课堂练习：证明$\mathbb{G}=<\mathbb{Z}_{12},\oplus>$为循环群，并求出所有的生成元和子群。

首先证明G是一个群，具有结合律，单位元，可逆性，封闭性

由 $\oplus$ 运算定义可知，$(a\oplus b)\oplus c = a\oplus(b\oplus c)$，结合律满足，且易得交换律也满足

由于$0\in Z_{12}, \forall a\in Z,$均有$a\oplus 0 = a;$因此$0$是$G$的单位元，单位元存在

$\forall a\in Z$根据 $\oplus$ 运算定义，$(12-a)\in Z_{12}$是a的逆元，$a\oplus(12-a)=0=e,$因此可逆

封闭性，$a\oplus b=(a+b)(mod \quad 12)\in Z_{12},$因此满足封闭性

所以，$G=<Z_{12},\oplus>$是一个群

进而证明，G是一个循环群，$Z_{12}=\{0,1,2,\ldots 11\},$因此$1\in G,$注意到$1^{12}=0=e,$有群元$1$的阶是$12$

所以，由群元1生成的循环子群 $<1>$ 的阶是12，等于G的阶，故有 $<1>=G=\{0,1,2...11\}$

因此，G是一个12阶循环群，生成元共有$\varphi(12)=4$个，有一个生成元$a=1$

下面求G的所有子群，循环群的子群仍然是循环群

$<1>$的阶是12，12的正因子是$1,2,3,4,6,12,$因此可以构成这些阶的子群，且各阶子群有且只有1个

1阶子群：有$\varphi(1)=1$个生成元，形如$a^j=1^j$($\oplus$运算)，$(j,12)=\dfrac{12}{1}=12,$因此$j=12,$生成元$1^{12}=0$

子群为 $<0>=\{0\};$

2阶子群：有$\varphi(2)=1$个生成元，$(j,12)=\dfrac{12}{2}=6, j=6,$生成元$1^6=6,$子群为 $<6>=\{6,0\}$

3阶子群：有$\varphi(3)=2$个生成元，$(j,12)=\dfrac{12}{3}=4, j=4,8;$生成元$1^4=4, 1^8=8,$子群为$\{4,8,0\}$

4阶子群：有$\varphi(4)=2$个生成元，$(j,12)=\dfrac{12}{4}=3, j=3,9;$生成元$1^3=3, 1^9=9,$子群为$\{3,6,9,0\}$

6阶子群：有$\varphi(6)=2$个生成元，$(j,12)=\dfrac{12}{6}=2, j=2,10,$生成元$2,10,$子群为$\{2,4,6,8,10,0\}$

12阶子群：有$\varphi(12)=4$个生成元，$(j,12)=\dfrac{12}{12}=1, j=1,5,7,11,$生成元$1,5,7,11;$子群为$Z_{12}$

课堂练习：证明素数阶群一定是循环群。

设素数阶群G，阶为素数p；设其一子群为$G';$于是有

根据拉格朗日定理，子群G'的阶m一定有$m|p;$而p是素数，所以$m=1$或者$m=p$

如果G'的阶$m=1,$那么G'就是单位元$\{e\},$由于p是素数，$p\geq 2,$所以G存在非单位元元素$a;$

设$G'=<a>,$由于$a^1!=e,$所以G'的阶不等于$1,$因此$|G'|=p=|G|,$即$G'=G$

所以，原素数阶群$G=<a>,$是一个循环群.

证明：阶是 p^m 的群（p 是素数）一定包含一个阶是 p 的子群。

构造法.

设群G的阶是$p^m,$由于p是素数，$p\geq 2,$因此$\exists a\in G, a^n=e,$设循环子群$H=<a>$

根据拉格朗日定理，$|H|=n|p^m,$由于p是素数，根据标准分解式，$n=p^i, i\leq m$

$\because a^n=a^{p^i}\in G, a\in G;$所以显然$b=a^{p^{i-1}}\in G, b^p=a^{p^i}=a^n=e$

p是使得$b^m=e$最小的m值，因此元素b的阶是$p,$因此循环子群 $<b>$ 的阶就是$p,$证明成立.

