离散数学之近世代数讲义附件(2)

12 章 群

定理

1. 证明 12.1 群的定义与第 11.3 节中的“每个元素均有逆元素的幺半群$(S,\circ)$称为群”的定义等价。

证明：$\Leftarrow$若$(S,\circ)$为幺半群且其中每个元素均可逆，则此时$(S,\circ)$显然满足群的定义中的 3 个条件，故$(S,\circ)$为群的定义的群。

$\Rightarrow$只须证明群的定义中的左单位元也为右单位元，同时群的定义中的左逆元也为右逆元即可。为此证明如下 2 个结论：

1）设b_l为a的左逆元，即$b_l \circ a = e_l$（e_l为左单位元），则有$a \circ b_l = e_l$。

2）对$\forall a \in G$，有$a \circ e_l = a$。

先证 1)：$\because ab_l = e_l(ab_l) = (b_l'b_l)(ab_l)$（其中$b_l'$为$b_l$的左逆元）

$$= b_l'(b_l a)b_l) = b_l'(e_l b_l) = b_l' b_l = e_l$$

$$\therefore\ ab_l = e_l$$

再证 2)：$\because a \circ e_l = a \circ (b_l \circ a) = (a \circ b_l) \circ a = e_l \circ a = a$

$\therefore e_l$为右单位元，从而为单位元e。

综上群的定义中的左单位元也为右单位元，左逆元也为右逆元即为逆元。

2. 教材 12.2 节定理 12.2.4

证明：1）$\because a^{-1} \circ a = a \circ a^{-1} = e$，$\therefore \left(a^{-1}\right)^{-1} = a$

2）$\because (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e$

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = e$$

$$\therefore (ab)^{-1} = b^{-1}a^{-1}$$

3. 教材 12.2 节定理 12.2.6

证明：$\Rightarrow$显然。

$\Leftarrow$根据群的定义只须证明 G 有左单位元及 G 中任意元素有左逆元。

1）左单位元e_l：由于对$\forall\ a, b \in G$，$ya = b$有解，则$yb = b$有解记为y_0，

即 $y_0 b = b$，又对 $\forall\ a \in G$，方程 $bx = a$ 有解记为 x_0，即 $bx_0 = a$

从而对 $\forall\ a \in G$ 有：$y_0 a = y_0(bx_0) = (y_0 b)x_0 = bx_0 = a$，故 y_0 为左单位元 e_l。

2）左逆元：对 $\forall\ a, b \in G$，$ya = b$ 有解，令 $b = e_l$ 则方程 $ya = e_l$ 有解 y_1，即

对 $\forall\ a \in G$ 均有左逆元。

4. 教材 12.2 节定理 12.2.8

证明：$\Rightarrow$ 显然。

$\Leftarrow$ 对 $\forall\ a \in G$，建立映射 $\varphi: G \to G$，对 $\forall\ x \in G$ 有 $\varphi(x) = a \circ x$，则对 $\forall x_1, x_2 \in G$，若 $x_1 \neq x_2$，则根据消去律知 $a \circ x_1 \neq a \circ x_2$，即 $\varphi(x_1) \neq \varphi(x_2)$，故 φ 为单射，从而 $|G| = |\varphi(G)|$，即 $|G| = |aG|$，又由 G 的有限性及 $aG \subseteq G$，则根据集合论的知识有 $aG = G$，即对 $\forall b \in G$，方程 $ax = b$ 在 G 中有解，同理可得方程 $ya = b$ 有解，根据定理 12.2.6 知 $(G, \circ)$ 为群。

//这里大家也可以用课堂的基本定义的证明方法，其主要原理就是有限集合上的双射为一 n 次置换，从而由置换的复合运算得到恒等映射。//

5. 教材 12.2 节定理 12.2.9

证明：设 $(G, \circ)$ 为群，且 $|G| = n$，对 $\forall a \in G(a \neq e)$，则有 $a^0, a^1, \cdots, a^n \in G$，而 $|G| = n$，故此 $n+1$ 个元素中至少有两个元素相同，即 $\exists i, j \in [0, n]$，使得 $a^i = a^j$（不妨设 $i > j$，从而 $0 < i - j \le n$），则有 $a^{i-j} = e$，从而元素 a 的阶不会超过 $i - j$，即元素 a 的阶不超过 G 的阶。

