武汉大学计算机学院
《离散数学》第六次练习

§7.1.1 加、减、乘和除是否为下列集合的二元运算：

(1) $\mathbb{R}$;

(2) $\mathbb{R}^* \triangleq \mathbb{R} - \{0\}$;

(3) $\mathbb{Z}_+ \triangleq \{n \mid n \in \mathbb{Z} \wedge n > 0\}$;

(4) $\mathbb{O}_d \triangleq \{2n+1 \mid n \in \mathbb{Z}\}$;

(5) $A = \{2^n \mid n \in \mathbb{Z}\}$;

(6) $B = \{a\sqrt{2} + b \mid a, b \in \mathbb{Z}\}$;

解:

运算	(1)	(2)	(3)	(4)	(5)	(6)
$+$	✓	✗	✓	✗	✗	✓
$-$	✓	✗	✗	✗	✗	✓
$\times$	✓	✓	✓	✓	✓	✓
$\div$	✗	✓	✗	✗	✓	✗

□

§7.1.2 设$*$是集合A上的二元运算，e和$\mathbf{0}$分别是关于$*$的单位元和零元. 试证明: 若$|A| > 1$, 则$e \neq \mathbf{0}$.

证明: 反证法：设$e = \mathbf{0} \because |A| \geqslant 2$, 则$\exists a \in A \wedge a \neq e$. 这样$a = a * e = a * \mathbf{0} = \mathbf{0}$. 矛盾. □

§7.1.4 定义$\mathbb{Z}$上的运算$*$: $x * y = x + y - xy$，证明：$*$是可交换的和可结合的，求出其单位元，并指出每个可逆元的逆元；

证明:

(1) $*$是可结合的:

$$\begin{aligned} & (x * y) * z \\ = {} & (x + y - xy) * z \\ = {} & x + y - xy + z - (x + y - xy)z \\ = {} & x + y + z - xy - yz - zx + xyz \end{aligned}$$

同理：

$$x * (y * z) = x + y + z - xy - yz - zx + xyz$$

$\therefore$

$$(x * y) * z = x * (y * z)$$

(2) $*$的幺元是：0；

(3) 仅2有逆元，其逆元是其自身. □

§7.1.7 下述二元运算$*$是否为可交换的、可结合的？是否有左单位元、右单位元、单位元？
下述运算定义在实数集$\mathbb{R}$上:

(1) $x * y = x + 2y$; (2) $x * y = |x - y|$;
(3) $x * y = \frac{x+y}{2}$;

以下运算定义在整数$\mathbb{Z}_+$上:

(4) $m * n = m^n$; (5) $m * n = (m, n)$.
(6) $m * n = [m, n]$;

其中$(m, n), [m, n]$分别表示m和n的最大公因子与最小公倍数.
解:

运算	(1)	(2)	(3)	(4)	(5)	(6)
交换律	✗	✓	✓	✗	✓	✓
结合律	✗	✗	✗	✗	✓	✓
左单位元	✗	✗	✗	✗	1	✗
右单位元	0	✗	✗	0	1	✗
单位元	✗	✗	✗	✗	1	✗

□

§7.1.8 设$|A| = n$，A上有多少个二元运算，其中有多少个对称运算？有多少个运算有么元？

解:

(1) 等于有多少个$A \times A \longrightarrow A$的函数, 而$|A^{A\times A}| = n^{n^2}$;

(2) 等价于运算表有多少个对称矩阵，即n阶方正对角线(包括该线)以上选择n个元素有多少不同的可能：$n^{\frac{n(n+1)}{2}}$；

(3) 设$a \in A$是某运算的幺元，则在运算表中a所对应的行和列唯一确定，因此以a为幺的运算有$n^{(n-1)^2}$，故有幺的运算共有：$nn^{(n-1)^2} = n^{(n-1)^2+1}$. □

§7.1.9 设$*$是A上可结合的二元运算，且$\forall a, b \in A$，若$a * b = b * a$，则$a = b$;

(1) $\forall a \in A,\ a * a = a$, 即$a$是幂等元(*idempotent element);*

(2) $\forall a, b \in A,\ a * b * a = a$*;*

(3) $\forall a, b, c \in A,\ a * b * c = a * c$*;*

证明:

(1) $\because$
$$\underbrace{(a * a)}_{b} * a = a * \underbrace{(a * a)}_{b}$$
$\therefore$
$$a * a = a$$

(2) $\because$
$$\begin{aligned} & \underbrace{(a * b * a)}_{\mathcal{B}} * a \\ = {} & a * b * (a * a) \\ = {} & a * b * a \\ = {} & a * a * (b * a) \\ = {} & a * \underbrace{(a * b * a)}_{\mathcal{B}} \end{aligned}$$
$\therefore$
$$a * b * a = a$$

(3) $\because$
$$\begin{aligned} & (a * b * c) * a * c \\ = {} & (a * (b * c) * a) * c \\ = {} & a * c \end{aligned}$$
又
$$\begin{aligned} & a * c * (a * b * c) \\ = {} & a * (c * (a * b) * c) \\ = {} & a * c \end{aligned}$$
$\therefore$
$$(a * b * c) * a * c = a * c * (a * b * c)$$
故
$$a * b * c = a * c$$

□

§7.2.1 考察代数系统$A = \langle \mathbb{N}, \cdot \rangle$和$B = \langle \{0, 1\}, \cdot \rangle$, 其中$\cdot$为普通乘法运算. 函数$f : \mathbb{N} \longrightarrow \{0, 1\}$定义为

$$f(n) = \begin{cases} 1, & \text{若} \exists k \in \mathbb{N} \text{使得 } n = 2^k; \\ 0, & \text{否则.} \end{cases}$$

试证明: f是从A到b的同态.

证明: 由于运算满足交换律，所以只需下述三种情况讨论：

① $m = 2^p \wedge n = 2^q$:

$$f(m{\cdot}n) = f(2^p{\cdot}2^q) = f(2^{p+q}) = 1 = f(2^p){\cdot}f(2^q) = f(x){\cdot}f(y)$$

② $m = 2^p \wedge (\forall q \in \mathbb{N}, n \neq 2^q)$. 即$q$含有非2的质因子，所以$mn$也含有非2质音质，这样$mn$也不具有$2^r$形式, 故

$$f(m \cdot n) = 0 = f(m) \cdot f(n)$$

③ m和n都不是仅有2作为其质因子. 则mn也不可能仅有2作为其质因子，即不具有2^r形式, 则

$$f(m \cdot n) = 0 = f(m) \cdot f(n)$$

故f是同态. □

§7.2.3 下述函数f中哪些是$\langle \mathbb{R}^+, \cdot \rangle$的自同态?

