引理：

P284.58 由于对Abel群，$|G|=n$，若素数$p|n$，则G中有p阶元

故由引理知此处存在p阶元a，q阶元b，$a\neq b$，由Abel群定义，$ab=ba$，故$|ab|=|ba|=pq=|G|$，从而G是由ab生成的循环群. 设生元为f，则$G=\langle f\rangle=\{e,f,\cdots,f^{pq-1}\}$

若H中有p阶元，也有q阶元，则亦可记$|H|=pq$，从而$H=G$

$G/H=\{[G]\}$为循环群，若H中既无p，也无q阶元，则H只有1阶元（pq阶元存在则分别含p、q阶元均存在），$H=\{e\}$

$G/H=\{[x]\mid x\in G\}$亦为循环群. 若H中仅有p阶元或仅有q阶元，不妨仅有p阶元，则$\{e,g,\cdots,g^{p-1}\}\subseteq H$，由于循环群子群也是循环群，故$p\mid|H|$，又$|H|\neq pq$，故$|H|=p$，从而$H=\{e,g,\cdots,g^{p-1}\}$，下面证明

$G/H=\{f^{ip}H\mid i\in N\}$，若$f^{ip}H=f^{jp}H$，$(i\neq j)$

则$f^{(i-j)p}\in H$，$f^{(i-j)p}\neq e$，故$|f^{(i-j)p}|=p$.

$f^{(i-j)p^2}=e$，$p^2\nmid f^{(i-j)p}$，从而$pq\nmid(i-j)p^2$，矛盾！

故$f^{ip}H$互不等，共q个. 又$|G/H|=\frac{|G|}{|H|}=q$，故G/H即为素阶的

且G/H也是循环群（因f与g可交下）

No.

Date

P284. 62.

(1) φ_t 将单位元 $e=a^0$ 映为 $a^{0t}=e$.

$a^{it} \in G$, 映射良定义.

$\varphi_t(a^i \cdot a^j) = \varphi_t(a^{i+j}) = a^{(i+j)t} = a^{it+jt} = a^{it} \cdot a^{jt}$

$= \varphi_t(a^i) \cdot \varphi_t(a^j)$, 故为自同态.

(2) $G/\ker\varphi_t \cong \mathrm{Im}\,\varphi_t$, $\frac{|G|}{|\ker\varphi_t|} = |\mathrm{Im}\,\varphi_t|$

φ_t 为自同构 $\Leftrightarrow |\mathrm{Im}\,\varphi_t| = |G| \Leftrightarrow |\ker\varphi_t| = 1$.

若 $(n,t)=1$. 则若 $a^i \to a^{it} = e$.

$n \mid it$, $i \le n$ 时不成立, 仅 $i=0$ 时成立. 故 $|\ker\varphi_t| = 1$.

若 $(n,t)>1$, 则 $a^{\frac{n}{(n,t)}} \to a^{\frac{nt}{(n,t)}}$, $n \mid \frac{nt}{(n,t)}$,

故 $a^{\frac{nt}{(n,t)}} = e$. 导致 $|\ker\varphi_t| > 1$.

故 $(n,t)=1 \Leftrightarrow |\ker\varphi_t| = 1 \Leftrightarrow \varphi_t$ 为自同构

No.

Date

6. 设 G 为群，C 为 G 的中心. 证明 $G/C \cong \mathrm{Inn}G$.

考虑同态 $\varphi: G \to \mathrm{Inn}G$,

$x \mapsto \varphi_x : a \to xax^{-1}$

$\varphi(xy^{-1}) = \varphi_{xy^{-1}}$

$\forall a \in G, \varphi_{xy^{-1}}(a) = xy^{-1}ayx^{-1} = \varphi_x(\varphi_{y^{-1}}(a))$

故 $\varphi_x \cdot \varphi_{y^{-1}} = \varphi_{xy^{-1}}$

从而保运算，又 $\mathrm{Inn}G$ 单位元为 φ_e, e

$\varphi(e) = \varphi_e$, 故为同态.

再证 $\ker\varphi = C$. $\varphi_x = I$

$C \subseteq \ker\varphi$ 是显然的（因为 $\forall c \in C, xc = cx, \forall x \in G$）

$\forall \varphi_x = I$, 有 $xax^{-1} = a$, 即 $xa = ax$ 对 $\forall a$ 成立.

