商群. 同态定理,有限循环群.

回顾商群的定义

对群G, $H\lhd G$. $G/H := \{aH:\ a\in G\}$

命题. $(G/H;\cdot)$ 构成群. 其中 $\cdot$ 是G的子集之间的乘法. (对$A\subseteq G$, $B\subseteq G$, $A\cdot B := \{ab:\ a\in A, b\in B\}$)

并且 (1) $\forall a,b\in G$, $(aH)\cdot(bH)=(ab)H$.

(2) H为幺元. 即$\forall a\in G$. $(aH)\cdot H = H\cdot(aH) = aH$.

(3) $\forall a\in G$, $a^{-1}H$为aH的逆元.

(4) 定义$\pi_H: G\to G/H$. $\forall a\in G$, $\pi_H(a):=aH$.

则π_H是G到G/H的同态,且为满同态.

正规子群的一个性质.

1) $H\leq G \Rightarrow H\cdot H = H$ (对一般的子群)

2) $H\lhd G \Rightarrow \forall a\in G$, 有$aH=Ha$ (这也是正规子群的一个充要条件)

$\forall A\subseteq G$, 有$AH=HA$. (对正规子群)

Pf: 1) $H\cdot H=\{ab: a\in H, b\in H\}$. 由封闭性知$H\cdot H\subseteq H$.

又由$e\subseteq H$. 故$\forall h\in H$, 有$h=eh\in H\cdot H \Rightarrow H\subseteq H\cdot H$.

故 $H\cdot H = H$

2) 只证第1条. 对$a\in G$, 有$\forall h\in H$. $ah = ah(a^{-1}a)=(aha^{-1})a$

由$H\lhd G$, 知$aha^{-1}\in H$. 故$(aha^{-1})a\in Ha$

故$aH\subseteq Ha$. 同理有$Ha\subseteq aH$. 故$aH=Ha$

回到上述命题的证明:

1) $(aH)(bH) = a(Hb)H = a(bH)H = (ab)(HH) = (ab)H$

实际上是集合·集合,有结合律.

2) $H(aH) = (aH)H = a(HH) = aH$

3) $(a^{-1}H)(aH) = (aH)(a^{-1}H) = a(Ha^{-1})H = a(a^{-1}H)H = H$.

4) $\forall a,b\in G$, 即证: $\pi_H(ab)=\pi_H(a)\pi_H(b)$

$\Leftrightarrow (ab)H=(aH)(bH)$. 由1)知该式成立.

满同态是显然的.

核: $\pi_H(a)=H \Leftrightarrow aH=H \Leftrightarrow a\in H$.

同态定理.

回顾同态的定义: 对群G, L. $f: G\to L$为同态,若$f(ab)=f(a)f(b)$. $\forall a,b\in G$.

$\mathrm{Ker}(f) := \{a\in G;\ f(a)=e_L\}$

我们已经知道 $\mathrm{Ker}(f)\lhd G$.

同态定理: 设G, L为群. $f: G\to L$为同态. 记$H:=\mathrm{Ker}(f)$. 则有:

1) $\forall a,b\in G$, $aH=bH \Leftrightarrow f(a)=f(b)$.

2) 如下定义$\varphi: G/H\to L$. $\forall a\in G$, $\varphi(aH):=f(a)$.

则φ是单同态. 且 $\mathrm{ran}(\varphi)=\mathrm{ran}(f)$.

借助这个定理,我们总可以将一个同态变为一个单同态. 进而得到一个同构.

则φ是G/H到$\mathrm{ran}(f)$的群同构. 即 $G/H \overset{\varphi}{\cong} \mathrm{ran}(f) \leq L$.

Fact. (1) $A\leq G$, 则$f(A)=\{f(a)\mid a\in A\}$, 且$f(A)\leq L$

(2) 设$B\leq L$, 则$f^{-1}(B)=\{a\in G: f(a)\in B\}\leq G$

(自行证明).

同态定理的证明:

1) 若有$aH=bH$. 则$\exists h\in H$,使得 $a=bh$

注意$h\in \mathrm{Ker}(f)$. 有$f(a)=f(bh)=f(b)f(h)=f(b)e=f(b)$

若有$f(a)=f(b)$. 则 $e=f(a)^{-1}f(b)=f(a^{-1})f(b)=f(a^{-1}b)$

故 $a^{-1}b\in H$. 即$aH=bH$.

($\exists h\in H$, 使$b=ah$, 则$bH=ahH=aH$)

(当然,也可以理解为 $a\sim b\Rightarrow$ 属于同一等价类,即陪集相同)

2) 首先, 验证φ的定义是可行的.

即对$a,b\in G$, $aH=bH$, 有$f(a)=f(b)$ (这就是1))

再证φ是同态. $\forall a,b\in G$, 欲证 $\varphi((aH)(bH))=\varphi(aH)\varphi(bH)$

即证 $\varphi((ab)H)=f(a)f(b)$

即证 $f(ab)=f(a)f(b)$

由f是同态知上式成立.

再证φ是单同态. 对$a,b\in G$, $\varphi(aH)=\varphi(bH)$, 欲证$aH=bH$.

$\varphi(aH)=\varphi(bH)\Rightarrow f(a)=f(b) \overset{(1)}{\Leftrightarrow} aH=bH$

φ与f像集相同是显然的.

以下的交换图是该结果的一个直观表示.

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi_H"'] & L \\
G/H \arrow[ur, dashed, "\varphi"'] &
\end{tikzcd}$$

$f=\varphi\circ\pi_H$.