(1) $f(x) = |x|$; ✓ (2) $f(x) = x^3$; ✓

(3) $f(x) = 2x$; ✗ (4) $f(x) = x + 1$. ✗

§7.2.4 令$\mathbb{E}_v$为偶数集. 试证明：$\langle \mathbb{Z}, \cdot \rangle$与$\langle \mathbb{E}_v, \cdot \rangle$ 不同构.

证明: 反证法：$\langle \mathbb{Z}, \cdot \rangle$有单位元1，设$f$是$\langle \mathbb{Z}, \cdot \rangle$到$\langle \mathbb{E}_v, \cdot \rangle$ 上的同构. 则$f(1)$是$\langle \mathbb{E}_v, \cdot \rangle$上的单位元，但是$\langle \mathbb{E}_v, \cdot \rangle$上没有单位元，矛盾. □

§7.2.5 设A为集合. 试证明：$\langle \mathscr{P}(A), \cup \rangle \cong \langle \mathscr{P}(A), \cap \rangle$同构.

证明: 定义函数$h : \mathscr{P}(A) \longrightarrow \mathscr{P}(A), X \longmapsto \overline{X}$, 则$h$是双射，且

$$h(X \cup Y) = \overline{X \cup Y} = \overline{X} \cap \overline{Y} = h(X) \cap h(Y)$$

故h是$\langle \mathscr{P}(A), \cup \rangle$到$\langle \mathscr{P}(A), \cap \rangle$的同构. □

§7.2.8 设$\langle \{\, 1, 2, 3, 4 \,\}, \times_5 \rangle$和$\langle \{\, 0, 1, 2, 3 \,\}, +_4 \rangle$是否同构.

答: 同构. 定义函数$h : \{\, 0, 1, 2, 3 \,\} \longrightarrow \{\, 1, 2, 3, 4 \,\}, n \longmapsto 2^n \mod 5$. 则可验证$h$是双射，且

$$h(m +_4 n) = 2^{m+n} \mod 5 = 2^m \times_5 2^n = h(m) \times_5 h(n)$$

即h是$\langle \{\, 0, 1, 2, 3 \,\}, +_4 \rangle$到$\langle \{\, 1, 2, 3, 4 \,\}, \times_5 \rangle$上的同构. □

§7.2.9 (1) 证明：$\langle \mathbb{N}_m, +_m \rangle$的自同态恰好$m$个;

证明: $\forall k \in \mathbb{N}_m$, 易验证$h : \mathbb{N}_m \longrightarrow \mathbb{N}_m, n \longmapsto nk \mod m$是$\mathbb{N}_m$上的自同态.
设h'是$\mathbb{N}_m$上的自同态，则$\forall n \in \mathbb{N}_m$,

$$h'(n) = h'(\underbrace{1 +_m 1 +_m \cdots +_m 1}_{n\text{个}1}) = nh'(1) \mod m$$

即h'由$h'(1)$唯一确定. 即$n \longmapsto knk$是同态的唯一形式. 而k的可能的取值为$0, 1, \ldots m-1$. 故自同态的个数为m.

(2) 描述从$\langle \mathbb{N}, + \rangle$到$\langle \mathbb{N}_m, +_m \rangle$的所有同态集合;

解: $\langle \mathbb{N}, + \rangle$到$\langle \mathbb{N}_m, +_m \rangle$上的同态$h$只有唯一的形式$n \longmapsto kn \mod m$(其中$k$为常数), 故同态集合为$\{ h \mid h : \mathbb{N} \longrightarrow \mathbb{N}_m, n \longmapsto kn \mod m, k \in \mathbb{N} \}$

(3) 描述从$\langle \mathbb{N}_2, +_2 \rangle$到$\langle \mathbb{N}_3, +_3 \rangle$的所有同态集合.

解: 设h是$\mathbb{N}_2$到$\mathbb{N}_3$上的同态，则$h(1)$的阶数应为2和2公因子，而2和3的公因子为1. 故$h(1) = 0, \therefore \forall n \in \mathbb{N}_2, h(n) = nh(1) \mod 3 = 0$. 所以$h(n) = 0$, 即$\mathbb{N}_2$到$\mathbb{N}_3$只有唯一的同态$h : \mathbb{N}_2 \longrightarrow \mathbb{N}_3, n \longmapsto 0$. □

§7.3.1 下述关系R是否为$\langle \mathbb{Z}, + \rangle$上的同余关系?

(1) iRj 当且仅当$i \cdot j \geqslant 0$;

解: 不是. 如$\langle -1, -3 \rangle \in R \wedge \langle 2, 2 \rangle \in R$, 但是$\langle -1+2, -3+2 \rangle \notin R$.

(2) iRj 当且仅当$i \leqslant 0 \wedge j \leqslant 0 \vee i > 0 \wedge j > 0$;

解: 不是. 如$\langle -1, -3 \rangle \in R \wedge \langle 2, 2 \rangle \in R$, 但是$\langle -1+2, -3+2 \rangle \notin R$.

(3) iRj 当且仅当$|i - j| \leqslant 4$;

解: 不是. 如$\langle -1, -5 \rangle \in R \wedge \langle -1, 5 \rangle \in R$, 但是$\langle -1-1, -5-5 \rangle \notin R$.

(4) iRj 当且仅当$i \geqslant j$;

解: 不是. 不是对称关系，所以不是等价关系. □

§7.3.2 设$m, n \in \mathbb{Z}_+$. $\mathbb{Z}$上的一元运算$*$定义为：$\forall i \in \mathbb{Z}, *(i) = i^n$. 试证明: $\equiv_n$是代数系统$\langle \mathbb{Z}, * \rangle$上的同余关系.

证明: 模m关系是等价关系. 设$i = j \mod m$，则$\exists p \in \mathbb{Z} \wedge i - j = pm$, 这样$i^n - j^n = (i-j)P(i,j)$ ($P(i,j)$是以i和j为变量的多项式). 即$*(i) - *(j)$也是m的倍数. 故$*(i) \equiv_m *(i)$. $\equiv_m$是同余关系. □

§7.3.4 设R是$\mathbb{N}_3$上的等价关系. 试证明若R对$+_3$有置换性质，则R对$\times_3$也有置换性质. 请举例说明若R对$\times_3$有置换性质，R对$+_3$却未必有置换性质.

