & e \\ a & a & a \end{array}.$$

4 由于群中的运算满足结合律,因此$a_1a_2\cdots a_n$是有意义的，通常记$\overbrace{aa\cdots a}^{n}$($n$为正整数)为$a^n$.

几点说明

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

注

5 群中元素a的逆元通常记为a^{-1}.且对任意整数m,n有

$$a^m \cdot a^n = a^{m+n}, (a^m)^n = a^{mn}.$$

几点说明

注

5 群中元素a的逆元通常记为a^{-1}.且对任意整数m, n有

$$a^m \cdot a^n = a^{m+n}, (a^m)^n = a^{mn}.$$

6 当群是加法群时,称逆元为负元,记a 的负元为$-a$;称单位元为零元,记为0.此时, 对任意整数m, n有

$$ma = \overbrace{a + a + \cdots + a}^{m},$$
$$0a \overset{\text{def}}{=} 0,$$
$$ma + na = (m+n)a, na + nb = n(a+b),$$
$$m(na) = (mn)a,$$
$$(-n)a = \overbrace{-a - a - \cdots - a}^{n} = -(\overbrace{a + a + \cdots + a}^{n}) = -(na).$$

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

群的几个例子

例

设$G=\{g\}$,乘法是$gg=g$.G关于这个乘法作成一个群.

群的几个例子

例

设$G = \{g\}$,乘法是$gg = g$.G关于这个乘法作成一个群.

例

设$G = \mathbb{Z}$,G关于通常的加法作成群,但G关于通常的乘法作成半群,不作成群.

群的几个例子

例

设$G=\{g\}$,乘法是$gg=g$.G关于这个乘法作成一个群.

例

设$G=\mathbb{Z}$,G关于通常的加法作成群,但G关于通常的乘法作成半群,不作成群.

例

设$G=\{0,1,2,3,4,5,6\}$,G中的运算为

$$i\circ j=\begin{cases} i+j, & 若 i+j\leq 6\\ i+j-6, & 若 i+j>6\end{cases}$$

则$(G,\circ)$作成一个群.这个群也记为$(\mathbb{Z}_7,+)$.

群的几个例子

例（上例的一般情形）

设$\mathbb{Z}_n$是模n的剩余类(即$\mathbb{Z}_n = \{[0],[1],\ldots,[n-1]\}$),定义$\mathbb{Z}_n$中的加法"+":$[i]+[j]=[i+j]$,则$(\mathbb{Z}_n,+)$ 成为一个群.

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例（上例的一般情形）

设$\mathbb{Z}_n$是模n的剩余类(即$\mathbb{Z}_n = \{[0],[1],\ldots,[n-1]\}$),定义$\mathbb{Z}_n$中的加法“+”:$[i]+[j]=[i+j]$,则$(\mathbb{Z}_n,+)$ 成为一个群.

例

设$\mathbb{Z}_7^* = \{[1],[2],[3],[4],[5],[6]\}$, $\mathbb{Z}_7^*$ 中的运算为

$$[i]\cdot[j]=[ij],$$

则$(\mathbb{Z}_7^*,\cdot)$作成一个群.

群的几个例子

例（上例的一般情形）

设$\mathbb{Z}_n$是模n的剩余类(即$\mathbb{Z}_n = \{[0],[1],\ldots,[n-1]\}$),定义$\mathbb{Z}_n$中的加法“+”:$[i]+[j]=[i+j]$,则$(\mathbb{Z}_n,+)$ 成为一个群.

例

设$\mathbb{Z}_7^* = \{[1],[2],[3],[4],[5],[6]\}$, $\mathbb{Z}_7^*$ 中的运算为

$$[i]\cdot[j]=[ij],$$

则$(\mathbb{Z}_7^*,\cdot)$作成一个群.

例

设$G=\mathbb{Z}$, G中的运算定义为$a\circ b=a+b-2$, $(G,\circ)$作成群.

群的几个例子

例

设F为数域,$M_n(F)$为数域F上的所有n阶矩阵的集合,则$M_n(F)$关于矩阵加法作成群,$M_n(F)$关于矩阵乘法不构成群.

群的几个例子

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

设F为数域,$M_n(F)$为数域F上的所有n阶矩阵的集合,则$M_n(F)$关于矩阵加法作成群,$M_n(F)$关于矩阵乘法不构成群.

例

设$GL_n(F)$为数域F上所有n阶可逆矩阵的集合,则$GL_n(F)$关于矩阵的乘法作成群.这个群叫做一般线性群.当$n>1$时, 这个群不是交换群.

群的几个例子

例

设F为数域,$M_n(F)$为数域F上的所有n阶矩阵的集合,则$M_n(F)$关于矩阵加法作成群,$M_n(F)$关于矩阵乘法不构成群.

例

设$GL_n(F)$为数域F上所有n阶可逆矩阵的集合,则$GL_n(F)$关于矩阵的乘法作成群.这个群叫做一般线性群.当$n>1$时,这个群不是交换群.

例

设$SL_n(F)$为数域F上所有行列式等于1的n阶矩阵的集合,则$GL_n(F)$关于矩阵的乘法作成群.这个群叫做特殊线性群.当$n>1$时,这个群也不是交换群.

练习

判断下列哪些代数体系是群,为什么?

1 $(\mathbb{Z},+)$; $(\mathbb{Z},\cdot)$;

2 $(\mathbb{Q},+)$; $(\mathbb{Q},\cdot)$; $(\mathbb{Q}^*,\cdot)$;

3 $(\mathbb{R},+)$; $(\mathbb{R},\cdot)$; $(\mathbb{R}^{\cdot},\cdot)$;

4 $(\mathbb{C},+)$; $(\mathbb{C},\cdot)$; $(\mathbb{C}^{\cdot},\cdot)$;

5 $(\mathbb{N},+)$; $(\mathbb{N},\cdot)$; $(\mathbb{N}^+,+)$; $(\mathbb{N}^+,\cdot)$;

6 $(M_n(F),+)$; $(M_n(F),\cdot)$; $(M_n(F)^*,\cdot)$;

7 $(\mathbb{R},\circ)$,其中运算为$x\circ y=x+y+c$, c为常数;

8 $(\mathbb{R}^*,\circ)$,其中运算为$x\circ y=xy/2$;

9 $(\mathbb{R}-\{-1\},\circ)$,其中运算为$x\circ y=x+y+xy$;

10 $(\{x \mid x\in\mathbb{R},-1<x<1\},\circ)$其中运算为$x\circ y=\dfrac{x+y}{xy+1}$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§2 单位元、逆元、削去律

元素的阶的定义

定义

设G为群,$a \in G$.使$a^m = e$的最小正整数m称为a的阶,记为$|a| = m$.如果这样的m不存在, 则称a的阶是无限的,记为$|a| = +\infty$.

元素的阶的定义

定义

设G为群,$a \in G$.使$a^m = e$的最小正整数m称为a的阶,记为$|a| = m$.如果这样的m不存在, 则称a的阶是无限的,记为$|a| = +\infty$.

例

群$(\mathbb{Z}_7^*, \cdot)$中,$|[1]| = 1, |[2]| = |[4]| = 3, |[3]| = |[5]| = 6, |[6]| = 2$.

元素的阶的定义

定义

设G为群,$a \in G$.使$a^m = e$的最小正整数m称为a的**阶**,记为$|a| = m$.如果这样的m不存在，则称a的阶是无限的,记为$|a| = +\infty$.

例

群$(\mathbb{Z}_7^*, \cdot)$中,$|[1]| = 1, |[2]| = |[4]| = 3, |[3]| = |[5]| = 6, |[6]| = 2.$

例

群$(\mathbb{Z}, +)$中,$|0| = 1, |n| = +\infty (n \neq 0).$

元素的阶的定义

第二章 群论

群的概念

单位元逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

定义

设G为群,$a \in G$.使$a^m = e$的最小正整数m称为a的阶,记为$|a| = m$.如果这样的m不存在, 则称a的阶是无限的,记为$|a| = +\infty$.

例

群$(\mathbb{Z}_7^*, \cdot)$中,$|[1]| = 1, |[2]| = |[4]| = 3, |[3]| = |[5]| = 6, |[6]| = 2.$

例

群$(\mathbb{Z}, +)$中,$|0| = 1, |n| = +\infty (n \neq 0).$

注

加法群G中,设$a \in G$, 能够使$ma = 0$的最小正整数m叫做a的阶,若这样的m不存在,则称a的阶是无限的,a的阶仍记为$|a|$.

消去律

例

设$G=\{\varepsilon_0,\varepsilon_1,\varepsilon_2\}$是$x^3=1$的三个复根的集合,$G$的运算是复数乘法,则$(G,\cdot)$作成一个群,且$|\varepsilon_0|=1,|\varepsilon_1|=|\varepsilon_2|=3.$

第二章 群论
群的概念
单位元 逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

设$G=\{\varepsilon_0,\varepsilon_1,\varepsilon_2\}$是$x^3=1$的三个复根的集合,$G$的运算是复数乘法,则$(G,\cdot)$作成一个群,且$|\varepsilon_0|=1,|\varepsilon_1|=|\varepsilon_2|=3.$

思考题

设$G=\{\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{n-1}\}$是$n$次单位根的集合,即$\varepsilon_k=\cos\dfrac{2k\pi}{n}+i\sin\dfrac{2k\pi}{n},k=0,1,\ldots,n-1$,则$G$关于复数乘法也构成群.元素$|\varepsilon_k|=$?

消去律

例

设$G=\{\varepsilon_0,\varepsilon_1,\varepsilon_2\}$是$x^3=1$的三个复根的集合,$G$的运算是复数乘法,则$(G,\cdot)$作成一个群,且$|\varepsilon_0|=1,|\varepsilon_1|=|\varepsilon_2|=3.$

思考题

设$G=\{\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{n-1}\}$是$n$次单位根的集合,即$\varepsilon_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n},k=0,1,\ldots,n-1$,则$G$关于复数乘法也构成群.元素$|\varepsilon_k|=$?

定理

每个群都适合消去律:

1. *左消去律* $ax=ax'\Rightarrow x=x'$;
2. *右消去律* $ya=y'a\Rightarrow y=y'$.

§3 有限群的另一定义

定理与定义

定理 (定理与定义)

设G是一个有限集,若$(G,\circ)$满足(1) 封闭性,(2) 结合律,(3) 消去律,那么$(G,\circ)$一定是一个群.

定理与定义

定理（定理与定义）

设G是一个有限集,若$(G,\circ)$满足(1) 封闭性,(2) 结合律,(3) 消去律,那么$(G,\circ)$一定是一个群.

证.

设$G=\{a_1,a_2,\ldots,a_n\}$,注意到对$\forall a_i\in G$有

$$\{a_ia_1,a_ia_2,\ldots,a_ia_n\}=G$$

即得. □

问题与性质

1 若$|G| = +\infty$,即使$(G,\circ)$能满足封闭性、结合律和消去律,$|G|$也不可能成为群.对吗?

2 设G是个有限半群,则G为群$\Leftrightarrow G$中消去律成立.

3 设G是群.

(1) $\forall a \in G$,若存在$n \in \mathbb{Z}^+$, 使$a^n = e$,则$|a| \leq n$;

(2) $\forall a \in G, |a| = |a^{-1}|$;

(3) $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$;

(4) $\forall a_1, a_2, \ldots, a_n \in G, (a_1a_2\cdots a_n)^{-1} = a_n^{-1}\cdots a_2^{-1}a_1^{-1}$;

(5) 在G中判断正误: $(i)\ x^2 = e \Rightarrow a = e$; $(ii)\ x^2 = a^2 \Rightarrow x = a$; $(iii)\ (ab)^2 = a^2b^2$; $(iv)\ x^2 = x \Rightarrow x = e$; $(v)\ a^k = e \Rightarrow |a| = k$;

(6) 在G中解关于x的方程: $(i)\ axb = c$; $(ii)\ x^2b = xa^{-1}c$; $(iii)\ (xax)^3 = bx$且$x^2a = (xa)^{-1}$; $(iv)\ ax^2 = b$且$x^3 = e$; $(v)\ x^2 = a^2$ 且$x^5 = e$;

4 如果G是有限群,则G的每个元素都是有限阶的.(其逆成立吗?为什么?)

