商群

2023 年 8 月 7 日

目录

1 商群

在这小节，我们将利用模m同余来构造群。一旦完成这个步骤，我们将能够使用群论来证明费马定理。这种构造是一种更普遍的从已给定的群中建立新群的方法的原型，我们一般叫商群。

1.1 定义：等价类

给定$m \geq 2$和$a \in Z$，则$a \mod m$的等价类是一个Z中的子集$[a]$：

$$\begin{aligned}[a] =&\{b \in Z : b \equiv a \mod m\} \\ =&\{a + km : k \in Z\} \\ =&\{\cdots, a-2m, a-m, a, a+m, a+2m, \cdots\}\end{aligned}$$

且我们定义所有模m的同余类构成的族称为**模m整数类**，记为I_m

例如，若$m = 2$，则$[0] = \{b \in Z : b \equiv 0 \mod 2\}$是所有偶数的集合。而$[1] = \{b \in Z : b \equiv 1 \mod 2\}$是所有奇数的集合。注意$[2] = \{b \in Z : b \equiv 2 \mod 2\}$也是所有偶数的集合，所以$[2] = [0]$，事实上$[0] = [2] = [-2] = [4] = [-4] = \cdots$

注意： 给定m，我们可以得到Z的循环子群$\langle m \rangle$由生成元m决定。我们可以简单的检查一下同余类$[a]$是陪集$a + \langle m \rangle$

我们定义$a + \langle m \rangle$为

$$a + \langle m \rangle = \{a + km : k \in Z\}$$

所以这个陪集实际上就是一个等价类$[a]$

记号$[a]$实际上不是一个好的记号，因为它没有提到模m。例如$[1]$在I_2中不同于$[1]$在I_3中的情况。因为前者是奇数的集合后者是满足$\{1 + 3k : k \in Z\} = \{\cdots, -2, 1, 4, \cdots\}$。但这不会有太大的问题，因为我们基本每次只处理一个。若还是怕混淆，我们就用$[a]_m$表示I_m中a的同余类。

1.1.1 引理：

I_m中的同余类$[a] = [b]$当且仅当$a \equiv b \mod m$

证明： 若$[a] = [b]$，则$a \in [a]$。并且$a \in [a] = [b]$有$a \equiv b \mod m$

反之，若$c \in [a]$，则$c \equiv a \mod m$由传递性可知$c \equiv b \mod m$，则$[a] \subseteq [b]$，通过对称性，则$b \equiv a \mod m$，则$[b] \subseteq [a]$，因此$[a] = [b]$

换句话说，这个命题告诉我们，我们可以有一种方法，吧同余符号变成相等符号，代价就是吧a, b用等价类$[a], [b]$代替。

特别的，I_m中$[a] = [0]$当且仅当$a \equiv 0 \mod m$。所以$[a] = [0]$当且仅当m是a的因子

1.1.2　命题：

给定$m \geq 2$，则

1. 若$a \in Z$，则存在r使得$[a] = [r]$,$0 \leq r < m$
2. 若$0 \leq r' < r < m$，则$[r'] \neq [r]$
3. I_m恰好有m个元素，即$[0], [1], \cdots, [m-1]$

证明：　对每个$a \in Z$，由除法算式给出$a = qm + r$，其中$0 \leq r < m$，因此$a - r = qm$有$a \equiv r \mod m$。这意味着$[a] = [r]$，其中r是a除m后的余数。

若$r \equiv r' \mod m$，则有$m \mid r - r'$意味着$r - r' \geq m$，但$r - r' \leq r < m$这是一个矛盾，所以$r' \not\equiv r \mod m$，所以$[r'] \neq [r]$

命题1证明了每个$[a]$的等价类$[r]$都在$I_m = \{[0], [1], \cdots, [m-1]\}$中，并且利用命题2可知$[r]$没有重复的类。

现在，我们通过加法来使得I_m变成一个阿贝尔群。引理1.1.1告诉我们$[a] = [b]$当且仅当$a \equiv b \mod m$，所以每个$[a] \in I_m$有很多记号。而我们重新定义I_m上的运算将依赖于记号的选择，这使得我们不得不证明这个运算是定义良好的。

1.1.3　引理：

若$m \geq 2$，则函数$\alpha : I_m \times I_m \to I_m$：

$$\alpha([a], [b]) = [a + b]$$

是一个I_m上的运算

证明： 该运算看上去依赖于我们选择记号$[a]$和$[b]$，如果我们选择了记号$[a'], [b']$呢？为了看到α是一个良好定义的函数，我们必须证明若$[a] = [a']$和$[b] = [b']$有$\alpha([a],[b]) = \alpha([a'],[b'])$，即$[a+b] = [a'+b']$。而这正是我们在同余中学过的一个命题：

若 $a_i \equiv a_i' \mod m$，$i = 1, 2, 3, \cdots, n$，则

$$a_1 + \cdots + a_n \equiv a_1' + \cdots + a_n' \mod m$$

特别的，若$a \equiv a' \mod m$和$b \equiv b' \mod m$，则

$$a + b \equiv a' + b' \mod m$$

1.1.4 引理：

I_m是一个m阶加法循环群，有生成元[1]

证明： 仅在这个证明，我们把同余类的加法用$\boxplus$作为其记号。：

$$\alpha([a],[b]) = [a] \boxplus [b] = [a+b]$$

而$\boxplus$的结合遵循加法的结合。

$$\begin{aligned}[a] \boxplus ([b] \boxplus [c]) =& [a] \boxplus [b+c] \\ =& [a + (b+c)] \\ =& [(a+b)+c] \\ =& [a+b] \boxplus [c] \\ =& ([a] \boxplus [b]) \boxplus [c]\end{aligned}$$

$\boxplus$的交换性遵循加法的交换性：

$$[a] \boxplus [b] = [a+b] = [b+a] = [b] \boxplus [a]$$

它的单位元是$[0]$，因为0是Z上的加法中的单位元

$$[0] \boxplus [a] = [0+a] = [a]$$

并且$[a]$的逆为$-a$，因为$-a$是加法群Z中元素a的逆元

$$[-a] \boxplus [a] = [-a+a] = [0]$$

因此I_m是一个加法群且阶为m的阿贝尔群。且为生成元$[1]$生成，这是因为当$0 \leq r < m$的时候，$[r] = [1] + \cdots + [1]$为通过添加r个$[1]$得到同余类。

所以通过上述的证明，我们可以看到I_m的群公理继承自Z的群公理。

我们有另一种群I_m的构造，定义G_m为集合$\{0, 1, \cdots, m-1\}$，并且定义G_m上的一个运算

$$a \boxplus b = \begin{cases} a+b & a+b \leq m-1 \\ a+b-m & a+b > m-1 \end{cases}$$