证明: 根据群论定理，群上的同余关系一定由正规子群所诱导. 而N_3是交换群，因此其上的同余关系由其子群诱导即可. 而N_3仅有两个平凡子群N_3和$\{0\}$，其对应的同余关系分别是全域关系和恒等关系. 因此它们对运算$\times_3$也是同余关系. 而等价类集合$\{\{0\},\{1,2\}\}$所诱导的等价关系R对运算$\times_3$保持置换性，但是对$+_3$没有置换性, 如$\langle 1,1\rangle \in R \wedge \langle 1,2\rangle \in R$, 但$\langle 1 +_3 1, 1 +_3 1\rangle = \langle 2,0\rangle \notin R$. □

§7.3.5 试证明：同一代数系统上的两个同余关系的交仍为同余关系. 举例说明它们的合成不一定是同余关系.

证明: 设R_1和R_2是代数系统$\langle A, *\rangle$上的同余关系($*$为二元运算). 则根据关系定理有$R_1 \cap R_2$ 是A上的等价关系. 设$a\mathcal{R}_1 \cap R_2 b \wedge cR_1 \cap R_2 d$, 则$aR_1 b \wedge cR_2 d \wedge aR_2 b \wedge cR_2 d$. 即有$a * cR_1 b * d \wedge a * cR_2 b * d$, $\therefore a * cR_1 \cap R_2 c * d$. 故$R_1 \cap R_2$是同余关系. 而根据习题\$4.4.2得知两个等价关系的合成不一定是等价关系，故更不可能是同余关系. □

§7.4.4 记$A_m = \langle N_m, +_m\rangle$.

(2) 证明：$A_m \times A_n \cong A_{mn}$当且仅当$m$和$n$互素.

证明:

$\Longleftarrow$ 定义函数h: $A_m \times A_n \longrightarrow A_{mn}, \langle p,q\rangle \longmapsto pn + qm \mod mn$, 则可验证$h$是群$A_m \times A_n$到群$A_{mn}$上的同态. 又$(m,n) = 1$, 根据Bézout引理存在$r, s \in \mathbb{Z}$使得$rn + sm = 1$. 设$r' = r \mod m, s' = s \mod n$, 则$\exists i,j \in \mathbb{Z}, r = mi + r', s = mj + s'$, $\therefore mni + r'n + mnj + s'm = 1$, 即$r'n + s'm \equiv_{mn} 1$, 所以存在$\langle r', s'\rangle \in A_m \times A_n$, $h(r', s') = 1$. 这样$\forall k \in A_{mn}$, $k = k1 = kh(r', s') = h(kr', ks')$. 故$h$是满射. 而$|A_m \times A_n| = mn = |A_{mn}|$, $\therefore$ h是双射，所以h是同构，即$A_m \times A_n \cong A_{mn}$.

$\Longrightarrow$ 设h是$A_m \times A_n$到A_{mn}上的同构，设$h(\langle 1,0\rangle) = n', h(\langle 0,1\rangle) = m'$, 则$h(\langle p,q\rangle) = n'p + m'q$. 定义函数$\phi : A_m \longrightarrow A_{mn}, x \longmapsto h(i_{A_m}(x))$, 其中$i_{A_m} : A_m \longrightarrow A_m \times A_n, x \longmapsto \langle x, 0\rangle$为嵌入同态. 则$\phi$为单同态，且$\phi(x) = n'x$. 即$A_m \cong \phi(A_m)$, 而$\phi(A_m) = \langle n'\rangle$, 所以$m = |A_m| = |n'| = mn/(n', mn)$, 即$\exists i, n' = in$; 同理$\exists j, m' = jm$. 另一方面由于$h$是满射，这样存在$\langle r,s\rangle \in A_m \times A_n$, $n'r + m's = 1 \mod mn$. 即$\exists t, rin + sjm = 1 + tmn$. 由此$(ri - tm)n + sjm = 1$. 根据Bézout引理$(m,n) = 1$, 即$m$和$n$互素. □

§8.1.4 设半群$\langle S, *\rangle$中消去律成立，S是交换半群，iff，$\forall a, b \in S$, $(a * b)^2 = a^2 * b^2$;

证明:

$\Longrightarrow$ $(a * b)^2 = (a * b) * (a * b) = a * a * b * b = a^2 * b^2$;

$\Longleftarrow$ $\forall a, b \in S$:

$\because$ $(a * b)^2 = a^2 * b^2$

即 $a * b * a * b = a * a * b * b$

等式两边消去a:

$$b * a * b = a * b * b$$

等式两边消去b:

$$b * a = a * b$$

故$*$满足交换率. □

§8.1.5 设$\langle \{ a, b \}, *\rangle$是半群，其中$a * a = b$，证明：

(1) $a * b = b * a$;

(2) $b * b = b$;

证明:

(1) $a * b = a * (a * a) = (a * a) * a = b * a$;

(2) 设$a * b = a$，则：

$$b * b = (a * a) * b = a * (a * b) = a * a = b$$

设$a * b = b$，则：

$$b * b = (a * a) * b = a * (a * b) = a * b = b$$

故：$b * b = b$ □

§8.1.6 试证明每个有限半群中一定有一个幂等元.

证明:

设$\langle S, *\rangle$是任意的一个有限半群，则$\{ a^i \mid i \in \mathbb{N}^+ \}$是一个有限集

合，根据抽屉原则，$\exists j, k \in \mathbb{N}^+$:

$$a^j = a^{j+k}$$

用归纳法证明：$\forall n \in \mathbb{N}^+$，有

$$a^{kj} * a^{nk} = a^{jk}$$

(i) $n = 1$时，if $k = 1$，then $a^j = a^{j+1}$, 而$a^{kj} * a^k = a^{j+1}$; $a^{jk} = a^j$, ∴结论成立；
if $k > 1$

$$\begin{array}{ll} \because & a^j = a^{j+k} \\ \therefore & a^{(k-1)j} * a^j = a^{(k-1)j} * a^{j+k} \\ \text{即} & a^{jk} = a^{jk+k} \end{array}$$

(ii) 设$n-1$时有:

$$a^{kj} * a^{(n-1)k} = a^{jk}$$

(iii) 当n时：

$$\begin{array}{ll} \because & a^{kj} * a^{(n-1)k} = a^{jk} \\ \therefore & a^{kj} * a^{(n-1)k} * a^k = a^{jk} * a^k = a^{jk+k} \\ \text{而} & a^{jk} = a^{jk+k} \\ \therefore & a^{kj} * a^{nk} = a^{jk} \end{array}$$

当$n = k$时有：

$$a^{jk} * a^{jk} = a^{jk}$$

这样a^{jk}就是幂等元. □

§8.2.1 下列代数系统中哪些是群，交换群？

(1) $\langle \mathcal{M}_{m\times n}, + \rangle$;
交换群.