6. 教材 12.3 节定理 12.3.1

证明：1）设 G_1 的单位元为 e_1，G 的单位元为 e。

则对 $\forall x \in G_1$，有 $xe_1 = x$；又 $G_1 \subseteq G$，$\therefore x \in G$，则有 $xe = x$

从而 $xe_1 = xe$，则由消去律得：$e_1 = e$

2）设 G_1 的元素 a 在 G_1 中逆元素为 b_1，a 在 G 中的逆元素 b，则有：

$ab_1 = e_1 = e = ab$，根据消去律得：$b_1 = b$

7. 教材 12.3 节定理 12.3.2

证明：设 $\{G_\alpha\}_{\alpha \in I}$ 为群 G 的任意多个子群构成的集族，令 $H = \bigcap_{\alpha \in I} G_\alpha$。

1） H 非空：由 G_α 为子群，则 $e \in G_\alpha$，从而 $e \in \bigcap_{\alpha \in I} G_\alpha$，即 $e \in H$ 。

2） H 封闭性：对 $\forall a,b \in H$，则 $a,b \in \bigcap_{\alpha \in I} G_\alpha$，从而 $a,b \in G_\alpha$，又由 G_α 为子群，则有 $ab \in G_\alpha$，故有 $ab \in \bigcap_{\alpha \in I} G_\alpha$，即 $ab \in H$ 。

3）逆元：对于 $\forall a \in H$，则 $a \in G_\alpha$，又由 G_α 为子群，则 $a^{-1} \in G_\alpha$，从而 $a^{-1} \in \bigcap_{\alpha \in I} G_\alpha$，即 $a^{-1} \in H$ 。

注：这里可以直接调用定理 11.4.1 来证明，由此只需给出逆元素的证明即可。

8. 教材 12.3 节定理 12.3.3

证明：设 $(G,\circ)$ 为群，G_1, G_2 为 G 的真子群。

假设 $G = G_1 \bigcup G_2$，由 $G_1 \subset G$，$G_2 \subset G$ 知 $\exists a \notin G_1$ 且 $a \in G$，$b \notin G_2$ 且 $b \in G$，

而 $G = G_1 \bigcup G_2$，故有 $a \in G_2$，$b \in G_1$。

又 $(G,\circ)$ 为群，则有 $ab \in G$，从而 $ab \in G_1$ 或 $ab \in G_2$。

1）若 $ab \in G_1$，则由 $b \in G_1$ 及 G_1 子群知 $b^{-1} \in G_1$，从而 $(ab)b^{-1} \in G_1$（封闭性），

即 $a \in G_1$，与 $a \notin G_1$ 矛盾。

2）若 $ab \in G_2$，则由 $a \in G_2$ 及 G_2 子群知 $a^{-1} \in G_2$，从而 $a^{-1}(ab) \in G_1$（封闭性），

即 $b \in G_2$，与 $b \notin G_2$ 矛盾。

综上 $ab \notin G$，矛盾，故假设不成立。

9. 教材 12.3 节定理 12.3.4

证明：$\Rightarrow$ 显然。

$\Leftarrow$ 由已知只需证明 S 中有单位元即可。在 1）中令 $b = a^{-1}$ 则有：$e \in S$ 。

10. 教材 12.3 节定理 12.3.5

证明：$\Leftarrow$：1） $e \in S$：由已知令 $b = a$，则有 $e \in S$；

2）逆元：令 $a = e$ 则由已知对 $\forall$ $b \in S$，$b^{-1} \in S$；

3)封闭性：对 $\forall b \in S$，由 2) $b^{-1} \in S$，则由已知对 $\forall$ $a \in S$，则有 $a(b^{-1})^{-1} \in S$，