这个例子比刚才给出的简单，但要验证满足结合律是非常乏味的，使用起来也很粗糙，所以证明一般需要通过案例来分析。

1.1.5 推论：

每个阶$m \geq 2$的循环子群都同构于I_m

证明： 在同态的例2我们已经证明了两个循环子群具备相同阶的时候是同构的。所以推论自然是成立的。

1.1.6 引理：

函数$\mu : I_m \times I_m \to I_m$定义为

$$\mu([a], [b]) = [ab]$$

是I_m上的一个运算。这个运算是满足交换和结合的。并且$[1]$是单位元。

证明： 我们选择一些同余类$[a], [b]$，然后选择另一些$[a'], [b']$。之前的证明一样，μ是一个良好定义的函数。这意味着我们也要证明若$[a] = [a']$和$[b] = [b']$则$\mu([a], [b]) = \mu([a'], [b'])$，即$[ab] = [a'b']$而这正是我们之前在同余中讲到的一个命题：

若$a_i \equiv a_i' \mod m$,$i = 1, 2, \cdots, n$则

$$a_1 \cdots a_n \equiv a_1' \cdots a_n' \mod m$$

特别的，若$a \equiv a' \mod m$，$b \equiv b' \mod m$则

$$ab \equiv a'b' \mod m$$

现在我们在这个证明中引入一个记号（只在这个证明中用）“$\boxtimes$ ”作为同余类的乘法。

$$\mu([a],[b]) = [a] \boxtimes [b] = [ab]$$

运算$\boxtimes$的结合律来自普通乘法的结合律：

$$\begin{aligned}[a] \boxtimes ([b] \boxtimes [c]) =& [a] \boxtimes [bc] \\ =& [a(bc)] \\ =& [(ab)c] \\ =& [ab] \boxtimes [c] \\ =& ([a] \boxtimes [b]) \boxtimes [c]\end{aligned}$$

并且也满足交换：

$$[a] \boxtimes [b] = [ab] = [ba] = [b] \boxtimes [a]$$

而且单位元是[1]

$$[1] \boxtimes [a] = [1a] = [a]$$

对所有$a \in Z$成立

所以，现在我们可以丢掉这个烦人的符号了直接记为

$$[a][b] = [ab]$$

表示I_m中同余类的积，注意到当我们使用乘法的时候它不是一个群，因为[0]没有逆元。

1.1.7 引理：

1. 若$(a,m)=1$，则$[a][x]=[b]$在I_m中有解
2. 若p是素数，则$I_p^\times$，是所有I_p中非零元素的集合，则$I_p^\times$是一个阶为$p-1$的乘法阿贝尔群

证明： 由于$(a,m)=1$，则同余式子$ax \equiv b \mod m$存在某个s有$as \equiv 1 \mod m$，即$1 = as+tm$是一个线性组合。然后我们再同乘一个b就有$b = sab+tmb$得到$asb \equiv b \mod m$，就得到了$x = sb$是一个解。

并且，若y是另一个解，则有$ax \equiv ay \mod m$，则$m \mid a(x-y)$，而因为$(a,m)=1$则$m \mid x-y$有$x \equiv y \mod m$，所以解x也是一个同余类在I_m中

所以当$(a,m)=1$时$[ax]=[b]=[a][x]$在I_m中有解

对于第二个命题，设$m=p$是一个素数，若$0<a<p$，则$(a,p)=1$并且$[a][x]=[1]$在I_p中有解，并且$a\neq 0$所以a存在一个逆在I_p中。由于同余类的乘法继承自普通的乘法，加上我们排除了非零元素，所以I_p是一个乘法阿贝尔群。并且有$p-1$个元素。因为我们丢弃了$[0]$。

现在让我们给出费马定理的新证明

1.2 费马定理

若p是素数和$a\in Z$则

$$a^p=a \mod p$$

证明： 我们实际上就是要证明在I_p中有$[a^p]=[a]$，若$[a]=[0]$。则利用引理1.1.6有$[a^p]=[a]^p=[0]^p=[0]=[a]$。若$[a]\neq[0]$，则$[a]\in I_p^\times$。利用拉格朗日定理的推论: 若有限群$G$的阶是$m$，则对所有的$a\in G$有$a^m=1$。由于$|I_p^\times|=p-1$则$[a]^{p-1}=[1]$，其中$[1]$是生成元。然后我们乘以$[a]$就得到了结果有$[a^p]=[a]^p=[a]$，因此$a^p\equiv a \mod p$

注意： 若$m\geq 2$不是素的。则$I_m^\times$不是群。设$m=ab$，其中$1<a,b<m$则$[a],[b]\in I_m^\times$，但$[a][b]=[m]=[0]\notin I_m^\times$。现在我们来定义一个$I_p^\times$的类似物用来推广费马定理。

1.3 定义：

令$\mathrm{U}(I_m)$为所有I_m中所有存在逆的同余类的集合，这意味着若$[a]\in\mathrm{U}(I_m)$，则存在$[s]\in I_m$使得$[s][a]=[1]$

1.3.1 引理：

1. $\mathrm{U}(I_m)=\{[r]\in I_m:(r,m)=1\}$
2. $\mathrm{U}(I_m)$是一个阶为$\phi(m)$乘法阿贝尔群，$\phi=|\{k\in Z:1\leq k\leq m,(k,m)=1\}$

证明1： 设$E=\{[r]\in I_m:(r,m)=1\}$。若$[r]\in E$，则$(r,m)=1$。存在一些整数s,t使得$sr+tm=1$成立。因此$sr\equiv 1 \mod m$，那么$[sr]=[s][r]=[1]$，则由定义可知$[r]\in\mathrm{U}(I_m)$有$E\subseteq\mathrm{U}(I_m)$。

反过来，我们设$[r] \in \mathrm{U}(I_m)$，则存在$[s] \in \mathrm{U}(I_m)$使得$[s][r] = 1$，但$[s][r] = [sr] = [1]$有$m \mid (sr-1)$，因此能找到一个t使得$sr-1 = tm$有$sr+tm = 1$是成立的。这说明$(r,m) = 1$。有$[r] \in E$得到$\mathrm{U}(I_m) \subseteq E$。所以$\mathrm{U}(I_m) = E$

证明2： 若$(r,m) = 1 = (r',m)$，则$(rr',m) = 1$。[1]

所以，若$[r],[r'] \in \mathrm{U}(I_m)$，则我们知道$[rr'] \in \mathrm{U}(I_m)$(因为(rr',m)=1)，所以乘法是$\mathrm{U}(I_m)$上的运算，并且满足结合和交换。其中[1]是单位元，利用引理1.1.7我们知道$[r][x] = [1]$在I_m中有解。因此每个$[r] \in \mathrm{U}(I_m)$都存在逆。所以$\mathrm{U}(I_m)$是一个乘法阿贝尔群。并且由于其中的同余类都与m互素，这个群的阶正好就是引理中的函数ϕ，ϕ是由小于m但与m互素的整数组成的集合。因为$[r]$中的r都是ϕ中的元素。