(2) $\langle \{ 1, 2, 3, 4, 6, 12 \}, \gcd \rangle$;
不是群，没有么元.

(3) $\langle \{ a + b\sqrt{2} \,|\, a, b \in \mathbb{Q} \}, + \rangle$;
交换群.

(4) $\langle \{ z \,|\, z \in \mathbb{C} \wedge |z| = 1 \}, + \rangle$;
不是群，运算不封闭.

(5) $\langle \{ z \,|\, z \in \mathbb{C} \wedge |z| = 1 \}, \times \rangle$;
交换群.

(6) $\langle \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}, \cdot \rangle$;
交换群. □

§8.2.7 设$\langle G,*,e\rangle$为群，试证明：$\forall a,b\in G,\ n\in\mathbb{Z}$，有

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

证明:
对n用归纳法：

(i) $n=0$时，$(a*b*a^{-1})^0=e=a*a^{-1}=a*e*a^{-1}=a*b^0*a^{-1}$

(ii) 设$\forall n\in\mathbb{N}$，有

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

(iii) $n+1$时，有

$$\begin{aligned}&(a*b*a^{-1})^{n+1}\\=&(a*b*a^{-1})^n*(a*b*a^{-1})\\=&a*b^n*a^{-1}*a*b*a^{-1}\\=&a*b^n*e*b*a^{-1}\\=&a*b^n*b*a^{-1}\\=&a*b^{n+1}*a^{-1}\end{aligned}$$

而

$$\begin{aligned}&(a*b*a^{-1})^{-(n+1)}\\=&((a*b*a^{-1})^{-1})^{n+1}\\=&(a*b^{-1}*a^{-1})^{n+1}\\=&a*(b^{-1})^{n+1}*a^{-1}\\=&a*b^{-(n+1)}*a^{-1}\end{aligned}$$

故对任意的$n\in\mathbb{Z}$，原式成立. □

§8.2.8 设$\langle G,*,e\rangle$为群，$a,b\in G,\ a\neq e$，并且$a^4*b=b*a^5$ 试证明：$a*b\neq b*a$.

证明(反证法):
设$a*b=b*a$，则:

$$b*a^5=a^5*b=a^4*b$$

由于群满足消去律，等式两边消去a^4：

$$a*b=b$$

再消去b：

$$a=e$$

与条件矛盾. □

§8.2.9 设$\langle G,*,e\rangle$为群，$\forall a,b\in G$，$a^3*b^3=(a*b)^3$, $a^5*b^5=(a*b)^5$ 试证明：G是Abelian;

证明:
$\because$

$$a^3 * b^3 = (a * b)^3 = a * b * a * b * a * b$$

$\therefore$

$$a^2 * b^2 = b * a * b * a = (b * a)^2 \tag{1}$$

而

$$\begin{aligned} & a^5 * b^5 \\ =&(a * b)^5 \\ =&a * (b * a)^4 * b \\ =&a * (a^2 * b^2)^2 * b \\ =&a * a^2 * b^2 * a^2 * b^2 * b \\ =&a^3 * b^2 * a^2 * b^3 \end{aligned}$$

$\therefore$

$$a^5 * b^5 = a^3 * b^2 * a^2 * b^3$$

等式两边消去a^3和b^3

$$a^2 * b^2 = b^2 * a^2 \tag{2}$$

由(1)和(2)得

$$b^2 * a^2 = b * a * b * a$$

即

$$b * a = a * b$$

故$*$满足交换率. □

§8.2.15 设$\langle G, *, e\rangle$为群，$a, b \in G$，且$a * b = b * a$，试证明：若$(|a|, |b|) = 1$，则$|a * b| = |a| \times |b|$.

证明: 设$|a| = m$, $|b| = n$, 设$\langle a\rangle$和$\langle b\rangle$分别是由元素a和b生成的子群，则$|\langle a\rangle| = m \wedge |\langle b\rangle = n|$. 则根据讲义例题(设$G$为有限群，$H \leqslant G \wedge K \leqslant G$，并且$(|H|, |K|) = 1$，则$H \cap K = \{ e \}$)有$\langle a\rangle \cap \langle b\rangle = \{ e \}$. 设$|a * b| = p$. $\because (a * b)^{mn} = a^{mn} * b^{nm} = (a^m)^n * (b^n)^m = e$. 这样$p \leqslant mn$; 又$(a * b)^p = e$, 则$a^p * b^p = e$, 即$a^p = (b^{-1})^p \in \langle a\rangle \cap \langle b\rangle = \{ e \}$. $\therefore a^p = (b^{-1})^p = e$. 即$m \big| p \wedge n \big| p$, 而$(m, n) = 1$, so $mn \big| p$. 即$mn \leqslant p$. 故$mn = p$. □

§8.2.16 设$\langle G, *, e\rangle$为交换群，a为G中阶数最大的元素，且$|a| = n$. 试证：若$\forall b \in G$，则$|b| \big| |a|$.

证明: 设$|b| = m$, $(n, m) = p$, 设p的质因分解为：$p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, 则$\forall i \in 1, 2, \ldots, k, p_i^{r_i} | m \wedge p_i^{r_i} | n$，且$m/p_i^{r_i}$和$n/p_i^{r_i}$中一定有一个没有$p_i$因子，定义函数$f : \{ 1, 2, \ldots, k \} \longrightarrow \{ 0, 1 \}$

$$f(i) = \begin{cases} 1 & \text{如果} m/p_i^{r_i} \text{中没有} p_i \text{因子} \\ 0 & \text{否则} \end{cases}$$

定义$s=(p_1^{r_1})^{f(1)}(p_2^{r_2})^{f(2)}\cdots(p_k^{r_k})^{f(k)}$, $t=(p_1^{r_1})^{1-f(1)}(p_2^{r_2})^{1-f(2)}\cdots(p_k^{r_k})^{1-f(k)}$, 则$(m/s,n/t)=1$ 且$st=p$, 而$|a^s|=m/s\wedge|b^t|=n/t$, 这样a^t和b^s的阶数互素. 根据习题§8.2.15有$|a^s*b^t|=\frac{mn}{st}=\frac{mn}{p}\leqslant n$, $\therefore m\leqslant p$. 而p是n和m的最大公约数，因此$p\leqslant m$. 即$p=m$. 故m整除n. □

§8.3.1 设$\langle G,*,e\rangle$为群，$H\leqslant G$，$K\leqslant G$，试证明：$H\cap K\leqslant G$，$H\cup K$是G的子群吗？