同态定理的一个例子

考虑群$(\mathbb{Z},+)$和$n\in\mathbb{Z}^+$

$f: (\mathbb{Z};+)\to(\{0,1,\dots,n-1\};+_{\mathrm{mod}\ n})$

$\forall a\in\mathbb{Z}$, $f(a):=a\%n$.

容易看出f是一个满同态

$H:=\mathrm{Ker}(f):=\{a\in\mathbb{Z}; f(a)=0\}=\{qn; q\in\mathbb{Z}\}$.

$G/H \overset{\varphi}{\cong} \{0,\dots,n-1\}$

实际上是模n的所有剩余类构成的集合.

设G为有限循环群, $|G|=n$. g为G的生成元.

(即$G=\langle g\rangle := \{g^i; i\in\mathbb{Z}\}$

$=\{g^i; i=0,1,\dots,n-1\}$

我们接下来考虑G的子群.

(1) 设$d\in\mathbb{Z}^+$, $d\mid n$, $H:=\langle g^d\rangle$. 则$H\leq G$, 且$|H|=\frac{n}{d}$

且有 $H=\{y\in G;\ y^{\frac{n}{d}}=1\}$

(2) 设$H\leq G$, 则$\exists d\in\mathbb{Z}^+$, $d\mid n$ 且$H=\langle g^d\rangle$.

pf: (2) 由 Lagrange Thm., 有$|H|\,\big|\,|G|$. 可设$|H|=\frac{n}{d}$.

记$I:=\{i\in\mathbb{N}; g^i\in H\}$

由: $\forall i,j\in I$, 有$g^{i+j}=g^i\cdot g^j\in H$, 即$i+j\in H$

$\forall i,j\in I$. $i<j$. 有$g^{j-i}=g^j\cdot(g^i)^{-1}\in H$. 即$j-i\in H$

由Week 2中的结论,可知$I=\{nd\mid n\in\mathbb{N}\}$, $\exists d\in\mathbb{Z}^+$

故原命题成立

(1) 由$|\langle g\rangle|=n$ 有$o(g)=n$. 我们希望证$o(g^d)=\frac{n}{d}$

一方面, $(g^d)^{\frac{n}{d}}=g^n=e$

另一方面, $\forall i\in\mathbb{Z}$, $(g^d)^i=e \Leftrightarrow g^{di}=e$

$\Leftrightarrow n\mid di$

$\Leftrightarrow \frac{n}{d}\mid i$

故 $o(g^d)=\frac{n}{d} \Rightarrow |H|=\frac{n}{d}$

$\forall h\in H=\langle g^d\rangle$. 即$\exists i\in\mathbb{Z}^+$使$h=(g^d)^i=g^{di}$

$h^{\frac{n}{d}}=(g^{id})^{\frac{n}{d}}=g^{ni}=e$

另一方面, 任取$y\in G$, $y^{\frac{n}{d}}=e$. 由$y\in G$有$y=g^i$, $\exists i\in\mathbb{N}$

即 $g^{\frac{in}{d}}=e$. 由$o(g)=n$

有 $n\mid\frac{in}{d} \Rightarrow d\mid i \Rightarrow y=g^i=(g^d)^{\frac{i}{d}}\in\langle g^d\rangle$

思考题: 1) 设$o(g)=n$ $d\in\mathbb{Z}^+$, $d\mid n$. 则$o(g^d)=\frac{n}{d}$

对$k\in\mathbb{Z}$, $o(g^k)=\frac{n}{\gcd(k,n)}$

2) $\langle g^k\rangle=\langle g^{\gcd(k,n)}\rangle$.

置换群.

定义. 对集合X, $\mathrm{Sym}(X):=\{\sigma\mid\sigma: X\to X$ 为双射$\}$

则$(\mathrm{Sym}(X);\circ)$构成群. 其中$\circ$为映射的复合运算. $(g\circ f)(x):=g(f(x))$.

称为X上的对称群. 其子群称为X上的置换群. 对$|X|=n$. 也可将$\mathrm{Sym}(X)$记作S_n.

容易验证$\mathrm{Sym}(X)$的封闭性、结合律. 幺元 —— Id_X. 逆元 —— 逆映射.

在数学史上, "群"的概念最早被引入时是多项式根的置换群引入的.

"群"的抽象定义此后逐步提取而出的.

Week 4 引入的 Cayley Thm., 将一般的抽象的群与其上的置换群联系在一起

一些简单的置换 (我们期望用一些简单的置换去复合出更复杂的)

对换(i,j) 对$i\in X$, $j\in X$, $i\neq j$. $\sigma(i)=i$. $\sigma(j)=j$ $\sigma(l)=l$. $\forall l\neq i,j$.

三轮换 (i,j,k) $i,j,k\in X$两两不同. $\sigma(i)=j$. $\sigma(j)=k$, $\sigma(k)=i$. $\sigma(l)=l$. $\forall l\neq i,j,k$

m轮换 $(a_1,a_2,\dots,a_m)$ $a_1,\dots,a_m\in X$两两不同 $\sigma(a_i)=a_{i+1}$. $i=1,2,\dots,m$. (约定$a_{m+1}=a_1$)

$\sigma(l)=l$. $l\notin\{a_1,\dots,a_m\}$.

例子.

S_5. $\alpha=(2,3,1,5,4)$. $\beta=(1,3,4,5,2)$

计算$\alpha\circ\beta=(2,1,5,4,3)$

$\beta\circ\alpha=(3,4,1,2,5)$

$\alpha^{-1}=(3,1,2,5,4)$