若p是素数，则$\phi(p) = p-1$并且$\mathrm{U}(I_p) = I_p^{\times}$

证明： 若p是素数，则对于$1 \leq k \leq p$满足(k,p)的个数一共有$p-1$个，因为$(p,p) = p$不满足在引理1.1.7我们是没有引入$[p] \in I_p$的。所以$\phi(p) = p-1$。利用引理1.1.7可知$I_p^{\times}$是阶为$p-1$的阿贝尔群。且$(k,p) = 1$意味着有$ak \equiv 1 = tp$为$[a][k] = [1]$刚刚好就是$\mathrm{U}(I_p)$的定义。所以$\mathrm{U}(I_p) = I_p^{\times}$

1.4 欧拉定理：

若$(r,m) = 1$，则

$$r^{\phi(m)} \equiv 1 \mod m$$

证明： 设G是阶为n的有限群，则利用拉格朗日定理对所有$x \in G$有$x^n = 1$。所以，若$[r] \in \mathrm{U}(I_m)$，则$[r]^{\phi(m)} = [r]^{p-1} = [1]$，这意味着$r^{\phi(m)} \equiv 1 \mod m$

---

[1]有a,b,s,t满足$ar+bm = 1 = sr'+tm = 1$那么我们考虑$(ar+bm)(sr'+tm) = asrr' + bmsr' + artm + bmtm = 1*1 = 1$得到

$$\begin{aligned} asrr' + bmsr' + artm + bmtm =& asrr' + m(bmt + art + bsr') \\ =& asrr' + m(bmt + art + bsr') \\ =& 1 \end{aligned}$$

现在只需要令$as = \alpha, (bmt + art + bsr') = \beta$我们就有$(rr',m) = 1$。

例1

利用引理1.3.1很清楚的看到

$$\mathrm{U}(I_8) = \{[1],[3],[5],[7]\} \cong V$$

其中$[3]^2 = [9] = [1], [5]^2 = [25] = [1], [7]^2 = [49] = [1]$ 其他的例子有：

$$\mathrm{U}(I_{10}) = \{[1],[3],[7],[9]\}$$

其中$[3]^4 = [81] = [1]$,但$[3]^2 = [9] = [-1] \neq [1]$

1.5 威尔森定理

一个整数p是素数当且仅当

$$(p-1)! \equiv -1 \mod p$$

证明： 设p是一个素数，若$a_1, a_2, \cdots, a_n$是所有有限阿贝尔群G中的元素。则乘积$a_1a_2\cdots a_n$等于满足$a^2 = 1$的所有元素，因为其他的元素和逆抵消。因为p是素数，且若$a^2 \equiv 1 \mod p$，则$a \equiv \pm1 \mod p$，所以我们知道如果$[a]^2 = [1] \in I_p^\times$，则$[a] = [1]$或者$[a] = [-1]$[2]，但$[1]$是单位元，所以这意味着$[a]^2 \in I_p^\times$满足这个条件的元素只有一个。就是$[-1]$。最后，由于$p$是素数，则$0 \leq k < p$都有$(k,p) = 1$，所以这些元素的乘积就是$(p-1)!$，综上所述有$[(p-1)!] = [-1]$即$(p-1)! \equiv -1 \mod p$

反之，若$(m-1)! \equiv -1 \mod m$，则$(m,(m-1)!) = 1$。若m是合数，则存在$a \mid m$其中$1 < a \leq m-1$。所以若$a \mid a!$意味着$a \mid (m-1)!$。因此$a > 1$是m和$(m-1)!$的因子。这是一个矛盾，所以a是素数。

注意： 就像欧拉定理推广了费马定理一样，我们也可以用同样的方法推广威尔森定理。把$\mathrm{U}(I_p)$替换为$\mathrm{U}(I_n)$，则对于下面的例子：我们可以证明，对所有$m \geq 3$的时候$U(I_{2^m})$恰好有3个二阶元素，即$[-1], [1+2^{m-1}]$和$[-(1+2^{m-1})]$。那么我们可以得到所有奇数的乘积[3]r其中$1 \leq r < 2^m$同余$1 \mod 2^m$的。

[2] 证明：若$a^2 \equiv 1 \mod p$，则有$p \mid a^2 - 1 \Rightarrow p \mid (a+1)(a-1)$，由于$p$是素数，由欧几里得引理可知，若$(p, a+1) = 1$，则$p \mid a-1$而$(a-1, a+1) = 1$，所以我们就得到了要证明的东西，若$p \mid a+1$，那么$a \equiv -1 \mod p$反之亦然有$a \equiv 1 \mod p$

[3] $1 + 2^{m-1}$可以表示所有的正奇数，但$-(1+2^{m-1})$在$m > 1$的时候能表示所有的负奇数

因为

$$\begin{aligned}(-1)(1+2^{m-1})(-1-2^{m-1}) =&(1+2^{m-1})^2\\ =&1+2^m+2^{2m-2}\\ \equiv&1 \mod 2^m\end{aligned}$$

同态$\pi : Z \to I_m$定义为$\pi : a \to [a]$，且是满射的。所以$I_m = \mathrm{im}\pi$。所以每个I_m中的元素都来自$\pi(a), a \in Z$。并且$\pi(a)+\pi(b) = \pi(a+b)$。这种I_m在加法群Z上的关系的描述可以推广到任何群（不一定是阿贝尔群）。

假设$f : G \to H$是G, H上的满射同态。由于f是满的，每个H形如$f(a)$的元素都有一个$a \in G$对应。并且H中的运算由$f(a)f(b) = f(ab)$给出。其中$a, b \in G$。现在$K = \ker f$是G的正规子群[4]，而现在我们要从G和K中重建$H = \mathrm{U}(I_m)f$。

为了描述一些关于正规群的东西，我们先来看点东西，首先引入G上所有非空子集的集合$S(G)$上的一个运算。若$X, Y \in S(G)$，定义

$$XY = \{xy : x \in X, y \in Y\}$$

而这个乘法是结合的，所以$X(YZ)$是所有$x(yz)$组成的集合，其中$x \in X, y \in Y, z \in Z$。我们也有$(XY)Z$是所有$(xy)z$的集合，。由于集合是$G$中满足乘法的集合，由群的结合性可知他们的子集是相同的，因为$(XY)Z = XYZ = X(YZ)$证明了它们的元素是相同的。

这个乘法的一个实例是，单点子集$\{a\}$和一个群$H \le G$得到一个陪集aH

第二个例子是，我们证明H是G的任意子群，则

$$HH = H$$

若$h, h' \in H$，则$hh' \in H$。所以子群对乘法封闭并且$HH \subseteq H$。反过来，若$h \in H$，则$h = h1 \in HH$，所以$H \subseteq HH$。

$S(G)$中可能会存在两个子集X, Y的乘法满足交换，即使X, Y中的元素不交换。例如刚才的$X = Y = H$，而H是G的非阿贝尔子群。这里还有另一个有趣的例子：令$G = S_3$和$K = \langle(1\,2\,3)\rangle$，现在$(1\,2)$并不和$(1\,2\,3) \in K$交换，但我们说$(1\,2)K = K(1\,2)$。实际上这就是在同态中我们证明的一个关于正规子群有关的问题的逆命题[5]。因此$H \lhd G$当且仅当像上述例子中的左