证明:

(i) 运算的封闭性:
$\forall a,b\in H\cap K$, 则$a,b\in H\wedge a,b\in K$，$\therefore a*b\in H\wedge a*b\in K$，$\therefore a*b\in H\cap K$;

(ii) 么元在$H\cap K$中：
$e\in H\wedge e\in K$, $\therefore e\in H\cap K$;

(iii) 取逆运算的封闭性：
设$a\in H\cap K$, 则$a\in H\wedge a\in K$, $\therefore a^{-1}\in H\wedge a^{-1}\in K$, $\therefore a^{-1}\in H\cap K$；

(iv) $H\cup K$不一定是G的子群:
如：$3\mathbb{Z}\leqslant\mathbb{Z}$，$4\mathbb{Z}\leqslant\mathbb{Z}$，$3\mathbb{Z}\cup 4\mathbb{Z}$ 不是$\mathbb{Z}$的子群，因为运算不封闭. □

§8.3.2 设$\langle G,*,e\rangle$为群，$H\leqslant G$，$K\leqslant G$，$HK\triangleq\{\,h*k\,|\,h\in H\wedge k\in K\,\}$，试证明：$HK\leqslant G$，iff，$HK=KH$

证明:

$\Longrightarrow$ 证明集合相等:
$\forall h\in H\wedge k\in K$, $\because e\in H\cap K$, $\therefore h=h*e\in HK\wedge k=e*k\in HK$, $\because HK\leqslant G$, $\therefore k*h\in HK$, so $KH\subseteq HK$.
$\therefore k^{-1}*h^{-1}\in KH\subseteq HK$, So $\exists h'\in H\wedge k'\in K$, $k^{-1}*h^{-1}=h'*k'$, hence $h*k=(k^{-1}*h^{-1})^{-1}=(h'*k')^{-1}=k'^{-1}*h'^{-1}\in KH$, 即$HK\subseteq KH$,
故$HK=KH$.

$\Longrightarrow$ (i) 运算的封闭性：
$\forall h,h'\in H\wedge k,k'\in K$, then $k*h'\in KH=HK$, so $\exists h''\in H\wedge k''\in K$, $k*h'=h''*k''$, hence $(h*k)*(h'*k')=h*(k*h')*k'=(h*h'')*(k''*k')\in HK$.

(ii) $e\in H\cap K$, so $e=e*e\in HK$.

(iii) 取逆运算的封闭性：
设$h*k \in HK$, then $(h*k)^{-1} = k^{-1}*h^{-1} \in KH = HK$.
$\therefore$ 取逆运算是封闭的.

由此, $HK \leqslant G$. □

§8.3.3 设$\langle G, *, e\rangle$是群，$a \in G$，令$H \triangleq \{\, x \mid x \in G \wedge a*x = x*a \,\}$，试证明：$H \leqslant G$

证明:

(i) $e \in H$：$\because a*e = e*a = a$;

(ii) 运算封闭性：$\forall x, y \in H$, $a*(x*y) = x*(a*y) = (x*y)*a$, so $x*y \in H$;

(iii) 取逆运算的封闭性：$\because \forall x \in H$, $a*x = x*a$, 则$x^{-1}*a*x = a$, $x^{-1}*a = a*x^{-1}$. 这样$x^{-1} \in H$. 取逆运算是封闭的. □

§8.3.4 设$\langle G, *, e\rangle$是群，$H \leqslant G$，$a \in G$. 令$aHa^{-1} \triangleq \{\, a*x*a^{-1} \mid x \in H \,\}$，试证明：$aHa^{-1} \leqslant G$

证明: 定义函数$h : G \longrightarrow G, x \longmapsto a*x*a^{-1}$, 根据习题§8.3.8, h是自同构，则$h(H) \leqslant G$, 而$h(H) = aHa^{-1}$，故$aHa^{-1} \leqslant H$. □

§8.3.5 证明：$\langle \mathbb{Q}, +\rangle$与$\langle \mathbb{Q}^*, \times\rangle$不同构，其中$\mathbb{Q}^* = \mathbb{Q} - \{\, 0 \,\}$.

证明:如果$\langle \mathbb{Q}, +\rangle$与$\langle \mathbb{Q}^*, \times\rangle$同构, 则两者之间子群也一一对应, 但是，$\{\, 1, -1 \,\} \leqslant \langle \mathbb{Q}^*, \times\rangle$，而$\langle \mathbb{Q}, +\rangle$上没有非平凡的有限子群. 因为设$H$是$\langle \mathbb{Q}, +\rangle$的一个非平凡子群，则$\exists x \in H \wedge x \neq 0$. 这样$\forall n \in \mathbb{Z}$, $nx \in H$. 故H的阶数无限. 故两个群不同构. □

§8.4.3 求8阶循环群所有的生成于那及所有的子群.

解:

(i) 8阶循环群同构$\langle N_8, \overline{+}\rangle$, N_8的生存元有：$1, 3, 5, 7$;

(ii) N_8的子群有：$\{\, 0 \,\}$, $\{\, 0, 4 \,\}$, $\{\, 0, 2, 4, 6 \,\}$和N_8. □

§8.4.4 设G是没有非平凡子群的有限群，试证明G是平凡群或质数阶数的循环群

证明: $G \neq \{\, e \,\}$，则$|G| \geqslant 2$. 设$a \in G \wedge a \neq e$，则$\langle a\rangle \leqslant G$且$\langle a\rangle \neq \{\, e \,\}$. 由于$G$仅有平凡子群，这样$\langle a\rangle = G$, $\therefore G$是循环群. 如果$|G|$不是质数, 即存在$p > 1 \wedge q > 1 \wedge |G| = pq$，则$|a^p| = q \neq |G|$，即$|\langle a^p\rangle| \neq 1 \wedge |\langle a^p\rangle| \neq |G|$. G有一个非平凡的子群. 故G的阶数必须是质数. □

§8.4.5 设$G = \langle a\rangle$是n阶循环群，$m \in \mathbb{Z}_+$, 且$(m,n) = d$. 试证明：$\langle a^m\rangle = \langle a^d\rangle$.