即 $x \in C$. 故 $\ker\varphi = C$.

由同态定理，$G/C \cong \mathrm{Inn}G$.

No.

Date

P284. 68 不证 $G \cong \{(gH, gK) \mid gH \in G/H,\ gK \in G/K\} = T$

首先证明 $T \leq G/H \times G/K$.

$T \subseteq G/H \times G/K$, 且单位元 $(H \cdot \cdot K) = (eH, eK) \in T$

又 $\forall (xH, xK), (yH, yK) \in T$. 因 H, K 为 正规子

$(xH, xK) \cdot (yH, yK)^{-1} = (xH \cdot xK) \cdot (y^{-1}H, y^{-1}$

$= (xy^{-1}H, xy^{-1}K) \in T$.

故 $T \leq G/H \times G/K$,

再证 $G \cong T$.

对 $\forall g_1 \neq g_2 \in G$, 若 $(g_1H, g_1K) = (g_2H, g_2K)$

则 $g_1 g_2^{-1} \in H \cap K$, 因 $H \cap K = \{e\}$, 故 $g_1 g_2^{-1} = e$

$g_1 = g_2$ 与假设矛盾.

故 $T \cong G$ 即 $G \cong T \leq G/H \times G/K$.

P297.5

(2) $\forall a\in R$, $(a+a)^2=a+a$, $(a+a)^2=a^2+a^2+a^2+a^2$
$=a+a+a+a=a+a$ 故 $a+a=0$.

(1) $\forall x,y\in R$, $(x+y)^2=x^2+xy+yx+y^2=x+xy+yx+y$
又 $(x+y)^2=x+y$, 故 $xy+yx=0$, 又 $\forall a\in R$
$a+a=0$, 故 $xy=yx$, R可交换

(3) 若 $|R|>2$. 若为整环, 有0, 1. ~~设a, b, c为R中3个互异元素~~ $\forall a\in R$, 若 $a\neq 0$ 且 $a\neq 1$
考虑 $a+a=0=a^2+a=a(a+1)$
因若R为整环, 要么 $a=0$ 要么 $a=-1=1$
故 $|R|\le 2$. 矛盾!

No.

Date

P297.7

(1) 设因 n 非零数故 $p|n$，p为素数

$\frac{n}{p}\cdot p = p\cdot\frac{n}{p} = n = 0$，故 $\frac{n}{p}$，p为零因子

(2) r是 Z_n 的零因子 $\Leftrightarrow ra \equiv 0 \pmod n$ $(n\nmid a)$

$\Leftrightarrow \frac{n}{(n,a)} \mid r$，$\Leftrightarrow (r,n)\neq 1$

故 $(r,n)=1 \Leftrightarrow$ r不是 Z_n 中的零因子

(3) Z_{18} 中的全体零因子为 2, 3, 6, 9

P297.11 考虑有限整环 $R=\{a_1,\cdots,a_n\}$，对 $\forall a$ 非零元，考虑 $aa_1,\cdots,aa_n$，知 $aa_i\neq aa_j$，否则，$a(a_i-a_j)=0$，导致 a 为零因子，矛盾！

又 $\{aa_1,\cdots,aa_n\}\subseteq\{a_1,\cdots,a_n\}$

故 $\{aa_1,\cdots,aa_n\}=\{a_1,\cdots,a_n\}$

从而 $aa_i=e$，从而 a 可逆，从而 R 可交换整环，从而为域.

P297.12 首先，域的特征必为素数，否则若 $n=pn_0$，$n_0>1$，p为素数，则对乘法幺元 e，$ne=0$，~~$p(n_0e)=0$~~ $(pe)\cdot(n_0e)=0$

~~$e+\cdots+e\neq 0$，与n的最小性矛盾！~~

因域中无零因子，故 $pe=0$ 或 $n_0e=0$，都将与n的最小性矛盾.

对素数 p，$(a+b)^p=a^p+b^p$ 成立，这是因为其余项为 $\sum C_p^i a^i b^{p-i}$，$p\mid C_p^i$，故 $C_p^i a^i b^{p-i}=0$ 均成立.