[4]因为若$x \in \ker f, a \in G$，则$f(axa^{-1}) = f(a)f(a)^{-1} = 1 \in \ker f$是正规子群。

[5]若H是子群且$bH = Hb = \{hb : h \in H\}$对每个$b \in G$成立，则$H$是正规子群，。

陪集等于右陪集的事实。所以我们接下来要来看看，满足乘法的可交换子集到底是怎么样的：

1.5.1 引理：正规子群

若K是G中的一个正规子群，则

$$bK = Kb$$

对每个$b \in G$成立

证明： 令$bk \in bK$，由于K是正规的，则$bkb^{-1} \in K$有$bkb^{-1} = k' \in K$，所以$bk = (bkb^{-1})b = k'b \in K$，则$bK \subseteq Kb$。反之，令$kb \in Kb$。由于$K$是正规的，则$(b^{-1})k(b^{-1})^{-1} = b^{-1}kb \in K$，使$b^{-1}kb = k'' \in K$，因此$kb = b(b^{-1}kb) = bk'' \in bK$，所以$Kb \subseteq bK$，因此当$K \lhd G$时$bK = Kb$。

以下是由一个给定群构造一个新群的基本方法。

1.6 定理：商群

令G/K表示为G的子群K中的所有陪集族。若K是正规子群，则

$$aKbK = abK$$

对所有$a, b \in G$并且G/K在运算下是群。

注意： 群G/K叫做$G \mod K$的商群，当G是有限群，它的阶$[G/K]$是其指数$[G:K] = |G| / |K|$(大概这既是为什么叫商群的原因)

证明： 两个陪集$(aK)(bK)$的乘积被看作是4个$S(G)$中的元素相乘。因此，$S(G)$中的结合律给出了广义结合律，我们有

$$(aK)(bK) = a(Kb)K = abKK = abK$$

对于K的正规性，通过引理1.5.1可知对所有$b \in K$有$Kb = bK$。而$KK = K$是因为K是一个子群。因此K的两个陪集的乘积也是K的陪集，并且G/K上的运算重新被定义。因为$S(G)$上的乘法是结合的，等式$X(YZ) = (XY)Z$成立。满足封闭和结合。特别的，当X, Y, Z是K的陪集，则G/K上的运算是结合的。单位元是陪集$1K = K$，因为$(1K)(bK) = bK$，而aK的逆是$a^{-1}K$有$(a^{-1}K)(aK) = K$。所以G/K满足群的条件，是一个群。

例2： 现在来证明商群$Z/\langle m\rangle$就是I_m，其中$\langle m\rangle$是正整数m的所有倍数组成的循环子群，由于Z是阿贝尔群。则$\langle m\rangle$是正规的。而I_m是所有等价类的集合，而我们在一开始的定义1.1中的注意已经小小的提出了一个验证（不是证明），即等价类可以表示为一个循环子群的陪集。所以$Z/\langle m\rangle$和I_m其实有相同的元素，所以是相等的：陪集$a+\langle m\rangle$是同余类$[a]$：

$$a+\langle m\rangle=\{a+km:k\in Z\}=[a]$$

并且它们的运算也是一样的：在$Z/\langle m\rangle$上的加法由如下式子给出：

$$(a+\langle m\rangle)+(b+\langle m\rangle)=(a+b)+\langle m\rangle$$

由于$a+\langle m\rangle=[a]$，所以上述方程也可以重写为$[a]+[b]=[a+b]$即I_m上的求和，所以I_m就是商群$Z/\langle m\rangle$

1.6.1 推论：

每个正规子群$K\lhd G$是某些同态的核。

证明： 定义自然映射$\pi:G\to G/K$为$\pi(a)=aK$,则方程$aKbK=abK$可以被重写为$\pi(a)\pi(b)=\pi(ab)$。因此π是满的同态。由于K是G/K中的单位元，则

$$\ker\pi=\{a\in G:\pi(a)=K\}=\{a\in G:aK=K\}=K$$

证毕。

1.7 第一同构定理

若$f:G\to H$是一个同态，则

$$\ker f\lhd H\ and\ G/\ker f\cong \mathrm{im}f$$

而其中更多的细节：若$\ker f=K$，则函数$\varphi:G/K\to \mathrm{im}f\le H$由函数$\varphi:aK\to f(a)$确定，是一个同构

证明： 若$K=\ker f$，则K是一个G的正规子群[6]。若$aK=bK$，则$a=bk$对某些$k\in K$成立，并且$f(a)=f(bk)=f(b)$，因为$f(k)=1$。

现在证明函数φ是同态，由于f是一个同态并且$\varphi(aK)=f(a)$，则

$$\varphi(aKbK)=\varphi(abK)=f(ab)=f(a)f(b)=\varphi(aK)\varphi(bK)$$

[6]因为$f(aka^{-1})=f(a)\,1\,f(a)^{-1}=1$，所以$aka^{-1}\in K$

所以$\mathrm{im}\varphi \leq \mathrm{im}f$，反之注意$y \in \mathrm{im}f$，则存在某个$a \in G$有$y = f(a)$。所以$y = f(a) = \varphi(aK)$有$\varphi$是满射的。

最后，我们证明φ是单射的。若$\varphi(aK) = \varphi(bK)$，则$f(a) = f(b)$。因此$f(b)^{-1}f(a) = f(b^{-1}a)$，所以$b^{-1}a \in \ker f = K$。所以$aK = bK$[7]。所以$\varphi$是一个单射。因此$\varphi(G/K) \to \mathrm{im}f$是一个同构。

注意： 我们用这个图表示第一同构定理，其中$\pi : G \to G/K$是自然映射$\pi : a \to aK$

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/K \arrow[ur, "\varphi"'] & \end{tikzcd}$$

我们给出一个第一同构定理的小应用，对任意群G，一个恒等映射$f : G \to G$是一个满射同态且$\ker f = \{1\}$，所以利用第一同构定理，有

$$G/\{1\} \cong G$$

当我们给定同态$f : G \to H$，我们应当立即去求它的核和象，第一同构定理进一步给出一个同构$G/\ker f \cong \mathrm{im}f$。因为同构去之间没什么太大的差别，所以第一同构定理还告诉了我们商群和同态象之间没什么太大的区别。

例2： 让我们回顾一下一些东西，我们知道两个m阶循环群是同构的。若$G = \langle a \rangle$是一个阶为m的循环群。定义同构$f : Z \to G$由函数$f(n) = a^n$给出，其中$n \in Z$，现在，f是满射的（因为a是一个生成元）。其中的核$\ker f = \{n \in Z : a^n = 1\} = \langle m \rangle$。那么由第一同构定理我们有$Z/\langle m \rangle \cong G$。所以我们就证明了阶为$m$的循环群$G$和$Z/\langle m \rangle$同构。所以，不妨取其他的$m$阶循环群$G, H$。由于$G \cong Z/\langle m \rangle$和$H \cong Z/\langle m \rangle$[8]。所以$G \cong H$可知任意两个$m$阶循环群同构。当然，另一种方法是，由于$Z/\langle m \rangle = I_m$，而$I_m$是$m$阶加法循环群。所以两个循环群彼此同态就有$G \cong I_m$是自然的。