证明: $(m,n) = d$, 根据Bezout定理，$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$. 这样$\forall p \in \mathbb{Z}$, $\exists q \in \mathbb{Z}$，$mp = dq$, 这样$(a^m)^p = a^{mp} = a^{mp} = a^{dq} = (a^d)^q$, 即$\langle a^m\rangle \subseteq \langle a^d\rangle$; 反之，$\forall q \in \mathbb{Z}$, $\exists r, s \in \mathbb{Z}$, $dq = mr + ns$, 这样，$(a^d)^q = a^{dq} = a^{mr+ns} = a^{mr} * a^{ns} = (a^m)^r * (a^n)^s = (a^m)^r * e = (a^m)^r$, 即$\langle a^d\rangle \subseteq \langle a^m\rangle$. 故$\langle a^m\rangle = \langle a^d\rangle$. □

§8.4.6 设G是循环群，$G \sim G'$. 试证: G'也是循环群.

证明: 根据循环群的定义: G是循环群当且仅当存在满同态$h : \mathbb{Z} \longrightarrow G$. $\because G \to G' \therefore \exists$满同态$f : G \longrightarrow G'$, 这样$f \circ h : \mathbb{Z} \longrightarrow G'$是$\mathbb{Z}$到$G'$上的满同态, 即$G'$是循环群. □

§8.4.7 设G是无限阶循环群，G'是任意的循环群，试证：$G \sim G'$.

证明: 设$G = \langle a\rangle$, $G' = \langle b\rangle$，则$\because G$是无限阶循环群，$\therefore a$为无限阶. 定义函数$h : G \longrightarrow G'$, $a^n \longmapsto b^n$. 设$m, n \in \mathbb{Z}, m \neq n$. 则$a^m \neq a^n$, 否则$a^{m-n} = e$, 破坏了$a$的无限阶. 这样$h$有定义. 则$\forall a^m, a^n \in G$, $h(a^m * a^n) = h(a^{m+n}) = b^{m+n} = b^m \cdot b^n$. 即$h$是同态. $\forall y \in G', \exists p \in \mathbb{Z}, b^p = y$, 则$h(a^p) = b^p = y$. 即$h$是满同态, 故$G \sim G'$. □

§8.4.8 试证明：$C_m \times C_n \cong C_{mn}$当且仅当$(m,n) = 1$, 其中$C_m$表示$m$阶循环群.

证明:

必要性 设$C_m \times C_n \cong C_{mn}$, 则存在同构$h : C_m \times C_n \longrightarrow C_{mn}$. 而设$H = C_m \times \{e\}$, $K = \{e\} \times C_n$, 则H和K分别是$C_m \times C_n$的阶数为m和n的子群, 且$HK = C_m \times C_n$. 这样$h(H)$和$h(K)$是C_{mn}上的子群，且$|h(H)| = m \wedge |h(K)| = n \wedge h(H)h(K) = C_{mn}$. 设$c$是$C_{mn}$的生成元，则$\langle c^n\rangle$是$C_{mn}$的唯一一个阶数为$m$的子群，$\langle c^m\rangle$是$C_{mn}$的唯一一个阶数为$n$的子群. 这样$h(H) = \langle c^n\rangle \wedge h(K) = \langle c^m\rangle$, 而$h(H)h(K) = C_{mn}$, $\therefore \exists pq \in \mathbb{Z} c^{nq}c^{mq} = c$, 即$c^{mq+nq} = c$, 这样$mp + nq = 1 \mod mn$. 根据Bezout定理有$(m,n) = 1$.

充分性 设C_{mn}的生成元是c. 则$\langle c^n\rangle$和$\langle c^m\rangle$分别是C_{mn}的两个阶数为m和n的循环子群. $\because C_{mn}$是交换群，这样根据习题§8.3.2有$\langle c^n\rangle\langle c^m\rangle = \langle c^m\rangle\langle c^n\rangle$, 即$\langle c^n\rangle\langle c^m\rangle \leqslant C_{mn}$. 根据讲义例题(设$G$为有限群，$H \leqslant G \wedge K \leqslant G$，并且$(|H|, |K|) = 1$，则$H \cap K = \{e\}$)有$\langle c^n\rangle \cap \langle c^m\rangle = \{e\}$. 根据Bezout定

理有$\exists pq \in \mathbb{Z},\ pm + qn = 1$. 即$\forall x \in C_{mn},\ \exists t \in \mathbb{Z},\ x = c^t = (c^n)^{qt}(c^m)^{pt} \in \langle c^n\rangle\langle c^m\rangle$. 这样$C_{mn} \subseteq \langle c^n\rangle\langle c^m\rangle$. 即$\langle c^n\rangle\langle c^m\rangle = C_{mn}$. 定义函数$h : \langle c^n\rangle \times \langle c^m\rangle \longrightarrow \langle c^n\rangle\langle c^m\rangle, \langle x, y\rangle \longmapsto xy$. 则易验证$h$是同态. 设$h(\langle x, y\rangle) = h(\langle x', y'\rangle)$，则$xy = x'y'$, 即$x'^{-1}x = y'y^{-1} \in \langle c^n\rangle \cap \langle c^m\rangle$. $\therefore x'^{-1}x = y'y^{-1} = e$. 即$h$是单射，而$|\langle c^n\rangle \times \langle c^m\rangle| = |\langle c^n\rangle\langle c^m\rangle| = mn$, 故$h$是满射，即$h$是同构. 又$\langle c^n\rangle \cong C_m \wedge \langle c^m\rangle \cong C_m$. 故$C_m \times C_n \cong C_{mn}$. □

§8.5.3 $H \leqslant G$, 证明H在G的所有左右陪集中有一个并只有一个是子群.

证明:

(i) H是一个H诱导的左陪集：$\because eH = H$;

(ii) H是唯一的一个成子群的陪集：设aH是子群，则$e \in aH$，而$e \in H$, $\therefore e \in aH \cap H \neq \varnothing$, 而陪集是$G$的划分，$\therefore H = aH$. □

§8.5.6 证明6阶群恰好有一个3阶子群.

证明: 设$|G| = 6$, $a \in G \wedge a \neq e$，则根据Lagrange定理a的阶数只有下述三种可能:

(i) $|a| = 6$, 则G是循环群，则G同构N_6，而N_6的唯一一个3阶子群为$\{0, 2, 4\}$.

(ii) 设$|a| = 3$，则$H = \{e, a, a^2\}$是G的一个3阶子群. 设$b \notin H$，则$|b| = 2$，否则, 设$|b| = 3$,即$b \neq b^2 \neq e$, 这样H, bH和b^2H为三个两两交为空的左陪集，且每个都已3为基数, 即$|H \cup bH \cup b^2H| = 9$, 而$H \cup bH \cup b^2H \subseteq G \wedge |G| = 6$，矛盾. 即$H$是$G$的唯一一个阶数为3的子群.