即 $ab \in S$ 。

11. 教材 12.3 节定理 12.3.6

证明：$\Rightarrow$ 显然。

$\Leftarrow$ 根据定理 12.2.8，只需证明 F 的封闭性即可（其上的结合律及消去律已自动成立）。封闭性显然。

12. 教材 12.3 节定理 12.3.7

证明：1）$e\in C$：因为对 $\forall x\in G$，$xe=ex=x$；

2）封闭性：对 $\forall a,b\in C$，则对 $\forall x\in G$，有

$(ab)x=a(bx)=a(xb)=(ax)b=(xa)b=x(ab)$，从而 $ab\in C$；

3）逆元：对 $\forall a\in C$，有 $ax=xa\Rightarrow xa^{-1}=a^{-1}x$，从而 $a^{-1}\in C$；

4）结合律：显然；

5）交换律：显然。

13. 教材 12.4 节定理 12.4.1

证明：设 $(G,*)$ 为群。

1）构造基于 G 的变换群

对 $\forall a\in G$，定义 $L(G)=\left\{f_a \middle| f_a:G\to G,\ f_a(x)=a*x,\ \forall x\in G\right\}$。

则由映射 f_a 的定义知其为单射、满射，从而为一一映射：

单射：对 $\forall x_1,x_2\in G$，若 $x_1\neq x_2$，则由消去律知 $a*x_1\neq a*x_2$，

即 $f_a(x_1)\neq f_a(x_2)$。

满射：对 $\forall y\in G$，显然 $a^{-1}*y\in G$，则 $f_a(a^{-1}*y)=a*(a^{-1}*y)=y$

即存在 $x=a^{-1}*y$，使得 $f_a(x)=y$。

2）$L(G)$ 关于映射的合成构成"$\circ$"构成变换群 $(L(G),\circ)$

结合律：映射的合成运算满足结合律。

封闭性：对 $\forall f_a$，$f_b\in L(G)$，

$\because\ f_a\circ f_b(x)=f_a(f_b(x))\qquad =f_a(b*x)=a*(b*x)\qquad =(a*b)*x$

$=f_{a*b}(x)$

$\therefore\ f_a\circ f_b=f_{a*b}$，由 $a*b\in G$ 知 $f_{a*b}\in G$。

单位元：令 $a=e$，则 $f_e(x)=e*x=x$ 为恒等映射。

逆元：对 $\forall f_a\in L(G)$，由 f_a 为双射知其逆映射 f_a^{-1} 为：

$f_a^{-1}(x)=a^{-1}*x=f_{a^{-1}}(x)$

由 $a\in G$ 知 $a^{-1}\in G$，从而映射 $f_{a^{-1}}\in L(G)$，即 $f_a^{-1}\in L(G)$。

注：根据幺半群的同构 Cayley 定理中的证明方法，知$(L(G),\circ)$至少为变换幺半群，故可以只需证明逆元即可。

3）构造同构映射

令$\varphi: G \to L(G)$，对$\forall a \in G$，$\varphi(a) = f_a$，则φ为一一映射：

单射：对$\forall a,b \in G$，若$a \neq b$，则对$\forall x \in G$，根据消去律知$a * x \neq b * x$，

即 $f_a \neq f_b$，从而$\varphi(a) \neq \varphi(b)$

满射：对$\forall f_a \in L(G)$，由 $f_a(x) = a * x$，且$a \in G$，故φ为满射。

同构：对$\forall a,b \in G$，由φ的定义知：$\varphi(a * b) = f_{a*b}$，又 $f_a \circ f_b = f_{a*b}$，

所以$\varphi(a * b) = f_a \circ f_b = \varphi(a) \circ \varphi(b)$

综上$\varphi: G \to L(G)$上的一个同构。

14. 教材 12.4 节定理 12.4.2

证明:设$(G,*)$为群。

1)封闭性:对$\forall f, g \in A(G)$,下证 $f \circ g \in A(G)$。

由 $f, g \in A(G)$知 f, g 为G上的双射，则由映射的复合知 $f \circ g$ 为G上的双射。又对$\forall a,b \in G$， $f \circ g(a * b) = f(g(a * b)) = f(g(a) * g(b))$

$$= f(g(a)) * f(g(b)) = (f \circ g(a)) * (f \circ g(b))$$

即 $f \circ g$ 为G上的自同构。

2）结合律：显然。

3）单位元：G上的恒等映射I_G。

4）逆元：对$\forall f \in A(G)$，下证 $f^{-1} \in A(G)$。

由 $f \in A(G)$知 f 为G上的双射，则 f^{-1}仍为G上的双射。

又对$\forall a,b \in G$，$\exists a',b' \in G$，使得$a = f(a')$，$b = f(b')$。且由 f 为G上的自同构，