[7]若$aH = bH$当且仅当$b^{-1}a \in H$

[8]关于两个群H_i, H_j同构于一个群G则H_i, H_j同构的证明在同态的章节以习题的方式给出来了

例3： 什么是商群R/Z？定义$f: R \to S^1$，由函数

$$f: x \to e^{2\pi i x}$$

给出，其中S^1是一个圆群。通过sine和cosine的加法公式[9]有$f(x+y) = f(x)f(y)$，所以f是一个同态。f是一个满射且$\ker f$是有所有$x \in R$和$e^{2\pi i x} = \cos(2\pi x) + i\sin(2\pi x) = 1$组成的。但是，$x$必须是一个整数才能满足$e^{2\pi i x} = 1$，因为$\cos(2\pi) = 1$而$\sin(2\pi) = 0$，所以$n \in Z$。有$Z = \ker f$。再利用第一同构定理就有

$$R/Z \cong S^1$$

注： 上述操作实际上就是二维上复单位圆的射影，通过f把R上的点映射到复单位圆上

一个符合直觉的问题是，当H, K是子群的时候，HK是否也是一个子群。一般来说这不成立，例如：令$G = S_3$而$H = \langle(1\,2)\rangle$，且$K = \langle(1\,3)\rangle$则

$$HK = \{(1), (1\,2), (1\,3), (1\,3\,2)\}$$

但HK不是一个子群，否则与拉格朗日定理矛盾。因为$\mid G \mid = 6$，而乘积HK是子群的必要条件在练习中我们将会证明。

1.7.1 命题：

1. 若H, K是群G的子群，若H或者$K \lhd G$，则$HK \lhd G$；并且$HK = KH$。
2. 若H和K是正规子群，则HK也是正规子群。

证明1： 设$K \lhd G$。如果$hk \in HK$，就会有$k' = hkh^{-1} \in K$因为$K \lhd G$且

$$hk = hkh^{-1}h = k'h \in KH$$

所以$HK \subseteq KH$，反过来记$kh = hh^{-1}kh = hk'' \in HK$。所以$HK = KH$。

现在证明HK是子群，由于$1 \in H$和$1 \in K$，所以$1 \cdot 1 \in HK$。若$hk \in HK$，则$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$。若$hk, h_1k_1 \in HK$，则$k' = h^{-1}kh_1 \in K$和

$$hkh_1k_1 = hh_1(h^{-1}kh_1)k_1 = (hh_1)(k'k)$$

因此HK是G的子群

[9] 棣莫弗定理

证明2： 若$g \in G$，则

$$ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$$

所以$HK \lhd G$

1.7.2 命题：乘积公式

若H和K是有限群G的子群，则

$$|HK||H \cap K| = |H||K|$$

其中$HK = \{hk : h \in H, k \in K\}$

证明： HK是所有K的左陪集，即：

$$HK = \bigcup_{h \in H} hK$$

由于每个K的陪集都有$|K|$个元素，所以我们能找到形如hK的不同左陪集的个数，其中$h \in H$。但$h_1K = h_2K$对$h_1, h_2 \in H$当且仅当$h_2^{-1}h_1 \in K$因此

$$h_1K = h_2K \iff h_2^{-1}h_1 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K)$$[10]

因此，形如hK的不同陪集的数量等于不同陪集$h(H \cap K)$的数量。由拉格朗日定理，$h(H \cap K)$的数量为$\dfrac{|H|}{|H \cap K|}$。所以HK是由$\dfrac{|H|}{|H \cap K|}$个不同的K的陪集构成的。那么有

$$|HK| = \frac{|H||K|}{|H \cap K|} \Rightarrow |HK||H \cap K| = |H||K|$$

注意： 我们并没有假设H, K是正规子群，这意味着HK可能不是一个子群。现在给出一个命题的例子：设$G = S_3$，其中两个子群$H = \langle (1\ 2) \rangle$,$K = \langle (2\ 3) \rangle$,有$|H| = |K| = 2$和$|H \cap K| = 1$，则$|HK| = 4$

[10] H可以表示为$H \cap K$的一些陪集$h(H \cap K)$，由于$h_1, h_2 \in H$有$h_1K = h_2K \iff h_2^{-1}h_1 \in K$，可知，能够使得$h_1K = h_2K$的元素$h$在$H \cap K$中，所以$h_1K$有$|H \cap K|$个表达方法。所以，$|H| = t|H \cap K|$由$t$个不同的陪集构成，所以我们能得到存在$t$个不同的陪集，即存在$t$个形如$hK$的陪集

1.8 定理：第二同构定理

若H, K是G的子群且$H \lhd G$，则HK也是子群，$H \cap K \lhd K$和

$$\frac{K}{H \cap K} \cong HK/H$$

证明： 我们首先通过证明HK/H是有意义的并列出它的元素。由于$H \lhd G$，利用命题1.7.1，则HK是子群。HK中的H其正规性质来自一些事实：若$H \le S \le G$并且H是G中正规的子群，则H在S中也是正规的。(若对每个$g \in G$都有$ghg^{-1} \in H$，则$ghg^{-1} \in H$对每个$g \in S$也成立。)

现在我们来证明每个陪集$xH \in HK/H$对一些$k \in K$形如kH，当然，$xH = hkH$其中$h \in H$和$k \in K$。但$hk = k(k^{-1}hk) = kh'$，对某些$h' \in H$成立。所以$hkH = kh'H = kH$[11]

由此可见函数$f : K \to HK/H$通过$f : k \to kH$得到。而且也是满射的（第二段的证明）。更多的，f是一个同构，这是自然映射$\pi : G \to G/H$的一个限制。由于$\ker \pi = H$，所以$\ker f = H \cap K$并且$H \cap K$也是个G中的正规群。由第一同构定理可知$K/(H \cap K) \cong HK/H$。

当一个子群是正规的时候，第二同构定理给出了乘积准则中的特殊例子：若$K/(H \cap K) \cong HK/H$，则$\mid K/(H \cap K) \mid = \mid HK/H \mid$而这恰好有

$$\mid K \mid / \mid H \cap K \mid = \mid HK \mid / \mid H \mid \Rightarrow \mid HK \mid \mid H \cap K \mid = \mid H \mid \mid K \mid$$

1.9 定理：第三同构定理

若H和K是群G中的正规子群，其中$K \le H$，则$H/K \lhd G/K$且

$$(G/K)/(H/K) \cong G/H$$

证明： 定义$f : G/K \to G/H$由$f : aK \to aH$给出。注意f是一个定义良好的函数。如果$a' \in G$和$a'K = aK$，那么$a^{-1}a' \in K \le H$得到$aH = a'H$。很容易得到f是一个同态：$f(aKbK) = f(abK) = abH = aHbH = f(aK)f(bK)$