有关群的元素的阶的几个结论

设G为.关于G的元素的阶有如下结论：

1 设$a \in G$,若$\exists m \in \mathbb{Z}^{+}, \ni a^{m}=e$,则$|a|=n<+\infty$且$n \mid m$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

有关群的元素的阶的几个结论

设G为.关于G的元素的阶有如下结论：

1 设$a \in G$,若$\exists m \in \mathbb{Z}^+, \ni a^m = e$,则$|a| = n < +\infty$且$n \mid m$.

2 设$a \in G$且$|a| = n$.则$\forall m \in \mathbb{Z}, a^m = e \Leftrightarrow n \mid m$.

有关群的元素的阶的几个结论

设G为.关于G的元素的阶有如下结论：

1 设$a \in G$,若$\exists m \in \mathbb{Z}^{+}, \ni a^m = e$,则$|a| = n < +\infty$且$n \mid m$.

2 设$a \in G$且$|a| = n$.则$\forall m \in \mathbb{Z}, a^m = e \Leftrightarrow n \mid m$.

3 设$a, b \in G$且$|a| = m, |b| = n, ab = ba$,记$g = [m, n]$,则

(1) $|ab| \mid g$;

(2) 若$(m, n) = 1$则$|ab| = g = mn$;

(3) 若$|a^k| = \dfrac{m}{(k, m)}$;

(4) 存在$d \in G \ni |d| = g$;

有关群的元素的阶的几个结论

设G为.关于G的元素的阶有如下结论：

1 设$a \in G$,若$\exists m \in \mathbb{Z}^+, \ni a^m = e$,则$|a| = n < +\infty$且$n \mid m$.

2 设$a \in G$且$|a| = n$.则$\forall m \in \mathbb{Z}, a^m = e \Leftrightarrow n \mid m$.

3 设$a, b \in G$且$|a| = m, |b| = n, ab = ba$,记$g = [m, n]$,则
  (1) $|ab| \mid g$;
  (2) 若$(m, n) = 1$则$|ab| = g = mn$;
  (3) 若$|a^k| = \dfrac{m}{(k, m)}$;
  (4) 存在$d \in G \ni |d| = g$;

4 若G为可换群,且G中存在阶最大的元素$a, |a| = m$,则$\forall b \in G, |b| \mid m$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§4 群的同态

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

一、 群同构

设$(G,\circ)$与$(\bar{G},\bar{\circ})$是两个群.如果存在双射$\varphi: G\to\bar{G}\ni\forall a,b\in G,\varphi(a\circ b)=\varphi(a)\bar{\circ}\varphi(b)$, 则称$\varphi$是**同构映射**, 并称$G$与$\bar{G}$同构,记为$G\cong\bar{G}$.对于同构的群,我们认为是代数相同的,因为它们除了符号与名称上的区别之外, 二者没有实质的差异.

一、 群同构

设$(G,\circ)$与$(\bar{G},\bar{\circ})$是两个群.如果存在双射$\varphi: G\rightarrow \bar{G}\ni \forall a,b\in G, \varphi(a\circ b)=\varphi(a)\bar{\circ}\varphi(b)$, 则称$\varphi$是同构映射, 并称$G$与$\bar{G}$同构,记为$G\cong \bar{G}$.对于同构的群,我们认为是代数相同的,因为它们除了符号与名称上的区别之外, 二者没有实质的差异.

性质

设$\varphi: G\rightarrow \bar{G}$是群的同构映射,则$\varphi^{-1}: \bar{G}\rightarrow G$ 也是群的同构映射.

第二章 群论

群的概念

单位元逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

一、 群同构

设$(G,\circ)$与$(\bar{G},\bar{\circ})$是两个群.如果存在双射$\varphi : G \to \bar{G} \ni \forall a,b \in G$, $\varphi(a\circ b) = \varphi(a)\bar{\circ}\varphi(b)$, 则称$\varphi$是同构映射, 并称$G$与$\bar{G}$同构,记为$G \cong \bar{G}$.对于同构的群,我们认为是代数相同的,因为它们除了符号与名称上的区别之外, 二者没有实质的差异.

性质

设$\varphi : G \to \bar{G}$是群的同构映射,则$\varphi^{-1} : \bar{G} \to G$ 也是群的同构映射.

性质

设$\varphi_1 : G_1 \to G_2, \varphi_2 : G_2 \to G_3$均为群的同构映射, 则$\varphi_2\varphi_1 : G_1 \to G_3$也是群的同构映射.

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

二、 群同态

设$(G,\circ)$与$(\bar{G},\bar{\circ})$是两个群.如果存在映射$\varphi: G \to \bar{G} \ni \forall a,b \in G, \varphi(a\circ b) = \varphi(a)\bar{\circ}\varphi(b)$, 则称$\varphi$是群**同态映射**; 如果$\varphi$是满射,则称$\varphi$是群满同态映射, 并称$G$与$\bar{G}$**同态**, 记为$G \sim \bar{G}$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

二、 群同态

设$(G,\circ)$与$(\bar{G},\bar{\circ})$是两个群.如果存在映射$\varphi: G\rightarrow\bar{G}\ni\forall a,b\in G, \varphi(a\circ b)=\varphi(a)\bar{\circ}\varphi(b)$，则称$\varphi$是群**同态映射**；如果$\varphi$是满射,则称$\varphi$是群满同态映射，并称$G$与$\bar{G}$**同态**，记为$G\sim\bar{G}$.

定理

设φ是$(G,\circ)$到$(\bar{G},\bar{\circ})$的同态满射.若$(G,\circ)$是群，则$(\bar{G},\bar{\circ})$也是群.

第二章 群论

群的概念

单位元逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

二、 群同态

设$(G,\circ)$与$(\bar{G},\bar{\circ})$是两个群.如果存在映射$\varphi: G\to\bar{G}\ni\forall a,b\in G,\varphi(a\circ b)=\varphi(a)\bar{\circ}\varphi(b)$, 则称$\varphi$是群**同态映射**; 如果$\varphi$是满射,则称$\varphi$是群满同态映射, 并称$G$与$\bar{G}$**同态**, 记为$G\sim\bar{G}$.

定理

设φ是$(G,\circ)$到$(\bar{G},\bar{\circ})$的同态满射.若$(G,\circ)$是群, 则$(\bar{G},\bar{\circ})$也是群.

注

本定理的逆是不成立的:令$G=\{$一切奇数$\}$,其运算为通常的乘法,$\bar{G}=\{e\}$ 是一个元素的群,$\varphi: G\to\bar{G}; n\mapsto e$是满同态,但$G$不是群.

例

设$A=\{a,b,c\}$, A的乘法为

$$
\begin{array}{c|ccc}
\cdot & a & b & c \\
\hline
a & a & b & c \\
b & b & c & a \\
c & c & a & b
\end{array}
$$

证明:A作成一个群.

群同态的一个应用

例

设$A=\{a,b,c\}$, A的乘法为

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

证明:A作成一个群.

分析:本题通过运算表也许能解决单位元和逆元问题,但结合律的检验相当麻烦. 证明思路是:设法找一个群G,使A是G的同态象.

群同态的一个应用

例

设$A=\{a,b,c\}$, A的乘法为

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

证明:A作成一个群.

分析:本题通过运算表也许能解决单位元和逆元问题,但结合律的检验相当麻烦. 证明思路是:设法找一个群G,使A是G的同态象.

证. $(\mathbb{Z},+)$是一个群,定义映射为

$$\varphi:\mathbb{Z}\to A;\quad n\mapsto\begin{cases} a,\text{若}n\equiv 0 \pmod 3;\\ b,\text{若}n\equiv 1 \pmod 3;\\ c,\text{若}n\equiv 2 \pmod 3.\end{cases}$$

群同态的一个应用

则φ为满射,且φ为同态:

(1) 当$m \equiv 0 \pmod 3, n \equiv 0 \pmod 3$时,$\varphi(m+n) = a = aa = \varphi(m)\varphi(n)$;

(2) 当$m \equiv 0 \pmod 3, n \equiv 1 \pmod 3$时,$\varphi(m+n) = b = ab = \varphi(m)\varphi(n)$;

(3) 当$m \equiv 0 \pmod 3, n \equiv 2 \pmod 3$时,$\varphi(m+n) = c = ac = \varphi(m)\varphi(n)$;

(4) 当$m \equiv 1 \pmod 3, n \equiv 1 \pmod 3$时,$\varphi(m+n) = c = bb = \varphi(m)\varphi(n)$;

(5) 当$m \equiv 1 \pmod 3, n \equiv 2 \pmod 3$时,$\varphi(m+n) = a = bc = \varphi(m)\varphi(n)$;

(6) 当$m \equiv 2 \pmod 3, n \equiv 2 \pmod 3$时,$\varphi(m+n) = b = cc = \varphi(m)\varphi(n)$.

所以,$\mathbb{Z}$与A同态,由定理,A是群. $\square$

群同态的基本性质

定理

设$\varphi : G \to \bar{G}$是群同态满射.则

(1) 若e是G的单位元,则$\varphi(e) = \bar{e}$是$\bar{G}$的单位元;

(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$.

群同态的基本性质

定理

设$\varphi: G \to \bar{G}$是群同态满射.则

(1) 若e是G的单位元,则$\varphi(e)=\bar{e}$是$\bar{G}$的单位元;

(2) $\varphi(a^{-1})=\varphi(a)^{-1}$.

注

设$\varphi: G \to \bar{G}$是两个代数系统的同态映射(未必是满射),上面两个定理就未必成立了.但我们可以考虑φ的象集合$\bar{\bar{G}}=\{\varphi(x) \mid \forall x \in G\}$,则$\varphi: G \to \bar{\bar{G}}$是同态满射,上面的定理又可以用了.

群同态的基本性质

定理

设$\varphi: G \to \bar{G}$是群同态满射.则

(1) 若e是G的单位元,则$\varphi(e)=\bar{e}$是$\bar{G}$的单位元;

(2) $\varphi(a^{-1})=\varphi(a)^{-1}$.

注

设$\varphi: G \to \bar{G}$是两个代数系统的同态映射(未必是满射),上面两个定理就未必成立了.但我们可以考虑φ的象集合$\bar{\bar{G}}=\{\varphi(x) \mid \forall x \in G\}$,则$\varphi: G \to \bar{\bar{G}}$是同态满射,上面的定理又可以用了.

定义

设G是 群.若φ是G到G自 身 的 同 态,则 称φ为G的 一 个**自 同 态**;若φ是G到G自身的同构, 则称φ为G的一个**自同构**.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

群的自同态与自同构的几个例子

例

设$G = F[x]$为多项式加法群,映射$\varphi : G \to G; (f(x)) \mapsto f'(x)$是$G$的自同态.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

设$G = F[x]$为多项式加法群,映射$\varphi : G \to G; (f(x)) \mapsto f'(x)$是$G$的自同态.

例

设G为群,G的自同态集合通常记为$End\ G$,则$End\ G$关于映射的复合作成一个幺半群.

例

设$G = F[x]$为多项式加法群,映射$\varphi : G \to G; (f(x)) \mapsto f'(x)$是$G$的自同态.

例

设G为群,G的自同态集合通常记为$End\ G$,则$End\ G$关于映射的复合作成一个幺半群.

例

设G为群,a为G的任一元素,则$\varphi_a : G \to G; x \mapsto axa^{-1}$是$G$的自同构,这个同构称为$G$的内自同构.

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

设G为群,G的所有自同构所组成的集合记为$Aut\ G$,则$Aut\ G$关于映射的复合作成一个群;G的所有内自同构所组成的集合记为$Inn\ G$,$Inn\ G$关于映射的复合也作成一个群.显然有

$$Inn\ G \subset Aut\ G \subset End\ G.$$

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

群的自同态与自同构的几个例子

例

设G为群,G的所有自同构所组成的集合记为$Aut\ G$,则$Aut\ G$关于映射的复合作成一个群;G的所有内自同构所组成的集合记为$Inn\ G$,$Inn\ G$关于映射的复合也作成一个群.显然有

$$Inn\ G \subset Aut\ G \subset End\ G.$$

例

设G为群,$\varphi: G \to G; x \mapsto x^{-1}$,则$\varphi$是自同构$\Leftrightarrow G$是$Abel$群.

作业

p. 35 1,2

p. 38 2,4

p. 44 习题

§5 变换群

代数体系的研究目标

研究一种代数体系就是要解决这种代数体系的下面三个问题：

代数体系的研究目标

研究一种代数体系就是要解决这种代数体系的下面三个问题:

1 存在问题;

代数体系的研究目标

研究一种代数体系就是要解决这种代数体系的下面三个问题:

1. 存在问题;
2. 数量问题

代数体系的研究目标

研究一种代数体系就是要解决这种代数体系的下面三个问题:

1. 存在问题;
2. 数量问题
3. 结构问题.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

代数体系的研究目标

研究一种代数体系就是要解决这种代数体系的下面三个问题:

1. 存在问题;
2. 数量问题
3. 结构问题.

