# 离散数学之近世代数讲义附件 2019(1)

## 第 11 章 半群和幺半群

**定理：**

1. 证明 $(Z_n,\oplus)$ 为半群。

证明：只须证明 $\oplus$ 为 $Z_n$ 的二元代数运算 。

1）封闭性：由 $[i]\oplus[j]=[i+j]$ 知 $[i+j]\in Z_n$

2）证 $\oplus$ 为 $Z_n$ 上的二元映射：即证对 $\forall[p],[q]\in Z_n$，若 $[i]=[p]$，$[j]=[q]$

则有：$[p+q]=[i+j]$

由 $[i]=[p]\Rightarrow n|(i-p)$，$[j]=[q]\Rightarrow n|(j-q)$

$\therefore n|(i-p)+(j-q)$，即 $n|(i+j)-(p+q)$

$\therefore [p+q]=[i+j]$

//////////////////////////////

2. 教材 11.3 节定理 11.3.2：

有限半群 $(S,\circ)$ 为一个有限么半群当且仅当 $\exists s,t\in S$ 使得：$sS=S, St=S$

证明：必要性显然。主证充分性：

令 $\varphi:S\to S$，且对 $\forall x\in S,\varphi(x)=s\circ x$。则可得像集 $\varphi(S)=sS$，又 $sS=S$，即像集 $\varphi(S)$ 与有限集合 $S$ 重合，从而 $\varphi$ 为有限集合 $S$ 上的一个双射，即为 $S$ 上的一个置换，从而存在正整数 $m$，使得置换 $\varphi$ 复合 $m$ 次后为恒等置换即为恒等映射（其中 $m$ 的取值为置换 $\varphi$ 分解为无共同文字后的循环置换的阶的最小公倍数）。又 $\varphi^m(x)=s^m\circ x$，而 $\varphi^m(x)=x$（为恒等映射），则有 $s^m\circ x=x$，即 $s^m$ 为左单位元，同理可证右单位元，故 $(S,\circ)$ 为幺半群。

//////////////////////////////////////

3. 教材 11.3 节定理 11.3.5：

有限半群 $(S,\circ)$ 是一个群的充要条件是 $\forall s\in S$ 有 $sS=S$ 且 $\exists t\in S$ 使得 $St=S$

证明：充分性的证明原理同上。下面给出必要性证明：

先证若 $(S,\circ)$ 为群则有：$\forall s\in S$ 有 $sS=S$ 。

1）由运算的封闭性知：$sS \subseteq S$。

2）下证 $S \subseteq sS$：

对 $\forall y \in S$，由 $S$ 为群知 $s$ 有逆元 $s^{-1} \in S$，从而 $s^{-1} \circ y \in S$，则由 $sS$ 的定义知

$s \circ (s^{-1} \circ y) \in sS$，即有 $(s \circ s^{-1}) \circ y \in sS$，$y \in sS$，故有 $S \subseteq sS$。

再证若 $(S,\circ)$ 为群则有：$\exists t \in S$ 使得 $St = S$。

显然。取单位元即可。

////////////////////////////////////////

4. 教材 11.4 节定理 11.4.1：

一个幺半群的任意多个子幺半群的交集仍是子幺半群。

证明：设 $(M,\circ,e)$ 是一个幺半群。令 $H = \bigcap_{\alpha \in I} M_a$ 表示 $M$ 的若干子幺半群的交，其中 $M_\alpha$ 为 $M$ 的子幺半群。则由子幺半群的定义知 $e \in M_\alpha$，从而 $e \in H$。又对 $\forall a,b \in H$ 有 $a,b \in M_\alpha$，由 $M_\alpha$ 的封闭性知 $a \circ b \in M_\alpha$，从而 $a \circ b \in \bigcap_{\alpha \in I} M_a$，即 $a \circ b \in H$（运算封闭性得到满足），从而 $H$ 为 $M$ 的子幺半群。