则有 $f(a' * b') = f(a') * f(b')$，从而：

$f^{-1}(a * b) = f^{-1}(f(a') * f(b')) = f^{-1}(f(a' * b'))$

$= f^{-1} \circ f(a' * b') = I_G(a' * b') = a' * b' = f^{-1}(a) * f^{-1}(b)$

故 f^{-1} 仍为 G 上的自同构，即 $f^{-1} \in A(G)$。

14. 教材 12.4 节定理 12.4.3

证明：设 $(G,*)$ 为群，设 $B(G)$ 为 G 的内自同构之集，即：

$$B(G) = \{\varphi_a \mid \varphi_a(x) = a * x * a^{-1}, a \in G, \forall x \in G\}$$

下证 $(B(G), \circ)$ 为群。

1）封闭性：对 $\forall \varphi_a, \varphi_b \in B(G)$，$\varphi_a(x) = a * x * a^{-1}$，$\varphi_b(x) = b * x * b^{-1}$，则：

$$\varphi_a \circ \varphi_b(x) = \varphi_a(\varphi_b(x) = \varphi_a(b * x * b^{-1}) = a * (b * x * b^{-1}) * a^{-1} = (a * b) * x * (a * b)^{-1}$$

所以 $\varphi_a \circ \varphi_b \in B(G)$。

2）结合律：显然。

3）单位元：取 $a = e$ 即可知 $\varphi_e \in B(G)$。

4）逆元：对 $\forall \varphi_a \in B(G)$，$\varphi_a(x) = a * x * a^{-1}$，则：

$$\varphi_a^{-1}(x) = a^{-1} * x * a = a^{-1} * x * (a^{-1})^{-1},$$

所以 $\varphi_a^{-1} \in B(G)$。

15. PPT 讲义 2-5(教材 12.5 节)生成元的唯一性问题：

1）设 $G = (a)$，且 a 的阶为无穷，则 a 与 a^{-1} 均为 G 的生成元；

2）设 $G = (a)$，且 a 的阶为 n，则其生成元为 a^l，(l,n)＝1，$l > 1$

证明：1）设 $a^l (l \neq 1)$ 为 G 的另一生成元，则有 $G = (a^l)$，又 $G = (a)$，$\therefore a \in (a^l)$，

则 $\exists m \in Z$，使得 $a = (a^l)^m$，即 $a = a^{lm}$，$\Rightarrow a^{lm-1} = e$，又 a 的阶为无穷，

所以 $lm - 1 = 0$，$\Rightarrow lm = 1 \Rightarrow \begin{cases} l = 1, m = 1 \\ l = -1, m = -1 \end{cases}$，即 a^{-1} 为 G 的另一生成元。

2）由 1）同理可得 $\exists m \in Z$，使得 $a = (a^l)^m$，$\Rightarrow a^{lm-1} = e$，此时由 a 的阶为 n 知 $n \mid lm - 1$，即 $lm - 1 = kn \Rightarrow m \cdot l + (-k) \cdot n = 1$，即 (l,n)＝1。

16. 教材 12.6 节定理 12.6.2

证明：由定理 12.6.1 得：$a^{-1}b \in H \quad \Leftrightarrow a^{-1}bH = H$

$$\Leftrightarrow a(a^{-1}bH) = aH$$

$$\Leftrightarrow bH = aH$$

17. 教材 12.6 节定理 12.6.3

证明:1）若 $a^{-1}b \in H$, 则由定理 12.6.2 知 $aH = bH$ 。

2）若 $a^{-1}b \notin H$ ，则 $aH \neq bH$ 。假设此时 $aH \cap bH \neq \phi$ ，记 $d \in aH \cap bH$ ，则 $\exists h_1, h_2 \in H$ 使得 $d = ah_1$ ， $d = bh_2$ ，则有 $ah_1 = bh_2 \Rightarrow a^{-1}b = h_1{h_2}^{-1} \in H$ ，矛盾，故必有 $aH \cap bH = \phi$ 。

18. 教材 12.6 节定理 12.6.4

证明：由映射 $\varphi(x) = a \circ x$ 为单射知 $|aH| = |H|$ ，同理 $|bH| = |H|$ ，从而 $|aH| = |bH|$ 。