如果这些问题都得到完满的解答就算达到了目的. 关于数量问题,指的是彼此不同构的代数体系的数量, 因为同构的代数体系抽象地看可以认为是相同的代数体系.

代数体系的研究目标

研究一种代数体系就是要解决这种代数体系的下面三个问题:

1. 存在问题;
2. 数量问题
3. 结构问题.

如果这些问题都得到完满的解答就算达到了目的. 关于数量问题,指的是彼此不同构的代数体系的数量, 因为同构的代数体系抽象地看可以认为是相同的代数体系.

凯莱定理告诉我们,如果将所有变换群都研究清楚了, 也就等于把所有群都研究清楚了.

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

一、集合A的变换和表示形式

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

一、集合A的变换和表示形式

先回顾一个定义:

定义

设$A \neq \emptyset$,若τ是A到A自己的映射,则称τ是A的一个变换.

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

一、集合A的变换和表示形式

先回顾一个定义:

定义

设$A \neq \emptyset$,若τ是A到A自己的映射,则称τ是A的一个变换.

注意

在表示形式方面,当$\tau : A \to B$是映射时,用“$\tau(a)$”表示a的象;当$\tau : A \to A$是变换时,使用“a^{τ}” 表示a的象.

如果τ_1, τ_2都是A的变换,$\tau_1\tau_2$还是A的变换,但是$\tau_1\tau_2(a) = \tau_1(\tau_2(a)), a^{\tau_1\tau_2} = (a^{\tau_1})^{\tau_2}$.

一个例子,恒等映射与变换

例

设$A=\{1,2\}$.

$$\tau_1: 1 \longrightarrow 1, 2 \longrightarrow 1 \quad (i.e.\ 1^{\tau_1}=1, 2^{\tau_1}=1)$$
$$\tau_2: 1 \longrightarrow 2, 2 \longrightarrow 2 \quad (i.e.\ 1^{\tau_2}=2, 2^{\tau_2}=2)$$
$$\tau_3: 1 \longrightarrow 1, 2 \longrightarrow 2 \quad (i.e.\ 1^{\tau_3}=1, 2^{\tau_3}=2)$$
$$\tau_4: 1 \longrightarrow 2, 2 \longrightarrow 1 \quad (i.e.\ 1^{\tau_4}=2, 2^{\tau_4}=1)$$

是A的所有变换.其中τ_3,τ_4是一一变换.

第二章
群论

群的概念

单位元逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

例

设$A=\{1,2\}$.

$$\tau_1:1\longrightarrow 1,2\longrightarrow 1\quad(i.e.\ 1^{\tau_1}=1,2^{\tau_1}=1)$$
$$\tau_2:1\longrightarrow 2,2\longrightarrow 2\quad(i.e.\ 1^{\tau_2}=2,2^{\tau_2}=2)$$
$$\tau_3:1\longrightarrow 1,2\longrightarrow 2\quad(i.e.\ 1^{\tau_3}=1,2^{\tau_3}=2)$$
$$\tau_4:1\longrightarrow 2,2\longrightarrow 1\quad(i.e.\ 1^{\tau_4}=2,2^{\tau_4}=1)$$

是A的所有变换.其中τ_3,τ_4是一一变换.

几个简单事实

在上面的例子中,容易验证:$\tau_1\tau_2=\tau_2$; $\tau_2\tau_4=\tau_1$; $\tau_3\tau_i=\tau_i=\tau_i\tau_3$.由$(a^\tau)^{\lambda\mu}=\{(a^\tau)^\lambda\}^\mu=(a^{\tau\lambda})^\mu$可知$\tau(\lambda\mu)=(\tau\lambda)\mu$.

一个例子,恒等映射与变换

例

设$A=\{1,2\}$.

$$\tau_1: 1 \longrightarrow 1, 2 \longrightarrow 1 \quad (i.e.\ 1^{\tau_1}=1, 2^{\tau_1}=1)$$
$$\tau_2: 1 \longrightarrow 2, 2 \longrightarrow 2 \quad (i.e.\ 1^{\tau_2}=2, 2^{\tau_2}=2)$$
$$\tau_3: 1 \longrightarrow 1, 2 \longrightarrow 2 \quad (i.e.\ 1^{\tau_3}=1, 2^{\tau_3}=2)$$
$$\tau_4: 1 \longrightarrow 2, 2 \longrightarrow 1 \quad (i.e.\ 1^{\tau_4}=2, 2^{\tau_4}=1)$$

是A的所有变换.其中τ_3, τ_4是一一变换.

几个简单事实

在上面的例子中,容易验证:$\tau_1\tau_2=\tau_2$; $\tau_2\tau_4=\tau_1$; $\tau_3\tau_i=\tau_i=\tau_i\tau_3$.由$(a^\tau)^{\lambda\mu}=\{(a^\tau)^\lambda\}^\mu=(a^{\tau\lambda})^\mu$可知$\tau(\lambda\mu)=(\tau\lambda)\mu$.

性质

设$A\neq\emptyset$, ε是A的恒等映射,则对A的任一变换τ, $\varepsilon\tau=\tau\varepsilon=\tau$.

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

二、变换群的概念和基本性质

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

二、变换群的概念和基本性质

设$A \neq \emptyset$, S为A的所有变换组成的集合,我们来考虑S的哪些元素能构成群的问题.对于上面的例子来说,由于$2^{\tau_i\tau_1} = 1$,所以τ_1不存在逆元素,因而S不构成群.

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

二、变换群的概念和基本性质

设$A \neq \emptyset$, S为A的所有变换组成的集合,我们来考虑S的哪些元素能构成群的问题.对于上面的例子来说,由于$2^{\tau_i\tau_1} = 1$,所以τ_1不存在逆元素,因而S不构成群.

S的某些子集G关于上面的乘法肯定能成为群,注意到群的元素都有逆元, 容易得到G作成群的一个必要条件:

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

二、变换群的概念和基本性质

设$A \neq \emptyset$, S为A的所有变换组成的集合,我们来考虑S的哪些元素能构成群的问题.对于上面的例子来说,由于$2^{\tau_i \tau_1} = 1$,所以τ_1不存在逆元素,因而S不构成群.

S的某些子集G关于上面的乘法肯定能成为群,注意到群的元素都有逆元, 容易得到G作成群的一个必要条件:

定理

假设G是集合A的若干个变换所成的集合,并且G包含恒等映射ε. 若G对于变换乘法作成一个群,则G只包含A的一一变换.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

二、变换群的概念和基本性质

设$A \neq \emptyset$, S为A的所有变换组成的集合,我们来考虑S的哪些元素能构成群的问题.对于上面的例子来说,由于$2^{\tau_i\tau_1} = 1$,所以τ_1不存在逆元素,因而S不构成群.

S的某些子集G关于上面的乘法肯定能成为群,注意到群的元素都有逆元, 容易得到G作成群的一个必要条件:

定理

假设G是集合A的若干个变换所成的集合,并且G包含恒等映射ε. 若G对于变换乘法作成一个群,则G只包含A的一一变换.

定义

*集合A的若干个双射作成的群叫做A的一个**变换群**.*

变换群的两个例子

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

变换群的存在性如何呢?下面我们给出相对于A来说"最大"的变换群.

变换群的两个例子

变换群的存在性如何呢?下面我们给出相对于A来说“最大”的变换群.

定理

非空集合A的所有一一变换作成一个变换群.

变换群的两个例子

变换群的存在性如何呢?下面我们给出相对于A来说“最大”的变换群.

定理

非空集合A的所有一一变换作成一个变换群.

例

设$A=\mathbb{R}^2, G=\{\tau_\theta \mid \tau_\theta$是绕原点逆时针转$\theta$角的旋转$\}$.则$G$作成一个变换群.但$G$显然不包含$A$的全部一一变换.

变换群的两个例子

变换群的存在性如何呢?下面我们给出相对于A来说“最大”的变换群.

定理

非空集合A的所有一一变换作成一个变换群.

例

设$A=\mathbb{R}^2, G=\{\tau_\theta \mid \tau_\theta$是绕原点逆时针转$\theta$角的旋转$\}$.则$G$作成一个变换群.但$G$显然不包含$A$的全部一一变换.

注

变换群也未必是交换群,例如仍设$A=\mathbb{R}^2$, G为A的全部一一变换组成的变换群,τ_1是A的一个平移变换,使$(0,0)^{\tau}_1=(1,0)$, τ_2是绕原点逆时针转$\pi/2$的旋转变换,则τ_1,τ_2都是A的一一变换,但$(0,0)^{\tau_1\tau_2}=(0,1)\neq(1,0)=(0,0)^{\tau_2\tau_1}$,即$\tau_1\tau_2\neq\tau_2\tau_1$.

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定理 (凯莱(Cayley)定理)

任何一个群都和一个变换群同构.

第二章 群论
群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定理 (凯莱(Cayley)定理)

任何一个群都和一个变换群同构.

证.

设$G=\{a,b,c,\dots\}$是一个群.$\forall x\in G$,规定G的一个变换$\tau_x: G\longrightarrow G; g\longmapsto gx=g^{\tau_x}$.则$\tau_x$ 是G的一一变换.

记由G的所有元所得到的G的一一变换所构成的集合为$\bar{G}$,即$\bar{G}=\{\tau_a,\tau_b,\tau_c,\dots\}$.则

$$\phi: G\longrightarrow \bar{G}; x\longmapsto \tau_x$$

是一一映射.且对$\forall g\in G$,

$$g^{\tau_{xy}}=g(xy)=(gx)y=(gx)^{\tau_y}=(g^{\tau_x})^{\tau_y}=g^{(\tau_x\tau_y)}$$

即$\tau_{xy}=\tau_x\tau_y$,所以是$G\overset{\phi}{\cong}\bar{G}$,而$G$是群,所以$\bar{G}$也是群. □

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

群论基本知识小结

一、群的定义.

第一定义

第二定义

第三定义

有限群的定义

群论基本知识小结

一、群的定义.

第一定义

第二定义

第三定义

有限群的定义

二、群的性质.

设G是一个群,则G

(1) G满足结合律;

(2) G满足消去律;

(3) G中有单位元e,且e是唯一的;

(4) $\forall a \in G, a$在G中必有逆元a^{-1},且a^{-1}是唯一的.

群论小结

群G可能发生的状况:

(1) G中的元素是有限的,此时称G是有限群.

(2) G中的元素个数是无限的,此时称G是无限群.

(3) 如果$\forall a, b \in G$,都有$ab = ba$,则称G是交换群.

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

群G可能发生的状况:

(1) G中的元素是有限的,此时称G是有限群.

(2) G中的元素个数是无限的,此时称G是无限群.

(3) 如果$\forall a, b \in G$,都有$ab = ba$,则称G是交换群.

三、群的阶和群元素的阶,以及这二个阶的联系

(1) 群G的阶=群G中所含元素的个数.

(2) 设$a \in G$.则a的阶=使"$a^k = e$"成立的最小自然数.记为$|a|$. 如果满足"$a^k = e$" 的自然数不存在,则称a的阶是无限的.

(3) $|G| < \infty \Rightarrow |a| < \infty, \forall a \in G$, 即:有限群的元素都是有限阶的.

问题:无限群的元素的阶是怎样的?

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

事实上,每个群都有有限阶的元素.譬如单位元.

无限群G中除e外,也许还有其他有限阶元素,如$(\mathbb{R}^*, \cdot)$除了单位元1外,-1也是有限阶元.

无限群G中除e外,其他元也可能都是无限阶的.如$(\mathbb{Z}, +)$除了单位元0外,其他元素是无限阶的.

无限群G中可能每个元素都是有限阶的,如$G = \{x | \exists n \in \mathbb{Z} \ni x^n = 1\}$关于复数乘法所构成的群.

(4) $|a| = 2 \Leftrightarrow a = a^{-1}$.

(5) 若$\forall a \in G$,都有$a^2 = e$,则G必是交换群.