注：教材定理 11.4.1 与 11.4.2 给出了一个求解生成子幺半群或生成子半群的理论方法，但希望大家能够根据生成子（幺）半群的定义给出其迭代生成算法过程。

/////////////////////////////////////

5. 教材 11.4 节定理 11.4.3：

设 $A$ 是半群 $(S,\circ)$ 的一个非空子集，则：

1）由 $A$ 生成的左理想是 $A \cup SA$

2）由 $A$ 生成的右理想是 $A \cup AS$

3）由 $A$ 生成的理想是 $A \cup SA \cup AS \cup SAS$

证 1)：根据生成左理想的定义从三个方面来证明：

①包含性：$A \subseteq A \cup SA$，显然。

②左理想：须证 $S(A \cup SA) \subseteq A \cup SA$

因为 $S(A \cup SA) = SA \cup S(SA) = SA \cup (SS)A$，又 $SS \subseteq S$，所以 $(SS)A \subseteq SA$，从而 $S(A \cup SA) \subseteq A \cup SA$

③“最小性”：设$P$是$S$的任一包含$A$的左理想，下证$A\bigcup SA\subseteq P$：

由$A\subseteq P$，知$SA\subseteq SP$，又$P$是$S$的左理想则有$SP\subseteq P$，从而$SA\subseteq A$，故有$A\bigcup SA\subseteq P$。

下面的2）3）证明同理，请大家自己完成。

//////////////////////////////////////////////////////

6.教材11.5节定理11.5.1：

任何幺半群$(M,*,e)$同构于变换幺半群$(L(M),\circ,I_M)$。

证明：设$(M,*,e)$为一个幺半群，$L(M)=\{\rho_a|\rho_a(x)=a*x,\forall x\in M,a\in M\}$（即$L(M)$为由$M$上的左线性变换（映射）构成的集合），则$L(M)$对映射的符合运算“$\circ$”构成一个幺半群称为变换幺半群$(L(M),\circ,I_M)$。（此处主要需要验证映射符合运算在$L(M)$上的封闭性，设$\rho_a(x)=a*x$，$\rho_b(x)=b*x$，则

$\rho_b\circ\rho_a(x)=\rho_b(\rho_a(x))=\rho_b(a*x)=b*(a*x)=(b*a)*x=\rho_{b*a}(x)$，

即$\rho_b\circ\rho_a=\rho_{b*a}$，显然$\rho_{b*a}\in L(M)$；结合律自动成立），其中单位元即为$M$上的恒等映射（取$a=e$即可）。

下证同构成立。

定义$\varphi:M\to L(M)$，且有对$\forall a\in M,\varphi(a)=\rho_a$，则由$L(M)$的构造知$\varphi$为满射，

下证$\varphi$为单射：对$\forall a,b\in M,a\neq b$，假设$\varphi(a)=\varphi(b)$，则有$\rho_a=\rho_b$，即对$\forall x\in M$，有$\rho_a(x)=\rho_b(x)$，即有$a*x=b*x$，令$x=e$可得$a=b$矛盾，故$\varphi(a)\neq\varphi(b)$为单射，从而$\varphi$为双射。

又对$\forall a,b\in M$，$\varphi(a*b)=\rho_{a*b}$，而$\varphi(a)\circ\varphi(b)=\rho_a\circ\rho_b=\rho_{a*b}$，

所以$\varphi(a*b)=\varphi(a)\circ\varphi(b)$，综上$\varphi:M\to L(M)$为同构。

////////////////////////////////////////

7.讲义PPT1-4节定理6 幺半群同态基本定理

先给出示意图中由普通集合升级为幺半群后的已知结果：

1）$(M_1,\circ,e_1)$与$(M_2,*,e_2)$为幺半群；

2）$\varphi:M_1\to M_2$**满**同态，即对$\forall a,b\in M_1$，$\varphi(a\circ b)=\varphi(a)*\varphi(b)$；

3）由升级关系知基于映射的分解关系和相关结论仍然成立：

①仍可由$\varphi$确定商集$M_1/E_\varphi$，即由等价关系$E_\varphi$所划分的等价类之集，且有$[a]=[b]$（或$aE_\varphi b$）当且仅当$\varphi(a)=\varphi(b)$；