课堂练习： 假定 a 和 b 是一个群 G 的两个元，并且 $ab=ba$。又假定 a 的阶是 m，b 的阶是 n，并且 $(m,n)=1$。证明：ab 的阶是 mn。

G为一个群，$a,b\in G, ab=ba,$ 由群的运算封闭性，$ab\in G,$ 设ab的阶为$k,(ab)^k=e$
根据题干，$a^m=b^n=e,$ 因此 $(ab)^{mn}=(a^m)^n(b^n)^m=e,$ 根据群元阶的性质，$k|mn$
而 $(ab)^k=a^kb^k=e,$ 所以 (b^k)是群元 (a^k)的逆元，设a的逆元是a^{-1}，于是 $(aa^{-1})^k=a^ka^{-k}=e$
所以，$(a^{-1})^k=a^{-k}$也就是a^k的逆元，所以根据逆元唯一性，$b^k=a^{-k}$
所以，$(b^n)^k=b^{kn}=(a^{-k})^n,$ 注意到$b^n=e,$ 所以$a^{-kn}=e$
所以$m|(-kn),$ 也就是$m|kn,$ 又根据题干条件 $(m,n)=1,$ 所以 $(m,kn)=(m,k)=m,$ 也就是$m|k$
同理，a^k是群元b^k的逆元，也就有了$a^k=b^{-k}$，根据$a^m=e;$ 于是有$a^{km}=b^{-km}=e$
所以$n|km,(n,km)=n,$ 根据 $(n,m)=1$有 $(n,km)=(n,k)=n,$ 所以$n|k,$
由以上有$m|k,n|k$所以 $[m,n]|k,$ 而 $(m,n)=1,$ 因此 $[m,n]=mn;$ 所以$mn|k,$ 又$k|mn,$ 所以$k=mn$

课堂练习3： p,q为不同素数，证明不存在pq阶整环。

反证法．假设p,q为不同素数时，存在pq阶的整环$R,$ 根据整环的定义
R是一个交换环（乘法也交换），有乘法单位元，没有零因子
$<R,+>$ 构成一个pq阶的$Abel$群，由于p,q是不同素数，$(p,q)=1,$ 由西罗定理
$\exists$群元$a,b\in<R,+>,$ 满足 $|a|=p,|b|=q;$
而 $(p,q)=1,$ 所以a(运算)$b=a+b$的阶是$pq=|R|,$ 所以 $<R,+>$ 是一个循环群，生成元$c=a+b$

$$\sum^{pq}c=cpq=e=0,(<R,+>\text{ 的单位元是}0)$$

$R=\{c,2c,\ldots pqc=0\},$ 取R中的元素$x=pc,y=qc$进行乘法运算，$xy=yx=pqc=0$
而x,y显然不是零元，所以x,y是R的零因子，这与R是整环，没有零因子矛盾，因此不存在．

例10.1.3 $\mathbf{Z}/6\mathbf{Z}=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$ 是一个有单位元的交换环.

对于$Z/6Z,+$和 $\times$ 运算都会模$6,$ 因此结果仍然属于$Z/6Z$，运算封闭性满足
设元素$a,b,c\in Z/6Z$
对于 $+$ 法，$a+b=b+a,(a+b)+c=a+(b+c),$ 满足结合律，交换律
$\bar{0}\in Z/6Z,$ 且$\forall a\in Z/6Z,$ 有$a+\bar{0}=a,$ 所以$\bar{0}$是 $+$ 的单位元，$a+(6-a)=\bar{0},$ 每个元素有逆元
所以，对于 $+$ 法，$Z/6Z$构成一个交换群．
对于 $\times$ 法，$(a\times b)\times c=a\times(b\times c),a\times b=b\times a,(a+b)\times c=a\times c+b\times c,$ 满足结合律，交换律，分配律
又$\bar{1}\in Z/6Z,$ 而$a\times\bar{1}=a,$ 所以a是 $\times$ 的单位元，综上，这是一个有单位元交换环

例10.1.4 $M_2(\mathbf{Z})=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\mid a,b,c,d\in\mathbf{Z}\right\}$ 对于矩阵的加法和乘法是一个有单位元和零因子的非交换环.