四. 群元素阶的性质

(1) 设$|G| = n < \infty, A = \{a \in G \mid |a| = e\}, B = \{b \in G \mid |b| \geq 3\}$,则$|B|$是偶数,且$n$的奇偶与$|A|$的奇偶相反. ,

(2)与元素a的阶n的有关问题:

群论小结

- n是自然数,且是使等式“$a^n = e$”成立的最小者.
- 如果有自然数(整数)m使$a^m = e$,则$n|m$反之也成立.
- 元素$e = a^0, a = a^1, a^2, \ldots, a^{n-1}$是$n$个两两不等的元.
- 如果$a^r = a^k$,则$n \mid r - k$.
- $a = e \Leftrightarrow n = 1$.
- $|a| = |a^{-1}|$.
- $a^{n-r} = a^{-r}$.
- $|ab| = |ba|$.
- $|abc| = |cab| = |bca|$(可推广到k个元素相乘的情形).
- $\forall m \in \mathbb{Z}, \exists r(0 \leq m \leq n) \ni a^m = a^r$.
- 如果n是奇数,则$|a^2| = n$(可推广为若$(m, n) = 1$,则$|a^m| = n$)

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0) \in \mathbb{Z}, a^m \neq e.$
- $a^m = a^n \Rightarrow m = n.$
- $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$是无限个两两不同的元素.

第二章 群论

群的概念

单位元 逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0) \in \mathbb{Z}, a^m \neq e.$
- $a^m = a^n \Rightarrow m = n.$
- $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$是无限个两两不同的元素.

五、几个重要的群

第二章 群论

群的概念

单位元逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0) \in \mathbb{Z}, a^m \neq e.$
- $a^m = a^n \Rightarrow m = n.$
- $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$是无限个两两不同的元素.

五、几个重要的群

- 整数加群$(\mathbb{Z}, +)$.

群论小结

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0) \in \mathbb{Z}, a^m \neq e$.
- $a^m = a^n \Rightarrow m = n$.
- $\dots, a^{-2}, a^{-1}, e, a, a^2, \dots$是无限个两两不同的元素.

五、几个重要的群

- 整数加群$(\mathbb{Z}, +)$.
- 数字乘群$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$等.

第二章 群论
群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0) \in \mathbb{Z}, a^m \neq e$.
- $a^m = a^n \Rightarrow m = n$.
- $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$是无限个两两不同的元素.

五、几个重要的群

- 整数加群$(\mathbb{Z}, +)$.
- 数字乘群$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$等.
- 模n剩余类加群$(\mathbb{Z}_n, +)$.

第二章 群论
群的概念
单位元 逆元削 去律
有限群 的另一 定义
群的同 态
变换群
置换群
循环群
子群
子群的 陪集
不变子 群、商 群
同态与

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0)\in\mathbb{Z}, a^m\neq e$.
- $a^m=a^n\Rightarrow m=n$.
- $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$是无限个两两不同的元素.

五、几个重要的群

- 整数加群$(\mathbb{Z},+)$.
- 数字乘群$(\mathbb{Q}^*,\cdot),(\mathbb{R}^*,\cdot),(\mathbb{C}^*,\cdot)$等.
- 模n剩余类加群$(\mathbb{Z}_n,+)$.

练习:设G是一个幺半群(有单位元的半群),则G中所有有逆元的元作成的集合必是群.

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0) \in \mathbb{Z}, a^m \neq e.$
- $a^m = a^n \Rightarrow m = n.$
- $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$是无限个两两不同的元素.

五、几个重要的群

- 整数加群$(\mathbb{Z}, +)$.
- 数字乘群$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$等.
- 模n剩余类加群$(\mathbb{Z}_n, +)$.

练习:设G是一个幺半群(有单位元的半群),则G中所有有逆元的元作成的集合必是群.

六、群同态

问题: 若$A \sim \bar{A}$,当$\bar{A}$是群时,能保证A也是群吗?

问题: 对两个群$A, \bar{A}$,若$A \sim \bar{A}$, A中哪些性质不能“传递”给$\bar{A}$?

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0) \in \mathbb{Z}, a^m \neq e.$
- $a^m = a^n \Rightarrow m = n.$
- $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$是无限个两两不同的元素.

五、几个重要的群

- 整数加群$(\mathbb{Z}, +)$.
- 数字乘群$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$等.
- 模n剩余类加群$(\mathbb{Z}_n, +)$.

练习:设G是一个幺半群(有单位元的半群),则G中所有有逆元的元作成的集合必是群.

六、群同态

问题: 若$A \sim \bar{A}$,当$\bar{A}$是群时,能保证A也是群吗?

问题: 对两个群$A, \bar{A}$,若$A \sim \bar{A}$, A中哪些性质不能“传递”给$\bar{A}$?

七、变换群.

(Cayley定理) 任何一个群都能与某个变换群同构.

作业

p. 50 2,4,5

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§6 置换群

置换群的概念

置换群是现今所研究的一切抽象群的来源,是抽象代数创始人E.Galais(1811-1832)在证明次数大于四的一元代数方程不可能用根号求解时引进的. 置换群是一种特殊的变换群.或者说,置换群就是有限集上的变换群. 由于是定义在有限集上,故每个置换的表现形式,固有特点都是可揣测的.

置换群的概念

置换群是现今所研究的一切抽象群的来源,是抽象代数创始人E.Galais(1811-1832)在证明次数大于四的一元代数方程不可能用根号求解时引进的. 置换群是一种特殊的变换群.或者说,置换群就是有限集上的变换群. 由于是定义在有限集上,故每个置换的表现形式,固有特点都是可揣测的.

由Cayley定理可以知道:如把所有置换群研究清楚了,就等于把所有有限群都研究清楚了,但实际上,研究置换群并不比研究抽象群容易.所以,一般研究抽象群用的还是直接的方法,并且也不能一下子把所有群都找出来.因为问题太复杂了,人们的方法是将群分成若干类(即附加一定条件),比如有限群、无限群;变换群、非变换群等等.对每个群类进行研究以设法回答上述三个问题.可惜,人们能弄清的群当今只有少数几类(后面的循环群就是完全解决了的一类群)大多数还在等待人们去解决.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

置换群的概念

定义

一个有限集合A到自身的一个一一变换(双射)叫做A的一个置换.

有限集合A的若干个置换作成的群叫做置换群.

含有n个元素的有限群的全体置换作成的群,叫做n次对称群.这个群通常记为S_n.

置换群的概念

群的概念
单位元 逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义

一个有限集合A到自身的一个一一变换(双射)叫做A的一个置换.

有限集合A的若干个置换作成的群叫做置换群.

含有n个元素的有限群的全体置换作成的群,叫做n次对称群.这个群通常记为S_n.

由于n个元的置换有$n!$个,

置换群的概念

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义

一个有限集合A到自身的一个一一变换(双射)叫做A的一个置换.

有限集合A的若干个置换作成的群叫做置换群.

含有n个元素的有限群的全体置换作成的群,叫做n次对称群.这个群通常记为S_n.

由于n个元的置换有$n!$个,所以有

定理

$$|S_n| = n!.$$

置换的表示

设$A=\{a_1,a_2,a_3\}$,π是A的一个置换:$a_1^\pi=a_2,a_2^\pi=a_3,a_3^\pi=a_1$.由于我们只关心置换中元素之间的关系,而不在乎元素的具体形式. 故可视$A=\{1,2,3\}$,而π为:$1\mapsto 2, 2\mapsto 3, 3\mapsto 1$.即

$$\pi:\begin{array}{ccc}1&2&3\\ \downarrow&\downarrow&\downarrow\\ 2&3&1\end{array}\quad \text{或}\quad \pi=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

设$A=\{a_1,a_2,a_3\}$,π是A的一个置换:$a_1^\pi=a_2,a_2^\pi=a_3,a_3^\pi=a_1$.由于我们只关心置换中元素之间的关系,而不在乎元素的具体形式. 故可视$A=\{1,2,3\}$,而π为:$1\mapsto 2,2\mapsto 3,3\mapsto 1$.即

$$\pi:\begin{array}{ccc}1 & 2 & 3\\ \downarrow & \downarrow & \downarrow\\ 2 & 3 & 1\end{array}\quad \text{或}\quad \pi=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$

显然,用$\pi=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$来描述$A$的一个置换是方便的.当然,上面的置换还可以写为$\begin{pmatrix}2 & 3 & 1\\ 3 & 1 & 2\end{pmatrix},\begin{pmatrix}3 & 1 & 2\\ 1 & 2 & 3\end{pmatrix},\ldots$.但习惯上都将第一行按自然序列排写, 这就可以让我们统一在一种表示置换的方法内进行工作了.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

置换的乘积

3次对称群有6个元素,$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in$ S_3,分别计算$i^{\pi\tau}, i^{\tau\pi}$得到

$$\pi\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ & & \end{pmatrix}$$

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

置换的乘积

3次对称群有6个元素,$\pi=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\tau=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\in S_3$,分别计算$i^{\pi\tau},i^{\tau\pi}$得到

$$\pi\tau=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&&\end{pmatrix}$$

置换的乘积

3次对称群有6个元素,$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$,分别计算$i^{\pi\tau}, i^{\tau\pi}$得到

$$\pi\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & \end{pmatrix}$$

第二章 群论
群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

3次对称群有6个元素,$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$,分别计算$i^{\pi\tau}, i^{\tau\pi}$得到

$$\pi\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

3次对称群有6个元素,$\pi=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\tau=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\in S_3$,分别计算$i^{\pi\tau},i^{\tau\pi}$得到

$$\pi\tau=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$\tau\pi=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\left(\begin{matrix}1&2&3\\ & & \end{matrix}\right.$$

置换的乘积

3次对称群有6个元素,$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$,分别计算$i^{\pi\tau}, i^{\tau\pi}$得到

$$\pi\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\tau\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & & \end{pmatrix}$$

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

置换的乘积

3次对称群有6个元素,$\pi=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\tau=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\in S_3$,分别计算$i^{\pi\tau},i^{\tau\pi}$得到

$$\pi\tau=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$\tau\pi=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\left(\begin{matrix}1&2&3\\3&1&\end{matrix}\right.$$

置换的乘积

3次对称群有6个元素,$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$,分别计算$i^{\pi\tau}, i^{\tau\pi}$得到

$$\pi\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\tau\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

所以,$\pi\tau \neq \tau\pi$.因此,S_3不是交换群.以后我们将知道,这是元素个数最少的非交换群.

置换的乘积

3次对称群有6个元素,$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in$ S_3,分别计算$i^{\pi\tau}, i^{\tau\pi}$得到

$$\pi\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\tau\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

所以,$\pi\tau \neq \tau\pi$.因此,S_3不是交换群.以后我们将知道,这是元素个数最少的非交换群.

注意

置换乘积中,是从左到右求变换值,这是与过去的习惯方法不同的.

循环置换的概念

前面已经引入了置换的记法,下面再介绍一种记法.设有8元置换$\pi=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 6 & 2 & 5 & 1 & 7 & 8 \end{pmatrix}$,$\pi$使$1 \to 4 \to 2 \to 3 \to 6 \to 1$,而其它元素保持不变.若将不发生改变的文字都删掉,那么上述置换可写成循环置换的形式:$\pi=(14236)$.一般地,

循环置换的概念

前面已经引入了置换的记法,下面再介绍一种记法.设有8元置换$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 6 & 2 & 5 & 1 & 7 & 8 \end{pmatrix}$,$\pi$使$1 \to 4 \to 2 \to 3 \to 6 \to 1$,而其它元素保持不变.若将不发生改变的文字都删掉,那么上述置换可写成循环置换的形式:$\pi = (14236)$.一般地,

定义

S_n的一个把A中i_1变到i_2, i_2变到i_3, $\ldots$, i_k变到i_1,而使A中其余元素不变的置换,叫做一个k-循环置换.这样的置换用符号

$$(i_1 i_2 \cdots i_k), (i_2 i_3 \cdots i_k i_1), \cdots, (i_k i_1 \cdots i_{k-1})$$

来表示.

如果S_n的两个循环置换π, τ没有共同的文字,则称这两个循环置换是不相连的

循环置换与置换的分解

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

注

- 循环置换是置换的另一种表达形式,它以发生变化的文字的变化次序为序, 表达成轮换的形式.虽然表达形式简捷,但所含置换的原有文字的数目可能反映不出来. 这要求事先予以说明.例如.“8元置换$\pi = (14236)$.”