②仍有映射的分解关系成立：$\varphi=\overline{\varphi}\circ\gamma$，其中：

$\gamma: M_1\to M_1/E_\varphi$的自然映射（满射），且有对$\forall a\in M_1$，$\gamma(a)=[a]$

$\overline{\varphi}: M_1/E_\varphi\to M_2$的单、满射（双射），且有对$\forall[a]\in M_1/E_\varphi$，$\overline{\varphi}([a])=\varphi(a)$

（此处的分解关系大家可以对照我们的举例来理解其逻辑关系）

下面分别回答 PPT 示意图中的问题。

问题 1：商集$M_1/E_\varphi$能否升级为幺半群？

定义商集$M_1/E_\varphi$上的二元运算“$\bullet$”：对$\forall[a],[b]\in M_1/E_\varphi$有$[a]\bullet[b]=[a\circ b]$。

可验证$(M_1/E_\varphi,\bullet,[e_1])$为幺半群，称为商幺半群。这里主要需要证明“$\bullet$”为$M_1/E_\varphi$上的二元代数运算，即需证“$\bullet$”为$M_1/E_\varphi\times M_1/E_\varphi\to M_1/E_\varphi$的二元映射。

（I）运算“$\bullet$”的封闭性：由$a,b\in M_1$，知$a\circ b\in M_1$，从而$[a\circ b]\in M_1/E_\varphi$。

（II）“$\bullet$”为映射：若有$[a]=[a']$，$[b]=[b']$，则由定义知：$[a']\bullet[b']=[a'\circ b']$，

下证$[a\circ b]$=$[a'\circ b']$（即当映射的自变量相等时因变量也相等）。

由$[a]=[a']\Rightarrow\varphi(a)=\varphi(a')$，

$[b]=[b']\Rightarrow\varphi(b)=\varphi(b')$

又$\varphi(a\circ b)=\varphi(a)*\varphi(b)$，从而$\varphi(a\circ b)=\varphi(a')*\varphi(b')$=$\varphi(a'\circ b')$，

即有$\varphi(a\circ b)$=$\varphi(a'\circ b')$，所以$[a\circ b]$=$[a'\circ b']$。

问题 2：自然映射$\gamma$（满射）也将升级为同态？

对$\forall a,b\in M_1$，因为$\gamma(a)=[a]$，$\gamma(b)=[b]$，则：

$\gamma(a\circ b)=[a\circ b]$，$\gamma(a)\bullet\gamma(b)=[a]\bullet[b]=[a\circ b]$

所以$\gamma(a\circ b)=\gamma(a)\bullet\gamma(b)$，即为$M_1\to M_1/E_\varphi$上的满同态。

问题 3：双射$\overline{\varphi}$也将升级为同态？

对 $\forall [a],[b] \in {M_1}/{E_\varphi}$，由，$\overline{\varphi}([b]) = \varphi(b)$ 知：

$\overline{\varphi}([a] \bullet [b]) = \overline{\varphi}([a \circ b]) = \varphi(a \circ b) = \varphi(a) * \varphi(b)$

$\overline{\varphi}([a]) * \overline{\varphi}([b]) = \varphi(a) * \varphi(b)$

从而 $\overline{\varphi}([a] \bullet [b]) = \overline{\varphi}([a]) * \overline{\varphi}([b])$，即 $\overline{\varphi}$ 为 ${M_1}/{E_\varphi} \to M_2$ 的同态，又 $\overline{\varphi}$ 为双射，故 $\overline{\varphi}$ 为 ${M_1}/{E_\varphi} \to M_2$ 的同构，即 $M_2 \cong {M_1}/{E_\varphi}$。

**注**：这里希望大家知道其重要的方法论意义：先从已知探知未知（教材定理11.5.2，11.5.3），然后对未知的研究转化为对已知的研究（幺半群同态基本定理）。