证明如下：

对于 ＋法，$A=\begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}, B=\begin{bmatrix}a_2 & b_2\\ c_3 & d_2\end{bmatrix}, C=\begin{bmatrix}a_3 & b_3\\ c_3 & d_3\end{bmatrix}$

显然$A+B=B+A=\begin{bmatrix}a_1+a_2 & b_1+b_2\\ c_1+c_2 & d_1+d_2\end{bmatrix},(A+B)+C=A+(B+C),$

而且运算结果$M\in M_2(Z)$，因此 ＋满足结合律，交换律，具有封闭性

注意到$e=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\in M_2(Z), A+e=A,$ 所以e是 ＋的单位元，对于$A, A'=\begin{bmatrix}-a_1 & -b_1\\ -c_1 & -d_1\end{bmatrix}$是逆元

所以对于 ＋法构成$Abel$群

对于 ×法，由矩阵乘法性质，$(AB)C=A(BC)\in M_2(Z),(A+B)C=AC+BC\in M_2(Z)$

满足结合律，分配律，具有运算封闭性

$\therefore M_2(Z)$是一个环，进一步地：

对于 ×运算，$I=\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}\in M_2(Z), A\times I=A,$ 所以是一个有单位元环

$E=\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}\in M_2(Z), E\times E=0,$ 而$E\neq 0,$ 所以是一个有零因子环

而根据矩阵乘法性质，$A\times B\neq B\times A,$ 所以是一个非交换环

综上，$M_2(Z)$是一个有单位元，零因子的非交换环

(7) 设 p 是奇素数. 证明: $\mathbf{Z}/p^2\mathbf{Z}$ 中的可逆元对乘法构成一个循环群, 并求其阶.

证明如下：

Z/p^2Z中的运算要模p^2，p是奇素数，根据模m存在原根的充要条件可知，模奇素数p^2存在原根g

g是模p^2的原根，根据原根的性质，$\{g^0, g^1\ldots g^{\varphi(p^2-1)}\}$构成了模$p^2$的简化剩余系

根据题干信息，元素为Z/p^2Z中的可逆元，设$\forall a\in Z/p^2Z$，a即可逆元，因此

$ax\equiv 1 \pmod{p^2}$有解，所以$(a,p^2)=1,$ 所以a也在模p^2的简化剩余系中

所以，Z/p^2Z中的可逆元就是构成模p^2的简化剩余系$(Z/p^2Z)*$，而$\{g^0, g^1\ldots g^{\varphi(p^2-1)}\}$也构成

模p^2的简化剩余系，因此原群 $=(Z/p^2Z)*=\{g^0, g^1\ldots g^{\varphi(p^2-1)}\}=<g>$

原群可以由原根g生成，是一个循环群.

课堂练习4：求$<\mathbb{Z}_6,\oplus,\otimes>$的理想及商环

理想是是一个子环，作为环，$\oplus$构成交换群，$\otimes$构成半群

既然子环是一个 $\oplus$ 群，阶同样满足拉格朗日定理，$<Z_6,\oplus,\otimes>$ 的阶是6，其因数是

$1,2,3,6,$ 子环的阶只有这几种情况

$\{0\}$和Z_6是Z_6的理想，是平凡理想

$2,3$阶集合中 $\otimes$ 满足半群(有封闭性)，$\oplus$满足$Abel$群

2阶子环只有$I_1=\{3,0\}$，3阶子环只有$I_2=\{2,4,0\}$，再验证其是否为理想

$\forall r\in<Z_6,\oplus,\otimes>, \forall a\in I_1$或$I_2$，$ar=ra\in I_1$或者$I_2$

所以I_1, I_2均是理想

$<Z_6,\oplus,\otimes>$ 的理想是$\{0\},\{3,0\},\{2,4,0\},Z_6$

$<Z_6,\oplus,\otimes>$ 商环是：

$Z_6/\{0\}=\{\{0\},\{1\},\{2\},\{3\},\{4\},\{5\}\}$

$Z_6/\{3,0\}=\{\{3,0\},\{4,1\},\{5,2\}\}$

$Z_6/\{2,4,0\}=\{\{2,4,0\},\{3,5,1\}\}$

$Z_6/\{Z_6\}=\{\{Z_6\}\}=\{Z_6\}$