//注意上述结论对右陪集也成立。

19. 教材 12.6 节定理 12.6.7

证明：设 H 的互不相同的左陪集为：$a_1H, a_2H, \cdots, a_jH$ ，则由定理 5 知 $j = [G:H]$ 。

由定理 5 知： $G = a_1H \cup a_2H \cup \cdots \cup a_jH$ ，且任意两个不同的陪集互不相交，根据容斥原理有： $|G| = |a_1H| + |a_2H| + \cdots + |a_jH|$

又由定理 4 知 $|a_iH| = |H|$ ， $i = 1, 2, \cdots, j$

$\therefore N = n + n + \cdots + n = n.j$ ， 即 $N = n.[G:H]$ 。

20. 教材 12.6 节推论 12.6.1

证明：设 G 是一个阶为 N 的有限群， 对 $\forall a \in G (a \neq e)$ 设其阶为 r 。

则由 a 生成的子群 $H = (a) = \{e, a^1, \cdots, a^{r-1}\}$ ，则 $|H| = r$ ，根据 Lagrange 定理有 $r|N$ ，即每个元素的阶能整除该有限群的阶。

21. 教材 12.6 节推论 12.6.2

证明：不妨设 $P > 2$ ，则对 $\forall a \in G (a \neq e)$ ，则由推论 1 知其阶为 r 满足： $r|P$ ，

而 P 为素数，故有 $r = 1$ 或 $r = P$ ，由于 $a \neq e$ 故 $r > 1$ ，所以 $r = P$ 。

从而 $|(a)| = p$ ，又 $(a) \subseteq G$, $|G| = P$ ，则由集合论的知识得 $(a) = G$ ，即 G 是个循环群。

22. 教材 12.6 节推论 12.6.3

证明：对 $\forall a \in G (a \neq e)$ ，设其阶为 r ，则有 $a^r = e$ 。又根据推论 1 有 $r|N$ ，即 $N = r.q$ 。

从而 $a^N = a^{r\cdot q} = (a^r)^q = e^q = e$。

23. 教材 12.7 节定理 12.7.1

证明：1）证 $HH = H$

先证 $HH \subseteq H$：由 H 是 G 的子群，根据封闭性知 $HH \subseteq H$。

再证 $H \subseteq HH$：对 $\forall x \in H$，由 $e \in H$ 知 $x \in HH$，从而 $H \subseteq HH$。

2）证 $H^{-1} = H$

先证 $H^{-1} \subseteq H$：对 $\forall x \in H^{-1}$，则 $\exists a \in H$ 使得 $x = a^{-1} \Rightarrow x^{-1} = a \in H$，即 $x^{-1} \in H$，又 H 是 G 的子群，所以 $(x^{-1})^{-1} \in H$，即 $x \in H$，所以 $H^{-1} \subseteq H$。

再证 $H \subseteq H^{-1}$：对 $\forall a \in H$，由 H 是 G 的子群知 $a^{-1} \in H$，根据 H^{-1} 的定义知 $(a^{-1})^{-1} \in H^{-1}$，即 $a \in H^{-1}$，所以 $H \subseteq H^{-1}$。

24. 教材 12.7 节定理 12.7.2

证明：$\Rightarrow$ 由 AB 是 G 的子群根据定理 1 有：$AB = (AB)^{-1}$，则有：$AB = B^{-1}A^{-1}$，

又 A, B 是群 G 的子群则有 $A = A^{-1}, B = B^{-1}$，所以 $AB = BA$。

$\Leftarrow$ 直接由子群的判定定义来证明：

1）封闭性：因为 $(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB)$，而 A, B 是群 G 的子群，所以 $AA \subseteq A, BB \subseteq B$，故有 $(AA)(BB) \subseteq AB$，从而 $(AB)(AB) \subseteq AB$，即满足封闭性。

2）结合律：显然；

3）单位元：由 A, B 是群 G 的子群知 $e \in AB$；

4）逆元：对 $\forall a \in A, b \in B$，$(ab)^{-1} = b^{-1}a^{-1} \in B^{-1}A^{-1}$，而 $A = A^{-1}, B = B^{-1}$，从而 $(ab)^{-1} \in BA$，又 $AB = BA$，所以 $(ab)^{-1} \in AB$。