[11] $h' \in H, h'H = H$

现在，$\ker f = H/K$。若对$aK = H$当且仅当$a \in H$。所以H/K是G/K中的正规子群。[12]由于f是满的。再利用第一同构定理就有

$$(G/K)/(H/K) \cong G/H$$

第三同构定理非常容易记住：K在分式$(G/\ K)/(H/K)$被约掉了。在证明了第三同构定理之后我们可以藉由更好的理解第一同构定理。商群$(G/K)(H/K)$是由所有陪集（关于H/K的）组成的。其代表的就是本身的陪集（关于G/K）。这个关于第三同构定理的证明可能会非常糟糕。

关于下一个结果，其中商群G/K的子群的描述可以被认为是第四个的同构定理。回想函数$f : X \to Y$可以直接使用逆象来在两个集合X, Y间建立对应。现在我们将把这一观点应用于当$f : G \to H$是同构的时候这一特殊情况。

若G是一个群且$K \lhd G$，则$\mathbf{Sub}(G; K)$记为所有G中包含K的子群S构成的族。并且记$\mathbf{Sub}(G/K)$是所有G/K的子群构成的族

1.10 定理：对应定理

若G是群且$K \lhd G$。则$S \to S/K$是双射。$\mathbf{Sub}(G; K) \to \mathbf{Sub}(G/K)$，记$S/K$为$S^*$，我们有

1. $T \leq S \leq G$在$\mathbf{Sub}(G; K)$中当且仅当若$T^* \leq S^*$在$\mathbf{Sub}(G/K)$中
2. $T \lhd S$在$\mathbf{Sub}(G; K)$中当且仅当若$T^* \lhd S^*$在$\mathbf{Sub}(G/K)$中，在这种情况下$S/T \cong S^*/T^*$

证明： 令$\Phi : \mathbf{Sub}(G; K) \to \mathbf{Sub}(G/K)$表示函数$\Phi : S \to S/K$。

为了证明Φ是双射，我们首先得要证明若$K \leq S \leq G$，则$\pi^{-1}\pi(S) = S$，其中$\pi : G \to G/K$为自然映射。当然，$S \subseteq \pi^{-1}\pi(S)$[13]，对于反包含，令$a \in \pi^{-1}\pi(S)$，则存在一些$s \in S$有$\pi(a) = \pi(s) \Rightarrow ak = sk \Rightarrow as^{-1} = 1$。这意味着有$as^{-1} \in \ker \pi = K$ 所以$a = sk$对某个$k \in K$成立，由于$K \leq S$，因此$a = sk \in S$。因此$\pi^{-1}\pi(S) = S$

现在假设$\pi(S) = \pi(S')$，其中S, S'读是G中包含K的子群。则$\pi^{-1}\pi(S) = \pi^{-1}\pi(S')$得到$S = S'$因此$\Phi$是一个单射。

---

[12] $f(a^{-1}H/Ka) = 1$，有$a^{-1}H/Ka \in \ker f$

[13] 取$s \in S$，则$f(s) \in f(S)$得到$f^{-1}f(s) \subseteq f^{-1}(S)$。若f是单射，则$f^{-1}f(S) = S$

为了证明Φ是满射，令U是G/K中的子群。$\pi^{-1}(U)$是G中包含$K=\pi^{-1}(\{1\})$的子群，利用π是单射，则$\pi(\pi^{-1}(U))=U$。因此Φ是满射。[14]

若$T\leq S\leq G$，则对于π也有相同的蕴含关系，即$T/K=\pi(T)\leq\pi(S)=S/K$，反过来，假设$T/K\leq S/K$。若$t\in T$，则$tK\in T/K\leq S/K$得到$tK=sK$对某个$s\in S$成立。因此$t=sk$对某些$k\in K\leq S$成立并且得到$t\in S$

当G有限的时候是一个重要且特殊的例子，我们来证明$[S:T]=[S^*:T^*]$

$$
\begin{aligned}
[S^*:T^*] &= \mid S^* \mid / \mid T^* \mid \\
&= \mid S/K \mid / \mid T/K \mid \\
&= \mid S \mid / \mid K \mid / \mid T \mid / \mid K \mid \\
&= \mid S \mid / \mid T \mid \\
&= [S:T]
\end{aligned}
$$

第三同构定理告诉我们若$T\lhd S$，则$T/K\lhd S/K$并且$(S/K)/(T/K)\cong S/T$，则$S^*/T^*\cong S/T$。反过来，我们证明若$T^*\lhd S^*$则$T\lhd S$，不难看出自然映射是同态的。若$s\in S,t\in T$，则$sts^{-1}\in T$。因为

$$\pi(sts^{-1})=\pi(s)\pi(t)\pi(s^{-1})=\pi(s)T^*\pi(s^{-1})=T^*$$

因此$sts^{-1}\in\pi^{-1}(T^*)=T$。

1.11 引理

若G是有限阿贝尔群，则G存在以$\mid G\mid$的每个因子d为阶的子群。特别的，若p是$\mid G\mid$的素因子，则G包含每个阶为p的元素

证明： 我们首先通过对$n=\mid G\mid$归纳证明，对每个$\mid G\mid$的素因子p都存在一个p阶元素在G中，基础步骤是当$n=1$的时候命题显然为真，因为不存在1的质因数。对归纳步骤，我们选择阶$k>1$的元素$a\in G$。若$p\mid k$，不妨记$k=pl$，则我们知道存在一个阶为p的元素a^l，因为$(a^l)^p=a^{pl}=a^k=1$。

其次，若$p\nmid k$，我们考虑循环子群$H=\langle a\rangle$，现在，由于G是阿贝尔群，这意味着$H\lhd G$，且商群G/H存在。注意，$\mid G/H\mid=n/k$是可以被p整除的，因为$p\mid n$，由欧几里得引理可知$p\nmid k$，所以$p\mid n/k\times k$得到$p\mid n/k$，因

[14] $ff^{-1}(U)\subseteq U$，若f是满射，则$ff^{-1}(U)=U$

此由归纳假设可知存在一个G/H中的p阶元素bH。若b阶为m，则$(bH)^m = b^m H = H \in G/H$。可知$p \mid m$，这样子我们就又回到了第一种情况。存在阶为$p$的元素。

现在我们来证明一般的情况。当$d=1$的时候也是明显的，现在我们假设$d > 1$。然后再假设d是素因子。通过归纳，G包含一个阶为p的子群H。由于G是阿贝尔群，则$H \lhd G$。可以定义商群G/H，则$\mid G/H \mid = \mid G \mid /p$。则$(d/p) \mid \ \mid G/H \mid$，则由归纳假设给出一个子群$S^* \leq G/H$，其中$\mid S^* \mid = d/p$。然后利用对应定理，可知存在一个子群$S(H \leq S \leq G)$，其中$S^* = S/H$。因此$\mid S \mid = p \mid S^* \mid = d$