循环置换与置换的分解

注

- 循环置换是置换的另一种表达形式,它以发生变化的文字的变化次序为序, 表达成轮换的形式.虽然表达形式简捷,但所含置换的原有文字的数目可能反映不出来. 这要求事先予以说明.例如.“8元置换$\pi = (14236)$.”
- 每个循环的表达方法一般不唯一,如$(i_1 i_2 \cdots i_k) = (i_2 i_3 \cdots i_k i_1) = \cdots = (i_k i_1 \cdots i_{k-1})$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

注

- 循环置换是置换的另一种表达形式,它以发生变化的文字的变化次序为序, 表达成轮换的形式.虽然表达形式简捷,但所含置换的原有文字的数目可能反映不出来. 这要求事先予以说明.例如.“8元置换$\pi = (14236)$.”
- 每个循环的表达方法一般不唯一,如$(i_1 i_2 \cdots i_k) = (i_2 i_3 \cdots i_k i_1) = \cdots = (i_k i_1 \cdots i_{k-1})$.
- S_8的单位(恒等置换)$\pi_0 = (1) = (2) = \cdots = (8)$,习惯写成$\pi_0 = (1)$.

循环置换与置换的分解

注

- 循环置换是置换的另一种表达形式,它以发生变化的文字的变化次序为序, 表达成轮换的形式.虽然表达形式简捷,但所含置换的原有文字的数目可能反映不出来. 这要求事先予以说明.例如.“8元置换$\pi=(14236)$.”
- 每个循环的表达方法一般不唯一,如$(i_1i_2\cdots i_k)=(i_2i_3\cdots i_ki_1)=\cdots=(i_ki_1\cdots i_{k-1})$.
- S_8的单位(恒等置换)$\pi_0=(1)=(2)=\cdots=(8)$,习惯写成$\pi_0=(1)$.

定理 (循环置换分解定理)

每一个n元置换π都可以写成若干个不相连的循环置换的乘积.

证

对π变动的元素个数进行归纳.如果π使任何元素都不变动,则$\pi = (1)$,结论成立.

假设对于最多变动$r-1(r \leq n)$个元的π定理是对的,则对变动r 个元的π,任取一个被π变动的元i_1,从i_1出发找i_1的象i_2, i_2 的象$i_3, \cdots$,直到找到一个i_k为止,i_k的象不再是一个新的元,而是我们已经得到的一个元:$i_k^\pi = i_j, j \leq k$.因为$i_j(2 \leq j \leq k)$是i_{j-1}的象, 所以$i_k^\pi = i_1$,即

$$i_1 \to i_2 \to \cdots \to i_k \to i_1.$$

因为π只使r个元变动,$k \leq r$.如果$k = r$,则π本身就是一个k-循环置换,结论成立.假设$k < r$,则

循环置换与置换的分解

$$
\begin{aligned}
\pi &= \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i'_{k+1} & \cdots & i'_r & i_{r+1} & \cdots & i_n \end{pmatrix} \\
&= \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \end{pmatrix} \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_1 & i_2 & \cdots & i_k & i'_{k+1} & \cdots & i'_r & i_{r+1} & \cdots & i_n \end{pmatrix} \\
&= (i_1 i_2 \cdots i_k)\pi_1
\end{aligned}
$$

但π_1只使$r-k<r$个元变动,由归纳假设,可以写成不相连的循环置换的乘积: $\pi_1=\eta_1\eta_2\cdots\eta_m$.

还需要说明:π_1中的所有循环置换$\eta_1,\ldots,\eta_m$中不可能再出现$i_1,\ldots,i_k$.否则,若$\eta_t=(\cdots i_p i_q\cdots),p\le k$,由于$\eta_1,\ldots,\eta_m$不相连,所以$i_p$只在$\eta_t$中出现,于是$i_p^{\pi_1}=i_q$,这与$\pi_1$使$i_p$不动相矛盾.所以

循环置换与置换的分解

$$\pi = (i_1 i_2 \cdots i_k)\eta_1 \cdots \eta_m$$

是不相连的循环置换的乘积. $\square$

循环置换与置换的分解

$$\pi = (i_1 i_2 \cdots i_k)\eta_1 \cdots \eta_m$$

是不相连的循环置换的乘积. □

把置换写成不相连的循环置换的乘积是表示置换的又一方法.

循环置换与置换的分解

$$\pi = (i_1 i_2 \cdots i_k)\eta_1 \cdots \eta_m$$

是不相连的循环置换的乘积. □

把置换写成不相连的循环置换的乘积是表示置换的又一方法.

由Caylay定理立得

定理

每一个有限群都与一个置换群同构.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

$$\pi = (i_1 i_2 \cdots i_k)\eta_1 \cdots \eta_m$$

是不相连的循环置换的乘积. □

把置换写成不相连的循环置换的乘积是表示置换的又一方法.

由Caylay定理立得

定理

每一个有限群都与一个置换群同构.

定义

每个2-循环置换叫做一个对换.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

循环置换的性质

性质

k-循环置换$(i_1 i_2 \cdots i_k)$的阶是k.

循环置换的性质

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

性质

k-循环置换$(i_1 i_2 \cdots i_k)$的阶是k.

性质

循环置换$\pi = (i_1 i_2 \cdots i_k)$的逆置换是$\pi^{-1} = (i_k i_{k-1} \cdots i_1)$.

循环置换的性质

性质

k-循环置换$(i_1 i_2 \cdots i_k)$的阶是k.

性质

循环置换$\pi = (i_1 i_2 \cdots i_k)$的逆置换是$\pi^{-1} = (i_k i_{k-1} \cdots i_1)$.

性质

两个不相连的循环置换可以交换.

循环置换的性质

性质

k-循环置换$(i_1i_2\cdots i_k)$的阶是k.

性质

循环置换$\pi=(i_1i_2\cdots i_k)$的逆置换是$\pi^{-1}=(i_ki_{k-1}\cdots i_1)$.

性质

两个不相连的循环置换可以交换.

性质

$$\begin{aligned}(i_1i_2\cdots i_k) &= (i_1i_2)(i_1i_3)\cdots(i_1i_k)\\ &= (i_1i_k)(i_2i_k)\cdots(i_{k-1}i_k).\end{aligned}$$

循环置换的性质

性质

k-循环置换$(i_1 i_2 \cdots i_k)$的阶是k.

性质

循环置换$\pi = (i_1 i_2 \cdots i_k)$的逆置换是$\pi^{-1} = (i_k i_{k-1} \cdots i_1)$.

性质

两个不相连的循环置换可以交换.

性质

$$
\begin{aligned}
(i_1 i_2 \cdots i_k) &= (i_1 i_2)(i_1 i_3)\cdots(i_1 i_k) \\
&= (i_1 i_k)(i_2 i_k)\cdots(i_{k-1} i_k).
\end{aligned}
$$

于是有

循环置换的性质

性质

每个n元置换都能表示成若干个对换的乘积.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

循环置换的性质

性质

每个n元置换都能表示成若干个对换的乘积.

性质

设$j \notin \{i_1, i_2, \ldots, i_k\}$,则$(i_1 i_2 \cdots i_k) = (j i_1 i_2 \cdots i_k)(j i_1)$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

循环置换的性质

性质

每个n元置换都能表示成若干个对换的乘积.

性质

设$j \notin \{i_1, i_2, \ldots, i_k\}$,则$(i_1 i_2 \cdots i_k) = (j i_1 i_2 \cdots i_k)(j i_1)$.

性质

任意一个置换表成对换之积时,表示式中对换个数的奇偶性不变.

循环置换的性质

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

性质

每个n元置换都能表示成若干个对换的乘积.

性质

设$j \notin \{i_1, i_2, \ldots, i_k\}$,则$(i_1 i_2 \cdots i_k) = (j i_1 i_2 \cdots i_k)(j i_1)$.

性质

任意一个置换表成对换之积时,表示式中对换个数的奇偶性不变.

定义

一个置换π叫做偶(奇)置换 $\Leftrightarrow$ π可以表成偶(奇)数个对换之积.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

循环置换的性质

性质

一个k-循环置换π是偶(奇)置换$\Leftrightarrow$ k为奇(偶)数.

循环置换的性质

性质

一个k-循环置换π是偶(奇)置换$\Leftrightarrow$ k为奇(偶)数.

定义

n次对称群S_n中全部偶置换组成的集合A_n构成一个群,叫做n次交错群. 并且有$|A_n| = \dfrac{1}{2}|S_n| = \dfrac{n!}{2}$.

作业

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

P. 55 1,3,4

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§7 循环群

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

整数加群$(\mathbb{Z},+)$中每个元素都是1的倍数.

循环群的概念

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

整数加群$(\mathbb{Z},+)$中每个元素都是1的倍数.

例

模n的剩余类加群$(\mathbb{Z}_n,+)$中每个元素都是$1([1])$的倍数.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

循环群的概念

例

整数加群$(\mathbb{Z},+)$中每个元素都是1的倍数.

例

模n的剩余类加群$(\mathbb{Z}_n,+)$中每个元素都是$1([1])$的倍数.

以上两个例子都说明群中有一个特殊的元素,使得其余元素都是这个元素的倍数(因为是加群,所以用倍数,如果是乘法群,则是方幂.以下用乘法群为例).一般地,

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

循环群的概念

例

整数加群$(\mathbb{Z},+)$中每个元素都是1的倍数.

例

模n的剩余类加群$(\mathbb{Z}_n,+)$中每个元素都是1([1])的倍数.

以上两个例子都说明群中有一个特殊的元素,使得其余元素都是这个元素的倍数(因为是加群,所以用倍数,如果是乘法群,则是方幂.以下用乘法群为例).一般地,

定义

*设G是一个(乘法)群,如果G中有一个元素a,使G中每个元素都是a的乘方,即$G=\{a^m|m\in Z\}$,则称G为**循环群**;也称G是由a所生成的,记为$G=(a)$.a叫做G的一个**生成元**.*

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

设G是一个群,a是G的生成元.则有

引理

$$|G| = |a|.$$

事实上,

(1) 若$|a| = \infty$,则$G =$

设G是一个群,a是G的生成元.则有

引理

$$|G| = |a|.$$

事实上,

(1) 若$|a| = \infty$,则$G = (\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots)$.

(2) 若$|a| = n < \infty$,则$G =$

第二章 群论
群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

设G是一个群,a是G的生成元.则有

引理

$$|G| = |a|.$$

事实上,

(1) 若$|a| = \infty$,则$G = (\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots)$.

(2) 若$|a| = n < \infty$,则$G = (e, a, a^2, \cdots, a^{n-1})$.

循环群的结构定理

设G是一个群,a是G的生成元.则有

引理

$$|G| = |a|.$$

事实上,

(1) 若$|a| = \infty$,则$G = (\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots)$.

(2) 若$|a| = n < \infty$,则$G = (e, a, a^2, \cdots, a^{n-1})$.

所以有

引理

设$G = (a)$,则:(1) G是无限循环群$\Leftrightarrow |a| = \infty$; (2) G是n阶循环群$\Leftrightarrow |a| = n$.

第二章 群论

群的概念
单位元 逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

考察

$$\begin{array}{ccccccccc} G & = & (\cdots, & a^{-2}, & a^{-1}, & e, & a^{1}, & a^{2}, & \cdots) \\ & & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \mathbb{Z} & = & (\cdots, & -2, & -1, & 0, & 1, & 2, & \cdots) \end{array}$$

与

$$\begin{array}{cccccccc} G & = & (e, & a, & a^{2}, & \cdots, & a^{n-1}) \\ & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ \mathbb{Z}_n & = & (0, & 1, & 2, & \cdots, & n-1) \end{array}$$

我们有

定理（循环群的结构定理）

设G是由a生成的循环群，

(1) *如果$|a| = \infty$,则$G \cong \mathbb{Z}$.*

(2) *如果$|a| = n < \infty$,则$G \cong \mathbb{Z}_n$.*

群的概念
单位元 逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

循环群的生成元

上面的定理说明,在同构的意义下,循环群只有两个:$\mathbb{Z}, \mathbb{Z}_n$.我们可以把循环群研究得更透彻一些.

很显然,$\mathbb{Z}$有且仅有两个生成元,而$\mathbb{Z}_n$的生成元就要复杂一些.我们再回到$G=(a), |G|=|a|=n$上来,若$b\in G \ni G=(b)$,则只需$|b|=n$ 就可以了,所以

$$b=a^k\text{是}G\text{的生成元}\Leftrightarrow (k,n)=1.$$

例如,$n=6$时,$G=(e,a,a^1,a^2,a^3,a^4,a^5), a, a^5$都是$G$的生成元,而$e, a^2, a^3, a^4$不是$G$的生成元.