(iii) G中没有阶数为3的元素，即$\forall x \in G - \{e\}, |x| = 2$，这样根据习题§8.2.11，$G$是交换群. 设$a, b \in G - \{e\}$, 且$a \neq b$，则$\{e, a, b, ab\}$是$G$的一个阶数为4的子群，但根据 Lagrange 定理G 的子群的阶数只可能是G阶数的因子，即1、2、3或6. 矛盾. 因此G必定有一个阶数为3的元素. □

§8.5.7 证明10阶交换群一定是循环群.

证明: 设$|G| = 10$, $a \in G \wedge a \neq e$，则根据Lagrange定理a的阶数只有下述3种可能:

(i) $|a| = 10$, 则G是循环群.

(ii) 设$|a| = 5$，则$H = \{e, a, a^2, a^3, a^4\}$是$G$的一个5阶子群. 设$b \notin H$，则$|b| \neq 5$，否则, 设$|b| = 5$,即$b \neq b^2 \neq b^3 \neq b^4 \neq e$, 这样$H, bH, b^2H, b^3H$和$b^4H$为5个两两交为空的左陪集，且每个都已5为基数, 即$|H \cup bH \cup b^2H \cup b^3H \cup b^4H| = 25$, 而$H \cup bH \cup b^2H \cup b^3H \cup b^4H \subseteq G \wedge |G| = 10$，矛盾. 设$|b| = 10$，则$b$是$G$的生成元，即$G$是循环群. 设$|b| = 2$，则根据讲义例题(设$G$是Abelian, $a, b \in G$, $|a| = p$, $|b| = q$, $(p, q) = 1$, 则$|ab| = |a||b| = pq$.)有$|ab| = 10$, 即ab是G的生成元.

(iii) G中没有阶数为5的元素，即$\forall x \in G - \{e\}, |x| = 2$，设$a, b \in G - \{e\}$, 且$a \neq b$，则$\{e, a, b, ab\}$是$G$的一个阶数为4的子群，但根据Lagrange定理$G$ 的子群的阶数只可能是G阶数的因子，即1、2、5或10. 矛盾. 因此G必定有一个阶数为5的元素. □

§8.6.1 求出4次交代群A_4中$H = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$的左、右陪集，并验证$H$是$A_4$的正规子群.

证明: A_4是有4次对称群S_4上的所有偶置换组成的群，因为偶置换的合成还是偶置换，所以对合成运算封闭，恒等变换也是偶置换，所以幺元也是偶置换，偶置换的反函数也是偶置换，所以它构成子群，称为交代群(Alternating Group).

$$\begin{aligned} A_4 = \{&(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),\\ &(1,2,3), (1,3,2), (2,3,4), (1,3,4),\\ &(1,4,3), (1,2,4), (1,4,3), (1,4,2)\} \end{aligned}$$

这样

$$\begin{aligned} &(1)H = (1,2)(3,4)H = (1,3)(2,4)H = (1,4)(2,3)H = H\\ &H(1) = H(1,2)(3,4) = H(1,3)(2,4) = H(1,4)(2,3) = H; \end{aligned}$$

$$\begin{aligned} (1,2,3)H &= (1,3,4)H = (1,2,4)H = (1,4,2)H\\ &= \{(1,2,3), (1,3,4), (1,4,3), (1,4,2)\}\\ H(1,2,3) &= H(1,3,4) = H(1,2,4) = H(1,4,2)\\ &= \{(1,2,3), (1,3,4), (1,4,3), (1,4,2)\}; \end{aligned}$$

$$\begin{aligned}(1,3,2)H &= (2,3,4)H = (1,3,4)H = (1,4,3)H\\ &= \{(1,3,2),(2,3,4),(1,3,4),(1,4,3)\}\\ H(1,3,2) &= H(2,3,4) = H(1,3,4) = H(1,4,3)\\ &= \{(1,3,2),(2,3,4),(1,3,4),(1,4,3)\}.\end{aligned}$$

由上可得，左右陪集相等，因此H是A_4的正规子群. □

§8.6.2 令$G = \left\{\begin{pmatrix} r & s\\ 0 & 1\end{pmatrix}\middle| r,s\in\mathbb{Q}, r\neq 0\right\}$，则$G$关于矩阵乘法构成群. 令$H = \left\{\begin{pmatrix} 1 & t\\ 0 & 1\end{pmatrix}\middle| t\in\mathbb{Q}\right\}$，试证明：$H$是$G$的不变子群.

证明:首先证明G是群：

(i) 单位矩阵$\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}\in G$;

(ii) 设$M = \begin{pmatrix} r & s\\ 0 & 1\end{pmatrix}\in G$, 则$M^{-1} = \begin{pmatrix} 1/r & -s/r\\ 0 & 1\end{pmatrix}\in G$, 即取逆运算封闭;

(iii) 设$M = \begin{pmatrix} r & s\\ 0 & 1\end{pmatrix}\in G$, $M' = \begin{pmatrix} r' & s'\\ 0 & 1\end{pmatrix}\in G$, $MM' = \begin{pmatrix} rr' & rs'+s\\ 0 & 1\end{pmatrix}\in G(\because rr'\neq 0)$.

由上所述G对矩阵乘法构成群.

再整H是群：

(i) 单位矩阵$\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}\in H$;

(ii) 设$N = \begin{pmatrix} 1 & t\\ 0 & 1\end{pmatrix}\in H$, 则$N^{-1} = \begin{pmatrix} 1/ & -t\\ 0 & 1\end{pmatrix}\in H$, 即取逆运算封闭;

(iii) 设$N = \begin{pmatrix} 1 & t\\ 0 & 1\end{pmatrix}\in H$, $N' = \begin{pmatrix} 1 & t'\\ 0 & 1\end{pmatrix}\in H$, $NN' = \begin{pmatrix} 1 & t+t'\\ 0 & 1\end{pmatrix}\in H$.

由上所述H对矩阵乘法构成群. 而$H\subseteq G$, 故$H\leqslant G$.