1.12 定义：直积

若H, K是群，则它们的直积记为$H \times K$，它是所有有序对(h, k)组成的集合，其中$h \in H, k \in K$。并带有运算

$$(h, k)(h', k') = (hh', kk')$$

很容易验证$H \times K$是群，因为它的单位元是$(1, 1)$，且$(h, k)^{-1} = (h^{-1}, k^{-1})$。注意：$H \times K$是阿贝尔群当且仅当$H, K$都是阿贝尔群

1.12.1 例4

四元群V同构于$I_2 \times I_2$。我们记映射$f : V \to I_2 \times I_2$由如下函数给出：

$$\begin{aligned} f : (1) &\to ([0], [0]) \\ f : (1\ 2)(3\ 4) &\to ([1], [0]) \\ f : (1\ 3)(2\ 4) &\to ([0], [1]) \\ f : (1\ 4)(2\ 3) &\to ([1], [1]) \end{aligned}$$

首先$f(1)f(1\ 2)(3\ 4) = f(1\ 2)(3\ 4) = ([0], [0]) + ([1], [0]) = ([1], [0])$成立

任取其中两个元素有

$$f(1\ 2)(3\ 4)(1\ 3)(2\ 4) = f(1\ 4)(2\ 3) = ([1], [0]) + ([0], [1]) = ([1], [1])$$

所以是一个同构。

现在我们把第一同构定理运用在直积中

1.12.2 命题：

令G, G'是两个群，且$K \lhd G$和$K' \lhd G$是两个正规子群，则$K \times K'$是$G \times G'$的正规子群。并且存在同构

$$(G \times G')/(K \times K') \cong (G/K) \times (G'/K')$$

证明： 令$\pi : G \to G/K$和$\pi' : G' \to G'/K'$为自然映射。则它们的直积映射$f : G \times G' \to (G/K) \times (G'/K')$由下列函数给出

$$f : (g, g') \to (\pi(g), \pi(g')) = (gK, gK') =$$

任意取$gK, g'K' \in (G/K) \times (G'/K')$，则$f^{-1}((gK, g'K')) = (g, g') \in G \times G'$，所以$f$是一个满射而其中$\ker f = K \times K'$，最后利用第一同构定理即证明完毕。

1.13 命题：

若G是包含正规子群H和K的群，其中$H \cap K = \{1\}$并且$HK = G$，则$G \cong H \times K$

证明：我们首先证明若$g \in G$，则一个因式分解有$g = hk$，其中$h \in H, k \in K$是唯一的，否则当$hk = h'k'$，则$(h')^{-1} = k'k^{-1} \in H \cap K = \{1\}$。因此，$h = h'$和$k = k'$。我们现在给出一个函数$\varphi : G \to H \times K$由$\varphi(g) = (h, k)$定义。其中$g = hk, h \in H, k \in K$。为了看出$\varphi$是同构，令$g' = h'k'$，则$gg' = hkh'k' = hh'kk'$[15]。因此$\varphi(gg') = \varphi(hkh'k')$，那我们继续可以得到

$$\begin{aligned}
\varphi(hkh'k') =& \varphi(hh'kk') \\
=& (hh', kk') \\
=& (h, k)(h', k') \\
=& \varphi(g)\varphi(g')
\end{aligned}$$

令$h \in H$和$k \in K$，由于K是正规的，所以$(hkh^{-1}k^{-1} \in K)$，并且由于H也是正规的，所以$h(kh^{-1}k^{-1}) \in H$。但$H \cap K = \{1\}$，因此$hkh^{-1}k^{-1} = 1$且$hk = kh$，最后，我们来证明这个同态是同构。其实已经很显然了，我们证明了满射、单射和同态。只需要将这些组在一起即可。

[15]这是因为H,K正规

若$(h,k)\in H\times K$，则元素$g\in G$由定义$g=hk$给出并满足映射$\varphi(g)=(h,k)$，所以φ是满的，若$\varphi(g)=(1,1)$，则$g=1$，所以$\ker\varphi=1$并且φ是单射。因此φ是一个同构。

我们刚才讲的命题里面所有条件都是必须的，例如：令$G=S_3$，其中$H=\langle(1\ 2\ 3)\rangle$，$K=\langle(1\ 2)\rangle$，则$S_3=HK$，其中$H\cap K=\{1\}$，且$H\lhd S_3$，但$K$不是正规的，所以$S_3\ncong H\times K$，且$S_3$不是阿贝尔群，$H\times K$是阿贝尔群只有$H,K$是阿贝尔群的时候成立。

1.14 定理：

若m,n互素，则

$$I_{mn}\cong I_m\times I_n$$

证明：若$a\in Z$，则记它在I_m中的等价类为$[a]_m$，我们来证明映射$f:Z\to I_m\times I_n$，它由函数$a\to([a]_m,[a]_n)$给出。且f是一个同态。

我们快速的验证一下，f是由函数$f(a)=([a]_m,[a]_n)$定义的。那么任取两个整数a,b，我们可以得到

$$\begin{aligned}f(ab)=&([ab]_m,[ab]_n)\\=&(([a][b])_m,([a][b])_n)\\=&([a]_m,[a]_n)([b]_m,[b]_n)\end{aligned}$$

很容易看出来是一个同态。明显的$\ker f=\langle mn\rangle$，而$\langle mn\rangle\leq\ker f$，因为$[0]_m,[0_n]$可以是任何数（mn互素。）对于反包含，若$a\in\ker f$，则$[a]_m=[0]_m$，$[a]_n=[0]_n$。那么$a\equiv 0\mod m$和$a\equiv 0\mod n$，即$m\mid a,n\mid a$得到$mn\mid a$，那么$a\in\langle mn\rangle$，那么$\ker f\leq\langle mn\rangle$，所以$\ker f=\langle mn\rangle$

现在证明f是满射，若$([a]_m,[a]_n)\in I_m\times I_n$，那么存在$x\in Z$有$f(x)=([x]_m,[x]_n)=([a]_m,[a]_n)$，所以我们关注的问题就是，是否存在一个$x$，它满足$x\equiv a\mod m$和$x\equiv b\mod n$。但确实是存在的，因为这就是中国剩余定理的内容，只要m,n互素，这种解就存在。最后，利用第一同构定理，我们知道$Z/\ker f\cong I_m\times I_n\Rightarrow I_{mn}\cong I_m\times I_n$。

例如，我们给出例子$I_6\cong I_2\times I_3$。但，m,n不是互素的，则不会同构。不过四元群V是个例外，因为$V\cong I_2\times I_2$。利用推论1.1.5我们知到I_m是一个同构于m的循环子群。$(m\geq 2)$，所以I_4同构于$I_2\times I_2$只是因为都拥有4个元素罢了。