循环群的生成元

上面的定理说明,在同构的意义下,循环群只有两个:$\mathbb{Z}, \mathbb{Z}_n$.我们可以把循环群研究得更透彻一些.

很显然,$\mathbb{Z}$有且仅有两个生成元,而$\mathbb{Z}_n$的生成元就要复杂一些.我们再回到$G=(a), |G|=|a|=n$上来,若$b\in G \ni G=(b)$,则只需$|b|=n$ 就可以了,所以

$$b=a^k\text{是}G\text{的生成元}\Leftrightarrow (k,n)=1.$$

例如,$n=6$时,$G=(e,a,a^1,a^2,a^3,a^4,a^5), a, a^5$都是$G$的生成元,而$e,a^2,a^3,a^4$不是$G$的生成元.

定义

设n为正整数,称$\varphi(n)$(=不超过n且与n互素的正整数的个数)为欧拉函数.

第二章 群论
群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

上面的定理说明,在同构的意义下,循环群只有两个:$\mathbb{Z},\mathbb{Z}_n$.我们可以把循环群研究得更透彻一些.

很显然,$\mathbb{Z}$有且仅有两个生成元,而$\mathbb{Z}_n$的生成元就要复杂一些.我们再回到$G=(a),|G|=|a|=n$上来,若$b\in G\ni G=(b)$,则只需$|b|=n$ 就可以了,所以

$$b=a^k\text{是}G\text{的生成元}\Leftrightarrow (k,n)=1.$$

例如,$n=6$时,$G=(e,a,a^1,a^2,a^3,a^4,a^5)$, a,a^5都是G的生成元,而e,a^2,a^3,a^4不是G的生成元.

定义

设n为正整数,称$\varphi(n)$(=不超过n且与n互素的正整数的个数)为欧拉函数.

推论

$\mathbb{Z}_n$有$\varphi(n)$个生成元.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§8 子群

子群的定义

定义

设G是一个群,$H(\neq \emptyset) \subseteq G$,如果$H$对于$G$的运算来说也作成群,则称$H$是$G$的一个子群.记为$H \leq G$.

子群的定义

定义

设G是一个群,$H(\neq \emptyset) \subseteq G$,如果$H$对于$G$的运算来说也作成群,则称$H$是$G$的一个子群.记为$H \leq G$.

例

设G为群,则$G \leq G$, $(e) \leq G$.这两个群称为G的平凡子群.

子群的定义

定义

设G是一个群,$H(\neq\emptyset)\subseteq G$,如果$H$对于$G$的运算来说也作成群,则称$H$是$G$的一个子群.记为$H\leq G$.

例

设G为群,则$G\leq G,(e)\leq G$.这两个群称为G的平凡子群.

例

设$G=S_3$,则$H=((1),(12))$是G的一个非平凡子群.

子群的定义

定义

设G是一个群,$H(\neq \emptyset) \subseteq G$,如果$H$对于$G$的运算来说也作成群,则称$H$是$G$的一个子群.记为$H \leq G$.

例

设G为群,则$G \leq G, (e) \leq G$.这两个群称为G的平凡子群.

例

设$G = S_3$,则$H = ((1),(12))$是G的一个非平凡子群.

例

$SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

子群的判定

定理（子群的判定定理1）

设G为群,$H(\neq \emptyset) \subseteq G$.则

$$H \leq G \Leftrightarrow \begin{cases} (1)\ a, b \in H \Rightarrow ab \in H; \\ (2)\ a \in H \Rightarrow a^{-1} \in H. \end{cases}$$

子群的判定

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定理（子群的判定定理1）

设G为群,$H(\neq \emptyset) \subseteq G$.则

$$H \leq G \Leftrightarrow \begin{cases} (1)\ a, b \in H \Rightarrow ab \in H; \\ (2)\ a \in H \Rightarrow a^{-1} \in H. \end{cases}$$

推论

设$H \leq G$,则H的单位元就是G的单位元,H中元a在H中的逆元就是a在G中的逆元.

子群的判定

定理（子群的判定定理1）

设G为群,$H(\neq \emptyset) \subseteq G$.则

$$H \leq G \Leftrightarrow \begin{cases} (1)\ a, b \in H \Rightarrow ab \in H; \\ (2)\ a \in H \Rightarrow a^{-1} \in H. \end{cases}$$

推论

设$H \leq G$,则H的单位元就是G的单位元,H中元a在H中的逆元就是a在G中的逆元.

判定定理1中的两个条件可以简化为一个条件:

子群的判定

定理（子群的判定定理1）

设G为群,$H(\neq \emptyset) \subseteq G$.则

$$H \leq G \Leftrightarrow \begin{cases} (1)\ a, b \in H \Rightarrow ab \in H; \\ (2)\ a \in H \Rightarrow a^{-1} \in H. \end{cases}$$

推论

设$H \leq G$,则H的单位元就是G的单位元,H中元a在H中的逆元就是a在G中的逆元.

判定定理1中的两个条件可以简化为一个条件:

定理（子群的判定定理2）

设G为群,$H(\neq \emptyset) \subseteq G$.则

$$H \leq G \Leftrightarrow \text{“}a, b \in H \Rightarrow ab^{-1} \in H\text{”}.$$

子群的判定

定理 (有限子群的判定定理)

设G为群,$H(\neq \emptyset) \subseteq G$,且$H$是有限集.则

$$H \leq G \Leftrightarrow \text{“}a, b \in H \Rightarrow ab \in H.$$

子群的判定

定理 (有限子群的判定定理)

设G为群,$H(\neq \emptyset) \subseteq G$,且$H$是有限集.则

$$H \leq G \Leftrightarrow \text{“}a, b \in H \Rightarrow ab \in H.$$

例

任一群不可能是两个真子群的并.

子群的判定

定理（有限子群的判定定理）

设G为群,$H(\neq \emptyset) \subseteq G$,且$H$是有限集.则
$$H \leq G \Leftrightarrow \text{“}a, b \in H \Rightarrow ab \in H.$$

例

任一群不可能是两个真子群的并.

例

设$K_4 = ((1), (12)(34), (13)(24), (14)(23))$,则$K_4 \leq S_4$.且$H_1 = ((1), (12)(34))$, $H_2 = ((1), (13)(24))$, $H_3 = ((1), (14)(23))$都是K_4的真子群，直接验证知$K_4 = H_1 \cup H_2 \cup H_3$.

子群的判定

定理（有限子群的判定定理）

设G为群,$H(\neq \emptyset) \subseteq G$,且$H$是有限集.则

$$H \leq G \Leftrightarrow \text{“}a, b \in H \Rightarrow ab \in H.$$

例

任一群不可能是两个真子群的并.

例

设$K_4 = ((1),(12)(34),(13)(24),(14)(23))$,则$K_4 \leq S_4$.且$H_1 = ((1),(12)(34))$, $H_2 = ((1),(13)(24))$, $H_3 = ((1),(14)(23))$都是K_4的真子群，直接验证知$K_4 = H_1 \cup H_2 \cup H_3$.

例

设$G = S_3, H_1 = ((1),(12)), H_2 = ((1),(13)), H_3 = ((1),(23)), H_4 = ((1),(123),(132))$,则$H_i$都是$G$的真子群,且$S_3 = H_1 \cup H_2 \cup H_3 \cup H_4$.

生成子群

对于群G的非空子集S,未必有$S \leq G$.但

$$K = \{a_1^{r_1} a_2^{r_2} \cdots a_m^{r_m} \mid a_i \in S, r_i = \pm 1, m \in \mathbb{N}, 1 \leq i \leq m\} \leq G.$$

并且K是G的含S的最小的子群,称K为由S生成的子群,记为$K = (S)$,称S为K的生成集.当$S = \{a_1, \ldots, a_n\}$为有限集合时,称$K = (a_1, \ldots, a_n)$为有限生成的, 当$S = \{a\}$只有一个元素时,称$K = (a)$为循环群(这正是我们前面所讨论的). 如果$S \leq G$,则$S = (S)$.

生成子群

对于群G的非空子集S,未必有$S \leq G$.但

$$K = \{a_1^{r_1} a_2^{r_2} \cdots a_m^{r_m} \mid a_i \in S, r_i = \pm 1, m \in \mathbb{N}, 1 \leq i \leq m\} \leq G.$$

并且K是G的含S的最小的子群,称K为由S生成的子群,记为$K = (S)$,称S为K的生成集.当$S = \{a_1, \ldots, a_n\}$为有限集合时,称$K = (a_1, \ldots, a_n)$为有限生成的, 当$S = \{a\}$只有一个元素时,称$K = (a)$为循环群(这正是我们前面所讨论的). 如果$S \leq G$,则$S = (S)$.

设$H \leq G, K \leq G$,记$HK = \{hk | h \in H, k \in K\}$, HK未必为G的子群.例如$H = ((1),(12)) \leq S_3, K = ((1),(13)) \leq S_3$,则$HK = \{(1),(12),(13),(123)\}$, 但$(13)(12) \notin HK$,即$HK \not\leq G$.何时有$HK \leq G$呢?

生成子群

对于群G的非空子集S,未必有$S \leq G$.但

$$K = \{a_1^{r_1} a_2^{r_2} \cdots a_m^{r_m} \mid a_i \in S, r_i = \pm 1, m \in \mathbb{N}, 1 \leq i \leq m\} \leq G.$$

并且K是G的含S的最小的子群,称K为由S生成的子群,记为$K = (S)$,称S为K的生成集.当$S = \{a_1, \ldots, a_n\}$为有限集合时,称$K = (a_1, \ldots, a_n)$为有限生成的, 当$S = \{a\}$只有一个元素时,称$K = (a)$为循环群(这正是我们前面所讨论的). 如果$S \leq G$,则$S = (S)$.

设$H \leq G, K \leq G$,记$HK = \{hk | h \in H, k \in K\}$, HK未必为G的子群.例如$H = ((1),(12)) \leq S_3, K = ((1),(13)) \leq S_3$,则$HK = \{(1),(12),(13),(123)\}$, 但$(13)(12) \notin HK$,即$HK \not\leq G$.何时有$HK \leq G$呢?

定理

设$H \leq G, K \leq G$,则$HK \leq G \Leftrightarrow HK = KH$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§9 子群的陪集

陪集的概念

例

$(\mathbb{Z}_4,+)$实际上给出了$\mathbb{Z}$的一个分类:$[0],[1],[2],[3]$. 在这个分类中,只有$[0]$构成$(\mathbb{Z},+)$的一个子群,而其余分类均不构成$(\mathbb{Z},+)$的子群.并且$\mathbb{Z}_4$中的每个类$[i]$都是类$[0]$中的每个元素普遍加上i 得到的,或者说,类$[i]$中任意两个元素的差是$[0]$中的元素.

第二章 群论
群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

$(\mathbb{Z}_4,+)$实际上给出了$\mathbb{Z}$的一个分类:[0],[1],[2],[3]. 在这个分类中,只有[0]构成$(\mathbb{Z},+)$的一个子群,而其余分类均不构成$(\mathbb{Z},+)$的子群.并且$\mathbb{Z}_4$中的每个类$[i]$都是类[0]中的每个元素普遍加上i 得到的,或者说,类$[i]$中任意两个元素的差是[0]中的元素.

例

给定S_3的一个分类$\Omega = \{H, K, M\}$,其中$H = \{(1),(12)\}, K = \{(13),(123)\}, M = \{(23),(132)\}$.只有$H \leq G$,而$K, M$均不构成$G$的子群,但$K$中的元素恰是由$H$中的元素右乘$(13)$所得到的类,$MK$中的元素恰是由$H$中的元素右乘$(23)$所得到的类,或者说,$\forall a, b \in K(M) \Rightarrow ab^{-1} \in H$.

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

$(\mathbb{Z}_4,+)$实际上给出了$\mathbb{Z}$的一个分类:[0],[1],[2],[3]. 在这个分类中,只有[0]构成$(\mathbb{Z},+)$的一个子群,而其余分类均不构成$(\mathbb{Z},+)$的子群.并且$\mathbb{Z}_4$中的每个类$[i]$都是类[0]中的每个元素普遍加上i 得到的,或者说,类$[i]$中任意两个元素的差是[0]中的元素.