25. 教材 12.7 节定理 12.7.3

证明：证 $3) \Rightarrow 1)$：即需证 $aH = Ha$

先证 $aH \subseteq Ha$：由 $aHa^{-1} \subseteq H \Rightarrow (aHa^{-1})a \subseteq Ha \Rightarrow aH \subseteq Ha$

再证 $Ha \subseteq aH$：由于对 $\forall a \in G$，有 $a^{-1} \in G$，从而 $a^{-1}H(a^{-1})^{-1} \subseteq H$，

即 $a^{-1}Ha \subseteq H$，则 $a(a^{-1}Ha) \subseteq aH$，即 $Ha \subseteq aH$。

综上 $aH = Ha$。

26. 教材 12.7 节定理 12.7.5

证明：1）先证 S_l 对群子集乘法"$\bullet$"构成一个代数系 $(S_l, \bullet)$

只需证"$\bullet$"为 S_l 上的一个二元代数运算。

①运算的封闭性：对 $\forall a_1H, b_1H \in S_l$，由 H 是群 G 的正规子群，

则有 $(a_1H)\bullet(b_1H) = a_1(Hb_1)H = a_1(b_1H)H = a_1b_1(HH) = a_1b_1H \in S_l$

②"$\bullet$"为二元映射

即需证若 $a_2H = a_1H$，$b_2H = b_1H$，则需证 $(a_2H)\bullet(b_2H) = (a_1H)\bullet(b_1H)$

由①得 $(a_2H)\bullet(b_2H) = a_2b_2H$，$(a_1H)\bullet(b_1H) = a_1b_1H$

根据子群的陪集的性质：$a_2H = a_1H \Rightarrow a_2^{-1}a_1 \in H$，

则 $\exists h_1 \in H$, 使得 $a_2^{-1}a_1 = h_1 \Rightarrow a_1 = a_2h_1$

同理由 $b_2H = b_1H \Rightarrow b_2^{-1}b_1 \in H$

则 $\exists h_2 \in H$, 使得 $b_2^{-1}b_1 = h_2 \Rightarrow b_1 = b_2h_2$

从而 $a_1b_1H = (a_2h_1)(b_2h_2)H = a_2(h_1b_2)h_2H$

又 H 是群 G 的正规子群则有：$Hb_2 = b_2H$，则对 $h_1 \in H, \exists h_3 \in H$，

使得 $h_1b_2 = b_2h_3$，从而 $a_2(h_1b_2)h_2H = a_2b_2(h_3h_2)H = a_2b_2H$。

（因为 $h_3h_2 \in H$，所以 $(h_3h_2)H = H$）

2）结合律：显然；

3）单位元：对 $\forall aH \in S_l$ 有 $(aH)\bullet(eH) = (eH)\bullet(aH) = aH$，

所以 eH 即 H 为 S_l 的单位元；

4）逆元：对 $\forall aH \in S_l$，

由①知：$(aH)\bullet(a^{-1}H) = (a^{-1}H)\bullet(aH) = eH = H$（$H$ 为 S_l 的单位元）

所以对 $\forall aH \in S_l$，其逆为 $a^{-1}H$。

27. 教材 12.8 节定理 12.8.1

证明：1）先证$\varphi(e_1)=e_2$

由φ为G_1到G_2的一个同态知：$\varphi(e_1)=\varphi(e_1\circ e_1)=\varphi(e_1)*\varphi(e_1)$

$\Rightarrow \varphi(e_1)=\varphi(e_1)*\varphi(e_1)$，则由消去律得：$\varphi(e_1)=e_2$

2）再证$\varphi(a^{-1})=[\varphi(a)]^{-1}$

由φ为G_1到G_2的一个同态，则有$\varphi(a^{-1})*\varphi(a)=\varphi(a^{-1}\circ a)=\varphi(e_1)=e_2$