1.15　命题：

令G是一个群，设$a, b \in G$是阶为m, n的交换元。若$(m, n) = 1$，则ab的阶为mn

证明：因为a, b可交换，则$(ab)^r = a^r b^r$对所有r成立，那么$(ab)^{mn} = a^{mn}b^{mn} = 1$，若$(ab)^k = 1$，则$mn \mid k$。且$a^k = b^{-k}$，因为$a$的阶是$m$，那么$1 = a^{mk} = b^{-mk}$。由于$b$的阶为$n$，那么$n \mid mk$，由于$(m, n) = 1$，则$n \mid k$成立。对于$m$的证明同理可得。而因为$mn \mid k$，$k \geq mn$，所以$ab$的阶就是$mn$。

1.16　引理：

若$(m, n) = 1$，则$\phi(mn) = \phi(m)\phi(n)$，其中$\phi$是欧拉$\phi$函数

证明：在定理1.14中我们记I_m的元素为$[a]_m$，其中一个函数$f : I_{mn} \to I_m \times I_n$由$[a]_{mn} \to ([a]_m, [a])$定义的。且$f$是同构。而利用引理1.3.1可知$|U(I_m)| = \phi(m)$，其中$\mathrm{U}(I_m) = \{[r] \in I_m : (r, m) = 1\}$，因此，我们就是要证明$f(\mathrm{U}(I_m)) = \mathrm{U}(I_m) \times \mathrm{U}(I_n)$。接下来，由于$f$是同构，那么我们有

$$\begin{aligned}\phi(mn) &= |\ \mathrm{U}(I_{mn}) = |\ f(\mathrm{U}(I_{mn}))\ | \\ &= |\ \mathrm{U}(I_m) \times \mathrm{U}(I_n)\ | = |\ \mathrm{U}(I_m)\ | \cdot |\ \mathrm{U}(\mathrm{I_n})\ | = \phi(m)\phi(n)\end{aligned}$$

其次，我们说$f(\mathrm{U}(I_{mn})) = \mathrm{U}(I_m) \times \mathrm{U}(I_n)$，这意味着有$[a]_{mn} \in \mathrm{U}(I_{mn})$，则$[a]_{mn}[b]_{mn} = [1]_{mn}$对某个$[b]_{mn} \in I_{mn}$成立，并有

$$\begin{aligned}f([ab]_{mn}) = ([ab]_m, [ab]_n) =& ([a]_m[b]_m, [a]_n[b]_n) \\ =& ([a]_m, [a]_n)([b]_m, [b]_n) = ([1]_m, [1]_n)\end{aligned}$$

因此，$[1]_m = [a]_m[b]_m$和$[1]_n = [a]_n[b]_n$。那么$f([a]_{mn}) = ([a]_m, [a]_n) \in \mathrm{U}(I_m) \times \mathrm{U}(I_n)$有$f(\mathrm{U}(I_{mn})) \leq \mathrm{U}(I_m) \times \mathrm{U}(I_n)$

对于反包含，若$f([c]_{mn}) = ([c]_m, [c]_n) \in \mathrm{U}(I_m) \times \mathrm{U}(I_n)$，那么我们必须证明存在$[c]_{mn} \in \mathrm{U}(I_{mn})$。

这里我们有$[d]_m \in I_m$且$[c]_m[d]_m = [1]_m$和$[e]_n \in I_n$有$[c]_n[e]_n = [1]_n$，由此我们可以看到f是一个满射。现在取$b \in Z$和$([b]_m, [b]_n) = ([c]_m, [e]_n)$，那么

$$f([1]_{mn}) = ([1]_m,[1]_n) = ([c]_m[b_n],[c]_n[b]_n) = f([c]_{mn}[b]_{mn})$$

因此f是单射，$[1] = [c]_{mn}[b]_{mn}$和$[c]_{mn} \in \mathrm{U}(I_{mn})$

1.17 定义：多个群的直积

若$H_1, \cdots, H_n$是群，则它们的**直积**：

$$H_1 \times \cdots \times H_n$$

是由所有n元组$(h_1, \cdots, h_n)$组成的集合，其中对所有i有$h_i \in H_i$，它们的坐标乘法是这样子的：

$$(h_1, \cdots, h_n)(h_1' \cdots, h_n') = (h_1h_1', \cdots, h_nh_n')$$

1.18 命题：

若G是有限阿贝尔群，对于其中的一个素因子p都有唯一的p阶子群，则G是循环的

证明：选择$a \in G$，它有最大的阶，记为n，若p是$|\ G\ |$的素因子，令$C = C_p$是G中阶为p的唯一一个子群。则子群C必是循环的。即$C = \langle c\rangle$，我们将通过证明$c \in \langle a\rangle$来证明$p \mid n$。若$(p, n) = 1$，则ca的阶$pn > n$，利用命题1.15，这就与我们的元素有最大阶矛盾。若$p \mid n$，则$n = pq$，因此$a^q = c^i$对某个i成立。则说明存在一个子群$\langle c\rangle$的阶为p，若$(i, p) = 1$，那么存在一些整数u, v使得$ui + vp = 1$，因此$c = c^{ui+vp} = c^{ui}c^{vp} = c^{ui}$，因此$a^{qu} = c^{ui} = c$，那么$c \in \langle a\rangle$。正如我们预期的$\langle a\rangle$包含每个$x \in G$其中$x^p = 1$对某个素数$p$成立。

若$\langle a\rangle = G$，则证明就直接完成了。因此，我们假设这有$b \in G$但$b \notin \langle a\rangle$，现在$b^{|G|} = 1 \in \langle a\rangle$，令$k$是最小正整数使得$b^k \in \langle a\rangle$，则

$$b^k = a^q$$

注意$k \mid |\ G\ |$,以为k是$G/\langle a\rangle$中的$b\langle a\rangle$的阶（因为核是$\langle a\rangle$）。当然，$k \neq 1$所以会有一个因式分解$k = pm$，其中p是素数。现在则有两种可能。若$p \mid q$，则$q = pu$且

$$b^{pm} = b^k = a^q = a^{pu}$$

因此，$(b^m a^{-u})^p = 1$，且$b^m a^{-u} \in \langle a \rangle$，因此$b^m \in \langle a \rangle$，但这与$k$是最小整数矛盾，这样子的$m$是不存在的。

第二种可能性是$p \nmid q$，我们选择$(p,q) = 1$，不出意外的，存在整数s,t使得$1 = sp + tq$，所以

$$a = a^{sp+tq} = a^{sp}a^{tq} = a^{sp}b^{pmt} = (a^s b^{mt})^p$$

因此，$a = x^p$，其中$x = a^s b^{mt}$。利用如下的习题：

> 若G是一个群，令$a \in G$对某个素数p存在阶为pk，其中$k \geq 1$。证明如果有$x \in G$其中$x^p = a$，则x的阶为p^2k并且x的阶比a大

利用这个命题，我们知道x的阶比a大。这也是一个矛盾，因为我们一开始就说a的阶是最大的。所以结论就是$G = \langle a \rangle$