例

给定S_3的一个分类$\Omega=\{H,K,M\}$,其中$H=\{(1),(12)\}, K=\{(13),(123)\}, M=\{(23),(132)\}$.只有$H\leq G$,而$K,M$均不构成$G$的子群,但$K$中的元素恰是由$H$中的元素右乘(13)所得到的类,$M$ K中的元素恰是由H中的元素右乘(23)所得到的类,或者说,$\forall a,b\in K(M)\Rightarrow ab^{-1}\in H$.

一般地,设$H\leq G$,规定G中的一个关系$\sim$如下:$a,b\in G, a\sim b\Leftrightarrow ab^{-1}\in H$.则$\sim$是$G$的一个等价关系.

陪集的概念

定义

由上面的等价关系确定的类叫做H的右陪集,包含元素a的右陪集记为Ha.

类似地,设$H \leq G, a, b \in G$.由等价关系$a \sim b \Leftrightarrow a^{-1}b \in G$确定的类叫做左陪集,包含元素$a$的左陪集记为$aH$.

陪集的概念

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义

由上面的等价关系确定的类叫做H的右陪集,包含元素a的右陪集记为Ha.

类似地,设$H \le G, a, b \in G$.由等价关系$a \sim b \Leftrightarrow a^{-1}b \in G$确定的类叫做左陪集,包含元素$a$的左陪集记为$aH$.

注

设H, K为两个集合,通常记$HK = \{ab | a \in K, b \in K\}$.特别地, $H\{b\}(\{a\}K)$记为$Hb(aK)$.

若群G的两个非空子集$H = K$,则$\forall a \in G, Ha = Ka$.

$Ha = Hb$是集合相等,未必有$ha = hb, h \in H$.

陪集的性质

定理

设$H \leq K, a, b \in G$.则下列叙述等价:

(1) $a \in Hb$;

(2) $Ha = Hb$;

(3) $ab^{-1} \in H$;

(4) $b \in Ha$;

(5) $ba^{-1} \in H$.

陪集的性质

定理

设$H \leq K, a, b \in G$.则下列叙述等价:

(1) $a \in Hb$;

(2) $Ha = Hb$;

(3) $ab^{-1} \in H$;

(4) $b \in Ha$;

(5) $ba^{-1} \in H$.

定理

一个群H的右陪集的个数和左陪集的个数相等.

陪集的性质

定理

设$H \leq K, a, b \in G$.则下列叙述等价:

(1) $a \in Hb$;

(2) $Ha = Hb$;

(3) $ab^{-1} \in H$;

(4) $b \in Ha$;

(5) $ba^{-1} \in H$.

定理

一个群H的右陪集的个数和左陪集的个数相等.

定义

一个群G的一个子群H的右(左)陪集的个数叫做H在G里的**指数**,记为$[G:H]$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

陪集的性质

引理

一个子群H与H的每一个右陪集Ha之间都存在一一映射.

陪集的性质

引理

一个子群H与H的每一个右陪集Ha之间都存在一一映射.

定理 (Lagrange定理)

设$H \leq G$,则$|G| = [G : H]|H|$.

陪集的性质

引理

一个子群H与H的每一个右陪集Ha之间都存在一一映射.

定理 (Lagrange定理)

设$H \leq G$,则$|G| = [G:H]|H|$.

推论

设G为有限群,$a \in G$.则$|a| \mid |G|$.

作业

p. 61 2,3,5

p. 64 1,2,4,5

p. 70 1,2,5

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§10 不变子群、商群

不变子群的引入

设$H \leq G$,由H决定的所有的右陪集构成的集合$S_l = \{aH|a \in G\}$. 我们来看S_l构成群的条件.

S_l中的运算应该与G中的运算有某种联系并且S_l中的运算应该封闭, 即对$\forall a, b \in G, \exists c \in G \ni (aH)(bH) = cH \in S_l$,于是$ab = (ae)(be) \in cH$,从而$aHbH = abH$. 特别地(取$a = e$), $HbH = bH$.于是有$b = h_1bh_2$,故$Hb \subseteq HbH = bH$;再由b 的任意性,有$Hb^{-1} \subseteq b^{-1}H$,所以,$bH \subseteq Hb$.

不变子群的引入

第二章 群论

群的概念

单位元 逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

设$H\le G$,由H决定的所有的右陪集构成的集合$S_l=\{aH|a\in G\}$. 我们来看S_l构成群的条件.

S_l中的运算应该与G中的运算有某种联系并且S_l中的运算应该封闭, 即对$\forall a,b\in G,\exists c\in G\ni(aH)(bH)=cH\in S_l$,于是$ab=(ae)(be)\in cH$,从而$aHbH=abH$. 特别地(取$a=e$), $HbH=bH$.于是有$b=h_1bh_2$,故$Hb\subseteq HbH=bH$;再由b的任意性,有$Hb^{-1}\subseteq b^{-1}H$,所以,$bH\subseteq Hb$.

事实上,我们证明了

性质

设$H\le G$,则对$\forall aH,bH\in S_l=\{aH|a\in G\},aHbH\in S_l\Leftrightarrow\forall a\in G,aH=Ha$.

不变子群的引入

设$H\leq G$,由H决定的所有的右陪集构成的集合$S_l=\{aH|a\in G\}$. 我们来看S_l构成群的条件.

S_l中的运算应该与G中的运算有某种联系并且S_l中的运算应该封闭, 即对$\forall a,b\in G,\exists c\in G\ni(aH)(bH)=cH\in S_l$,于是$ab=(ae)(be)\in cH$,从而$aHbH=abH$. 特别地(取$a=e$), $HbH=bH$.于是有$b=h_1bh_2$,故$Hb\subseteq HbH=bH$;再由b的任意性,有$Hb^{-1}\subseteq b^{-1}H$,所以,$bH\subseteq Hb$.

事实上,我们证明了

性质

设$H\leq G$,则对$\forall aH,bH\in S_l=\{aH|a\in G\},aHbH\in S_l\Leftrightarrow\forall a\in G,aH=Ha$.

在证明S_l关于如上定义的运算作成一个群之前,我们先来看"$aH=Ha$"的几个性质.

不变子群的概念

满足条件“$aH = Ha, \forall a \in G$”的子群H具有极其重要的意义.

不变子群的概念

群的概念
单位元 逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

满足条件“$aH = Ha, \forall a \in G$”的子群H具有极其重要的意义.

定义

*设$H \leq G$,如果对$\forall a \in G$都有$aH = Ha$,则称H为G的**不变子群**(或**正规子群**),记为$H \lhd G$.如果$H \lhd G$,则G的左(右)陪集统一称为G的**陪集**.*

不变子群的概念

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

满足条件“$aH = Ha, \forall a \in G$”的子群H具有极其重要的意义.

定义

设$H \leq G$,如果对$\forall a \in G$都有$aH = Ha$,则称H为G的不变子群(或正规子群), 记为$H \lhd G$.如果$H \lhd G$,则G的左(右)陪集统一称为G的陪集.

例

$G \lhd G, \quad \{e\} \lhd G.$

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

如果G为交换群,则G的每一个子群都是G的不变子群.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

如果G为交换群,则G的每一个子群都是G的不变子群.

例

设G为群,称$C(G) = \{a \in G | \forall x \in G, ax = xa\}$为$G$的**中心**,我们有$C(G) \leq G$且$C(G) \lhd G$.

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

例

如果G为交换群,则G的每一个子群都是G的不变子群.

例

设G为群,称$C(G) = \{a \in G | \forall x \in G, ax = xa\}$为$G$的**中心**,我们有$C(G) \leq G$且$C(G) \lhd G$.

例

设$H = \{(1),(123),(132)\} \leq S_3$,则$H \lhd S_3$.

不变子群的概念

例

如果G为交换群,则G的每一个子群都是G的不变子群.

例

设G为群,称$C(G)=\{a\in G|\forall x\in G, ax=xa\}$为$G$的中心,我们有$C(G)\leq G$且$C(G)\lhd G$.

例

设$H=\{(1),(123),(132)\}\leq S_3$,则$H\lhd S_3$.

本题可以直接验证,也可以利用Lagrange定理来证明.

证 由于$|S_3|=6, |H|=3$,所以H只有两个左(右陪集),并且其中有一个为H. 故有$(12)H=(13)H=(23)H=H(12)=H(13)=h(23), (123)H=(132)H=(1)H=H(1)=H(123)=H(132)$. $\square$

不变子群的性质

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

一般地,我们有

例

如果$H \leq G$*且*$[G:H]=2$,*则*$H \lhd G$.

第二章
群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

一般地,我们有

例

如果$H \leq G$*且*$[G:H]=2$,*则*$H \lhd G$.

证 $\forall x \in G$,若$x \in H$,则$Hx = H = xH$;若$x \notin H$,则$Hx \cap H = \emptyset$, $xH \cap H = \emptyset$,且此时有$G = H \cup Hx = H \cup xH$, 于是$Hx = xH$.总之有$Hx = xH$,即$H \lhd G$. □

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

一般地,我们有

例

如果$H \leq G$且$[G:H]=2$,则$H \lhd G$.

证 $\forall x \in G$,若$x \in H$,则$Hx = H = xH$;若$x \notin H$,则$Hx \cap H = \emptyset$, $xH \cap H = \emptyset$,且此时有$G = H \cup Hx = H \cup xH$, 于是$Hx = xH$.总之有$Hx = xH$,即$H \lhd G$. □

注意

$aH = Ha$只是集合相等,绝不意味着元素乘积可以交换.

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定理

设$H \leq G$.下列叙述等价:

(1) $aH = Ha, \forall a \in G$;

(2) $aHa^{-1} = H, \forall a \in G$;

(3) $aHa^{-1} \subseteq H, \forall a \in G$;

(4) $aha^{-1} \in H, \forall a \in G, \forall h \in H$.

不变子群的性质

定理

设$H \leq G$.下列叙述等价:

(1) $aH = Ha, \forall a \in G$;

(2) $aHa^{-1} = H, \forall a \in G$;

(3) $aHa^{-1} \subseteq H, \forall a \in G$;

(4) $aha^{-1} \in H, \forall a \in G, \forall h \in H$.

例

设$H \leq G$,称$N(H) = \{x \in G | xH = Hx\}$为$H$在$G$中的*正规化子*.则$H \lhd N(H) \leq G$.

不变子群的性质

由此可以看出,$N(H)$是将H作为不变子群的G的最大的子群.特别地, 若$H \lhd G$,则$N(H) = G$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

由此可以看出,$N(H)$是将H作为不变子群的G的最大的子群.特别地, 若$H \lhd G$,则$N(H) = G$.

例

设$H \leq G, N \leq G$.则

(1) $H \lhd G \Rightarrow H \cap N \lhd N$;

(2) $H \lhd G \ and \ N \lhd G \Rightarrow H \cap N \lhd G$;

(3) $H \lhd G \Rightarrow HN \leq G \ and \ H \lhd HN$;

(4) $H \lhd G \ and \ N \lhd G \Rightarrow HN \lhd G$;

(5) $H \lhd G \ and \ N \lhd G \ and \ H \cap N = \{e\} \Rightarrow \forall h \in H, n \in N, hn = nh$.

不变子群的性质

由此可以看出,$N(H)$是将H作为不变子群的G的最大的子群.特别地, 若$H \lhd G$,则$N(H) = G$.

例

设$H \leq G, N \leq G$.则

(1) $H \lhd G \Rightarrow H \cap N \lhd N$;

(2) $H \lhd G$ and $N \lhd G \Rightarrow H \cap N \lhd G$;

(3) $H \lhd G \Rightarrow HN \leq G$ and $H \lhd HN$;

(4) $H \lhd G$ and $N \lhd G \Rightarrow HN \lhd G$;

(5) $H \lhd G$ and $N \lhd G$ and $H \cap N = \{e\} \Rightarrow \forall h \in H, n \in N, hn = nh$.

例

设$G = S_4, H = \{(1), (12)(34), (13)(24), (14)(23)\}, N = \{(1), (1234)\}$,则$H \lhd G, N \lhd H$,但$N \ntriangleleft G$.这说明正规子群没有传递性.

不变子群与商群

引理

设$H \lhd G$,则S_l中的运算$(aH)(bH) = (ab)H$是一个代数运算,即若$aH = a'H, bH = b'H$,则$(ab)H = (a'b')H$.

不变子群与商群

引理

设$H \lhd G$,则S_l中的运算$(aH)(bH) = (ab)H$是一个代数运算,即若$aH = a'H, bH = b'H$,则$(ab)H = (a'b')H$.

定理

设$H \lhd G$,则S_l关于运算$(aH)(bH) = (ab)H$作成一个群.