同理有：$\varphi(a)*\varphi(a^{-1})=e_2$，所以$\varphi(a^{-1})=[\varphi(a)]^{-1}$。

28. 教材 12.8 节定理 12.8.3

证明：1）先证$\varphi^{-1}(e_2)$为G_1的子群：具体参见习题作业 12.3.（5）。

2）再证$\varphi^{-1}(e_2)$为G_1的正规子群，记$H=\varphi^{-1}(e_2)$

只需证对$\forall a\in G_1$，$aHa^{-1}\subseteq H$

即只需证对$\forall h\in H$，$a\circ h\circ a^{-1}\in H$，则只需证$\varphi(a\circ h\circ a^{-1})=e_2$

由φ是群$(G_1,\circ)$到群$(G_2,*)$的满同态，则有：

$\varphi(a\circ h\circ a^{-1})=\varphi(a)*\varphi(h)*\varphi(a^{-1})$，又$\varphi(h)=e_2$，所以

$\varphi(a\circ h\circ a^{-1})=\varphi(a)*e_2*\varphi(a^{-1})=\varphi(a)*\varphi(a^{-1})=\varphi(a\circ a^{-1})=\varphi(e_1)=e_2$。

综上$\varphi^{-1}(e_2)$为G_1的正规子群。

28. 教材 12.8 节定理 12.8.4

证明：

1)A．封闭性：$\forall x,y\in\varphi(H)$，则由φ为满射知：$\exists\, t_1,t_2\in H$，使得：$x=\varphi(t_1)$，

$y=\varphi(t_2)$，则$x*y=\varphi(t_1)*\varphi(t_2)=\varphi(t_1*t_2)\in\varphi(H)$

B．结合律：显然

C．单位元：$e_2=\varphi(e_1)$

C．逆元：对$\forall x\in\varphi(H)$，$\exists\, t\in H$，使得$x=\varphi(t)$，则$x^{-1}=(\varphi(t))^{-1}=\varphi(t^{-1})\in\varphi(H)$

2）只需要证明$\varphi(N)$的正规性，即证对$\forall x\in G_2$有$x*\varphi(N)*x^{-1}\subseteq\varphi(N)$。

同 1）对 $\forall x \in G_2$，$\exists\, t \in G_1$，使得 $x = \varphi(t)$，则 $x^{-1} = \varphi(t^{-1})$

又对 $\forall\, h \in \varphi(N)$，$\exists\, h_0 \in N$，使得 $h = \varphi(h_0)$

则 $x * h * x^{-1} = \varphi(t) * \varphi(h_0) * \varphi(t^{-1}) = \varphi(t \circ h_0 \circ t^{-1})$

由 N 正规知：$t \circ h_0 \circ t^{-1} \in N$，所以 $x * h * x^{-1} \in \varphi(N)$

从而有 $x * \varphi(N) * x^{-1} \subseteq \varphi(N)$。

3）记 $H = \varphi^{-1}(\overline{H}) = \{x \mid x \in G_1 \wedge \varphi(x) \in \overline{H}\}$

A．封闭性：对 $\forall x, y \in H$，则 $\varphi(x \circ y) = \varphi(x) * \varphi(y)$，由 $\varphi(x) \in \overline{H}$，$\varphi(y) \in \overline{H}$ 及 $\overline{H}$ 为子群知 $\varphi(x) * \varphi(y) \in \overline{H}$，从而 $\varphi(x \circ y) \in \overline{H}$，所以 $x \circ y \in H$

B．结合律：显然

C．单位元：由 $e_2 \in \overline{H}$，而 $e_2 = \varphi(e_1)$，所以 $e_1 \in \varphi^{-1}(\overline{H}) = H$

D．逆元：对 $\forall x \in H$，则 $\varphi(x) \in \overline{H}$ 且 $(\varphi(x))^{-1} = \varphi(x^{-1})$，而 $\overline{H}$ 为子群，所以 $(\varphi(x))^{-1} \in \overline{H}$，即 $\varphi(x^{-1}) \in \overline{H}$，故有 $x^{-1} \in \varphi^{-1}(\overline{H}) = H$

4）记 $N = \varphi^{-1}(\overline{N})$

同上只需要证明正规性，即证对 $\forall x \in G_1$ 有 $x \circ N \circ x^{-1} \subseteq N$。

或只需要证对 $\forall h \in N$ 有 $x \circ h \circ x^{-1} \in N$，从而只需要证 $\varphi(x \circ h \circ h^{-1}) \in \overline{N}$。