最后证明$H \lhd G$：设$M \in G$, $N \in H$如上所述，则：

$$\begin{aligned} MNM^{-1} &= \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1/r & -s/r \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -\dfrac{s(rt+s)}{r} \\ 0 & 1 \end{pmatrix} \in H \end{aligned}$$

这样$MHM^{-1} \in H$, 即$H \lhd G$. □

§8.6.3 群G的中心$C(G)$定义为$C(G) = \{\, a \,|\, a \in G \wedge \forall x \in G, ax = xa \,\}$, 证明：$C$是$G$的不变子群

证明: 首先证明$C \leqslant G$. $\because \forall x \in G ex = xe$, $\therefore e \in C$; $\forall c, c' \in C$, $\forall x \in G$, $x(cc') = cxc' = (cc')x$, 这样$cc' \in C$, 即C对运算封闭；而$x^{-1}c = cx^{-1}$，这样$(x^{-1}c)^{-1} = (cx^{-1})^{-1}$, 即$c^{-1}x = cc^{-1}$, 故$c^{-1} \in C$, 即取逆运算封闭. $\therefore C \leqslant G$.
再证$C \lhd G$. 设$\forall c \in C$, $\forall a \in G$, $\forall x \in G$, 则

$$\begin{aligned} x(aca^{-1}) &= x(aa^{-1})c \\ &= xc \\ &= cx \\ &= aa^{-1}cx \\ &= (aca^{-1})x \end{aligned}$$

$\therefore aca^{-1} \in C$, 这样$\forall a \in G$, $aCa^{-1} \in C$, 即$C \lhd G$. □

§8.6.4 $H \leqslant G$, $N(H) \triangleq \{\, n \,|\, n \in G, nHn^{-1} = H \,\}$, 证明：$H \lhd N(H)$

证明:

(i) $H \subseteq N$:
$\forall h \in H, \forall x \in H$, $x = h * (h^{-1} * x * h) * h^{-1} \in hHh^{-1}$, so $hHh^{-1} \subseteq H \subseteq hHh^{-1}$, hence $hHh^{-1} = H$, 即$h \in N(H)$.

(ii) $N \leqslant G$:

(1) 运算的封闭性：
$\forall a, b \in N(H)$, $bHb^{-1} = H$, $(a*b)H(a*b)^{-1} = a(bHb^{-1})a^{-1} = aHa^{-1} = H$, so $a * b \in H$

(2) $e \in H \subseteq N(H)$,

(3) 取逆运算的封闭性：
设$a \in N(H)$, then $aHa^{-1} = H$, so $Ha^{-1} = a^{-1}H$, $\therefore a^{-1}Ha = H$, hence $a^{-1} \in H$

(iii) $H \lhd N(H)$
由上有: $H \subseteq N(H) \wedge N(H) \leqslant G$, So $H \leqslant N(H)$.
$\because \forall n \in N(H)$, $nHn^{-1} = H$, so $H \lhd N(H)$. □

§8.6.6 设$H \lhd G, K \lhd G$, 证明：$H \cap K \lhd G \wedge HK \lhd G$

证明:

(i) $H \cap K \lhd G$:
(1) $H \cap K \leqslant G$.
(2) $H \cap K \lhd G$: $\forall a \in G$,
$$a(H \cap K)a^{-1} \subseteq aHa^{-1} \subseteq H$$
$$a(H \cap K)a^{-1} \subseteq aKa^{-1} \subseteq K$$
so $a(H \cap K)a^{-1} \subseteq H \cap K$, 故$H \cap K \lhd G$.

(ii) $HK \lhd G$:
(1) $HK \leqslant G$: $\forall k \in K$, 有$Hk = kH$, so
$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH$$
根据习题§8.3.2有：$HK \leqslant G$
(2) $HK \lhd G$: $\forall a \in G$,
$$\begin{aligned} & aHK \\ = {} & (aH)K \\ = {} & (Ha)K \\ = {} & H(aK) \\ = {} & HKa \end{aligned}$$
so $HK \leqslant G$. □

§8.6.8 设H是循环群G的子群, 证明：G/H也是循环群.

证明: G是循环群，则G是可交换群, 这样H一定是G的正规子群，G/H有定义, 设a是G的生成元, 则同态$h : \mathbb{Z} \longrightarrow G$, $n \longmapsto a^n$是满同态，而函数$f : G \longrightarrow G/H$, $x \longmapsto xH$也是满同态，这样$f \circ h$是$\mathbb{Z}$到G/H上的满同态，即$G/H = \{ (f(h(1))^n \mid n \in \mathbb{Z} \}$, 即$G/H$是循环群. □

§8.6.9 设$H \lhd G, K \lhd G$, 且G/H, G/K是可交换的，证明：$G/(H \cap K)$也是可交换的.

证明: 由习题§8.6.6得知$H \cap K \lhd G$，$\therefore$ $G/(H \cap K)$有定义.
$\because$ G/H, G/K是可交换的, 则$\forall a, b \in G$:
$$abH = baH$$
$$abK = baK$$

这样

$$\begin{aligned}
&(a(H\cap K))*(b(H\cap K))\\
=&\,ab(H\cap K)\\
=&\,abH\cap abK\\
=&\,baH\cap baK\\
=&\,ba(H\cap K)\\
=&\,(b(H\cap K))*(a(H\cap K))
\end{aligned}$$

故$G/(H\cap K)$是可交换的. □

§8.6.10 设f是从群G_1到G_2上的满同态，$H_2\lhd G_2$. 证明: $G_1/f^{-1}(H_2)\cong G_2/H_2$.

证明: 定义函数$g:G_2\longrightarrow G_2/H_2, y\longmapsto yH_2$，则$g$是满同态. $\ker(g)=H_2$. 证明$\ker(g\circ f)=f^-1(H_2)$: 根据ker的定义有$\ker(g\circ f)=\{\,x\,|\,x\in G_1\wedge g(f(x))=H_2\,\}=\{\,x\,|\,x\in G_1\wedge f(x)\in H_2\,\}=f^{-1}(H_2)$, 由于$g\circ f$是满同态，这样$G_1/f^{-1}(H_2)\cong G_2/H_2$. □

§8.6.11 设$K\lhd G$，$H\leqslant G$. 证明: $H/(H\cap K)\cong HK/K$.

证明: $\because K\lhd G$, $\therefore\forall h\in H$, $hK=kH$, 这样

$$HK=\bigcup_{h\in H}hK=\bigcup_{h\in H}Kh=KH.$$

由习题§8.3.2有$HK\leqslant G$，而$\forall hk\in HK, hkKk^{-1}h^{-1}=hKh^{-1}=K$, 即$K\lhd HK$. 这样$HK/K$有定义.

定义函数$f:H\longrightarrow HK/K, h\longmapsto hHK$，则$\forall hkK\in HK/K$, $\because kK=K$, $\therefore hkK=hK$, 即$f(H)=\{\,hK\,|\,h\in H\,\}=HK/K$，$f$是满同态. 而$\ker(f)=\{\,h\,|\,h\in H\wedge f(h)=K\,\}=\{\,h\,|\,hK=K\,\}$, 而$hK=K$当且仅当$h\in K$, 故$\ker(h)=H\cap K$, 即$H/(H\cap K)\cong HK/K$. □