不变子群与商群

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

引理

设$H \lhd G$,则S_l中的运算$(aH)(bH) = (ab)H$是一个代数运算,即若$aH = a'H, bH = b'H$,则$(ab)H = (a'b')H$.

定理

设$H \lhd G$,则S_l关于运算$(aH)(bH) = (ab)H$作成一个群.

定义

一个群G的一个不变子群H的陪集所作成的群叫做G关于H的**商群**,记为G/H.

第二章 群论

群的概念

单位元 逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

引理

设$H \lhd G$,则S_l中的运算$(aH)(bH) = (ab)H$是一个代数运算,即若$aH = a'H, bH = b'H$,则$(ab)H = (a'b')H$.

定理

设$H \lhd G$,则S_l关于运算$(aH)(bH) = (ab)H$作成一个群.

定义

一个群G的一个不变子群H的陪集所作成的群叫做G关于H的**商群**,记为G/H.

由于$\mid G/H \mid$等于H在G中的指数,根据Lagrange定理可得

推论

设$H \lhd G$,则$\dfrac{|G|}{|H|} = \mid G/H \mid$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

§11 同态与不变子群

群同态与同态核

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定义

设$\varphi : G \longrightarrow \bar{G}$是群同态映射,称$ker\varphi = \{x \in G \mid \varphi(x) = \bar{e}\}$为$\varphi$的**核**.

群同态与同态核

定义

设$\varphi: G \longrightarrow \bar{G}$是群同态映射,称$ker\varphi = \{x \in G \mid \varphi(x) = \bar{e}\}$为$\varphi$的**核**.

性质

设$\varphi: G \longrightarrow \bar{G}$是群同态,则$ker\varphi \lhd G$.

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

群同态与同态核

定义

设$\varphi: G \longrightarrow \bar{G}$是群同态映射,称$ker\varphi = \{x \in G \mid \varphi(x) = \bar{e}\}$为$\varphi$的**核**.

性质

设$\varphi: G \longrightarrow \bar{G}$是群同态,则$ker\varphi \lhd G$.

性质

设$\varphi: G \longrightarrow \bar{G}$是群同态,则$\varphi$为单同态$\Leftrightarrow ker\varphi = \{e\}$.

群的同态基本定理(第一同态定理)

定理

设$N \lhd G$,则有群满同态$\varphi : G \longrightarrow G/N; x \longmapsto xN.$

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

群的同态基本定理(第一同态定理)

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定理

设$N \lhd G$,则有群满同态$\varphi : G \longrightarrow G/N; x \longmapsto xN$.

注

1. 定理中的同态通常称为自然同态;
2. 自然同态的同态核为N;
3. 群G的每个商群都是G的同态象,进而可由商群的性质得到G的一些性质;
4. 由下面的定理还可以看出,G的每个同态象也只能是G的商群(在同构的意义下),这两个定理合称为同态基本定理(或第一同态定理).

群的同态基本定理(第一同态定理)

定理

设G与$\bar{G}$是同态的群:$G \overset{\varphi}{\sim} \bar{G}$且$ker\varphi = N$,则$G/N \cong \bar{G}$.

群的同态基本定理(第一同态定理)

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

定理

设G与$\bar{G}$是同态的群:$G \overset{\varphi}{\sim} \bar{G}$且$ker\varphi = N$,则$G/N \cong \bar{G}$.

证.

由$N \lhd G$得商群G/N.定义$\phi : G/N \longrightarrow \bar{G}; gN \longmapsto \varphi(g)$,则直接验证即得$G/N \cong \bar{G}$. □

群的同态基本定理(第一同态定理)

定理

设G与$\bar{G}$是同态的群:$G \overset{\varphi}{\sim} \bar{G}$且$ker\varphi = N$,则$G/N \cong \bar{G}$.

证.

由$N \lhd G$得商群G/N.定义$\phi : G/N \longrightarrow \bar{G}; gN \longmapsto \varphi(g)$,则直接验证即得$G/N \cong \bar{G}$. □

例

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong R^*.$$

定理 (分解定理,第一同构定理)

设$\varphi: A \longrightarrow B$是群同态映射,则存在唯一的群单同态$\bar{\varphi}: A/\mathrm{ker}\varphi \longrightarrow B$使下图可换:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\eta"'] & B \\ A/ker\varphi, \arrow[ur, dashed, "\exists 1\bar{\varphi}"'] & \end{tikzcd}$$

且$\bar{\varphi}$满$\Leftrightarrow$ φ满.

第二章 群论

群的概念

单位元逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

定理 (分解定理,第一同构定理)

设$\varphi: A \longrightarrow B$*是群同态映射,则存在唯一的群单同态*$\bar{\varphi}: A/\ker\varphi \longrightarrow B$*使下图可换:*

$$
\begin{tikzcd}
A \arrow[rr, "\varphi"] \arrow[d, "\eta"'] & & B \\
A/ker\varphi, \arrow[urr, dashed, "\exists 1\bar{\varphi}"'] & &
\end{tikzcd}
$$

且$\bar{\varphi}$*满*$\Leftrightarrow \varphi$*满.*

证.

注意到φ是群同态,$N = \ker\varphi \lhd A$,有自然同态$\eta: A \longrightarrow A/N$,且$\bar{\varphi}: A/N \longrightarrow B; gN \longmapsto \varphi(g)$满足条件. $\square$

群的同态基本定理(第一同态定理)

定理 (分解定理,第一同构定理)

设$\varphi : A \longrightarrow B$是群同态映射,则存在唯一的群单同态$\bar{\varphi} : A/\ker\varphi \longrightarrow B$使下图可换:

$$\begin{tikzcd}
A \arrow[rr, "\varphi"] \arrow[d, "\eta"'] & & B \\
A/ker\varphi, \arrow[urr, dashed, "\exists 1\bar{\varphi}"'] & &
\end{tikzcd}$$

且$\bar{\varphi}$满$\Leftrightarrow$ φ满.

证.

注意到φ是群同态,$N = \ker\varphi \lhd A$,有自然同态$\eta : A \longrightarrow A/N$,且$\bar{\varphi} : A/N \longrightarrow B; gN \longmapsto \varphi(g)$满足条件. □

通常称$\bar{\varphi}$为φ的导出同态.

对应定理

定义

设$\phi: A \longrightarrow B$.称$\phi(S) = \{y \in B \mid \exists x \in S \ni \phi(x) = y\}$为$A$的子集$S$在$\phi$下的**象**; 称$\phi^{-1}(T) = \{x \in A \mid \exists y \in T \ni \phi(x) = y\}$为$B$的子集$T$ 在ϕ下的**原象**.

对应定理

定义

设$\phi: A \longrightarrow B$.称$\phi(S)=\{y \in B \mid \exists x \in S \ni \phi(x)=y\}$为$A$的子集$S$在$\phi$下的象; 称$\phi^{-1}(T)=\{x \in A \mid \exists y \in T \ni \phi(x)=y\}$为$B$的子集$T$ 在ϕ下的原象.

定理

设$\phi: A \longrightarrow B$.是群同态满射,则

(1) $H \leq A \Rightarrow \phi(H) \leq B$;

(2) $H \lhd A \Rightarrow \phi(H) \lhd B$;

(3) $H \leq B \Rightarrow \phi^{-1}(H) \leq A$且$ker\phi \leq \phi^{-1}(H)$;

(4) $H \lhd B \Rightarrow \phi^{-1}(H) \lhd A$且$ker\phi \leq \phi^{-1}(H)$.

群的第二同态定理

第一同态定理是说,若$A \overset{\varphi}{\sim} B$,则$A/\ker\varphi \cong B$,其中$\ker\varphi = \varphi^{-1}(e_B)(=\varphi^{-1}(\{e_B\}))$.我们现在来推广这一定理,将$\{e_B\}$换成$B$的不变子群.

第二章 群论

群的概念

单位元 逆元削去律

有限群的另一定义

群的同态

变换群

置换群

循环群

子群

子群的陪集

不变子群、商群

同态与

第一同态定理是说,若$A \overset{\varphi}{\sim} B$,则$A/\ker\varphi \cong B$,其中$\ker\varphi = \varphi^{-1}(e_B)(=\varphi^{-1}(\{e_B\}))$.我们现在来推广这一定理,将$\{e_B\}$换成$B$的不变子群.

定理 (群的第二同态定理)

设$A \overset{\varphi}{\sim} B, H \lhd B$,则$A/N \cong B/H$,其中$N = \varphi^{-1}(H)$.

群的第二同态定理

第一同态定理是说,若$A \overset{\varphi}{\sim} B$,则$A/\ker\varphi \cong B$,其中$\ker\varphi = \varphi^{-1}(e_B)(=\varphi^{-1}(\{e_B\}))$.我们现在来推广这一定理,将$\{e_B\}$换成$B$的不变子群.

定理 (群的第二同态定理)

设$A \overset{\varphi}{\sim} B, H \lhd B$,则$A/N \cong B/H$,其中$N = \varphi^{-1}(H)$.

证.

由$H \lhd B$知$N \lhd A$,于是$A/N, B/H$都有意义.于是有交换图

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\eta_A"'] & B \arrow[r, "\eta_B"] & B/H \\ A/N \arrow[urr, dashed, "\exists 1\bar{\varphi}"'] & & \end{tikzcd}$$

注意到$N = \ker(\eta_B\varphi)$,由同态基本定理即得结论. $\square$

作业

p.74 1,2,4
p.79 2,3

练习与思考题

1 设G是一个有限群,A和B是G的两个非空子集.证明:如果$|A|+|B|>G$,则$G=AB$.特别地,若$|A|>|G|/2$,则$G=A^2$.

2 证明:若群G中有惟一的2阶元素,则这个2阶元素必是G的一个中心元.

3 设G是一个群,且$|G|>1$.

(1) 证明:若G中除单位元外其余元素的阶都相同,则这个相同的阶不是无限就是素数.

(2) 说明这样的两种群是存在的.

4 设a,b是群G中的元素,且$|a|=s,|b|=t,ab=ba$.证明:

(1) $|ab|\,|\,[s,t]$;

(2) 对$[s,t]$的任一正因数h, G中有阶是h的元素.

5 设a是群G中的一个元素,且$|a|=mn,(m,n)=1$.证明:$\exists 1 b,c\in G\ni a=bc,bc=cb,|b|=m,|c|=n$.

6 证明:交换群中所有有限阶元素作成一个群.

7 求S_3的所有子群.

第二章 群论

群的概念
单位元逆元削去律
有限群的另一定义
群的同态
变换群
置换群
循环群
子群
子群的陪集
不变子群、商群
同态与

8 设H是群G的一个非空子集,且$H^2 = H$.

(1) H是否为G的一个子群?

(2) 当H有限时,$H \leq G$.

9 设$H \leq G, a \in G$.证明:$aHa^{-1} \leq G$, 且$H \cong aHa^{-1}$.

10 设$H, K \leq G$.证明:

(1) $H \cap K \leq G$;

(2) $H \cup K \leq G \Rightarrow H \cup K = HK$;

(3) $H \cup K \leq G \Leftrightarrow H \subseteq K$ or $K \subseteq H$.

11 设G是一个$2n$阶交换群.证明:如果n是一个奇数,则G有且仅有一个2阶子群.

12 设$H, K \leq G$,且$|H| = m, |K| = n$.证明:若$(m, n) = 1$,则$H \cap K = \{e\}$. 反之,若$H \cap K = \{e\}$,是否一定有$(m, n) = 1$?

13 设G是一个$2p$(p为素数)阶有限非交换群.证明:

(1) G一定有一个p阶子群;

(2) G的元素可写成$e, a, \ldots, a^{p-1}, b, ab, \ldots, a^{p-1}b$的形式.

14 设H, K是群G的两个有限子群.证明:$|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

练习与思考题

15 设$N \lhd G$,且$(G:N)=m$,则$\forall a \in G, a^m \in N$.

16 证明:四元数群$G=\{\pm 1, \pm i, \pm j, \pm k\}$ (其中$i^2=j^2=k^2=-1, ij=k=-ji, jk=i=-kj, ki=j=-ik$) 是非交换群且每个子群都是正规子群.该群被称为Hamilton 群.

17 证明:

(1) 无限循环群的自同构只有两个;

(2) n阶循环群的自同构有$\varphi(n)$个,即小于n且与n互素的正整数个数.

18 证明:在同构的意义下,4阶群只有两个,一个是循环群,另一个是Klain四元群$K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$.

19 求S_5中阶为2的元素.