由 $\varphi(x \circ h \circ x^{-1}) = \varphi(x) * \varphi(h) * \varphi(x^{-1}) = \varphi(x) * \varphi(h) * (\varphi(x))^{-1}$，且 $\varphi(x) \in G_2$，$\varphi(h) \in \overline{N}$ 及 $\overline{N}$ 为正规子群知：$\varphi(x) * \varphi(h) * (\varphi(x))^{-1} \in \overline{N}$，则 $\varphi(x \circ h \circ x^{-1}) \in \overline{N}$。

29. 教材 12.8 节定理 12.8.5

证明：定义 $\varphi : G \to G/N$，且对 $\forall a \in G$，$\varphi(a) = aN$，则显然 φ 为满射。

下证 φ 为 G 到 G/N 的同态。

对 $\forall a, b \in G$，根据 φ 的定义有 $\varphi(a \circ b) = (ab)N$，

又 $\varphi(a) \cdot \varphi(b) = (aN) \cdot (bN) = a(Nb)N = a(bN)N = (ab)NN = (ab)N$

从而 $\varphi(a \circ b) = \varphi(a) \cdot \varphi(b)$，即 φ 为 G 到 G/N 的同态。

由商群G/N的单位元为N，则

$$Ker\ \varphi=\varphi^{-1}(N)=\{a|\ \varphi(a)=N, a\in G\}=\{a|\ aN=N, a\in G\}=\{a|\ a\in N\}=N$$

即$Ker\ \varphi=N$

30. 教材 12.8 节定理 12.8.6

证明：主要是找到一个G_1/E到G_2的双射，且满足同构方程。

1）商群G_1/E存在：由定理 3 知$E=Ker\ \varphi$为正规子群，故商群G_1/E存在。

2）定义$\overline{\varphi}:G_1/E\to G_2$，对$\forall aE\in G_1/E$ (其中$a\in G_1$)，有：

$$\overline{\varphi}(aE)=\varphi(a)$$

下证$\overline{\varphi}$为双射：

①$\overline{\varphi}$为映射：即需证对$\forall aE,bE\in G_1/E$，若$aE=bE$，则有$\overline{\varphi}(aE)=\overline{\varphi}(bE)$。

由$aE=bE\Rightarrow a^{-1}b\in E$，则由$E$的构造知$\varphi(a^{-1}b)=e_2$（$e_2$为$G_2$的单位元），又由$\varphi$是群$(G_1,\circ)$到群$(G_2,*)$的满同态得：

$\varphi(a^{-1}b)=\varphi(a^{-1})*\varphi(b)=e_2\Rightarrow(\varphi(a))^{-1}*\varphi(b)=e_2\Rightarrow\varphi(a)=\varphi(b)$，

则由$\overline{\varphi}$的定义知$\overline{\varphi}(aE)=\overline{\varphi}(bE)$。

②$\overline{\varphi}$为单射：对$\forall aE,bE\in G_1/E$，若$aE\neq bE$，下证$\overline{\varphi}(aE)\neq\overline{\varphi}(bE)$。

若$\overline{\varphi}(aE)=\overline{\varphi}(bE)$，则由$\overline{\varphi}$的定义知$\Rightarrow\varphi(a)=\varphi(b)\Rightarrow(\varphi(a))^{-1}*\varphi(b)=e_2$

$\Rightarrow\varphi(a^{-1})*\varphi(b)=e_2\Rightarrow\varphi(a^{-1}b)=e_2\Rightarrow a^{-1}b\in E\Rightarrow aE=bE$，矛盾。

③$\overline{\varphi}$为满射：由$\overline{\varphi}$的定义显然成立。

综上$\overline{\varphi}$为双射

3）再证$\overline{\varphi}$为G_1/E到G_2同构：即对$\forall aE,bE\in G_1/E$，需证

$$\overline{\varphi}((aE)\cdot(bE))=\overline{\varphi}(aE)*\overline{\varphi}(bE)$$

因为$\overline{\varphi}((aE)\cdot(bE))=\overline{\varphi}(abE)=\varphi(ab)=\varphi(a)*\varphi(b)=\overline{\varphi}(aE)*\overline{\varphi}(bE)$

所以$\overline{\varphi}$为G_1/E到G_2同构。