六、（10分）证明 pq 阶群必可解，这儿 p,q 为素数且 $p>q$.

设 G 为群且 $|G|=pq$

则 G 有 Syl_p p-子群和 Syl_q q-子群

个数 n_p 个数 n_q

$n_p|q$ 且 $n_p=1+k_q$ ~~$n_q|p$ 且 $n_q=1+k_q$~~

$\because q<p$ 且 $n_p=1$.

$\therefore G$ 有正规 Syl_p p-子群 H

$\{e\}\trianglelefteq H\trianglelefteq G$

$|G/H|=|G|/|H|=q$ 为素数 $\therefore G/H$ 为Abel群

$|H|=p$ 也为Abel群

故 $\{e\}\trianglelefteq H\trianglelefteq G$ 为 G 的一个正规群列

即 G 可解.

七、（每小题5分，共15分）设 G 为有限 Abel 群，对 $g\in G$ 我们以 $o(g)$ 表示 g 的阶。

(1) 设 $o(a)=p^\alpha m$, $o(x)=p^\beta n$, 这儿 $a,x\in G$, p 为素数，$p\nmid mn$ 且 $0\leqslant\alpha<\beta$. 试证对 $y=a^{p^\alpha}x^n$ 有 $o(y)=p^\beta m>o(a)$.

设 $o(y)=k$. 则 $y^k=(a^{p^\alpha}x^n)^k=a^{p^\alpha k}\cdot x^{nk}=e$

$\therefore a^{p^\alpha k}=x^{-nk}$ $e=a^{p^\alpha km}=x^{-nkm}$

故 $p^\beta n\mid nkm\Rightarrow p^\beta\mid km$ $\because p\nmid m$ $\therefore p^\beta\mid k$

$e=x^{-nk\cdot p^\beta}=a^{p^\alpha k\cdot p^\beta}$ $\therefore p^\beta m\mid p^\alpha k p^\beta$ 即 $m\mid kp^{\beta-\alpha}$ $\therefore o(y)=p^\beta m>o(a)$

又 $m\nmid p$ $\therefore m\mid k$. 又 $(p,m)=1$ 故 $p^\beta m\mid k$.

$y^{p^\beta m}=(a^{p^\alpha}\cdot x^n)^{p^\beta m}=a^{p^{\alpha+\beta}m}\cdot x^{np^\beta m}=e$

(2) 设 $a\in G$ 且 $o(a)=\max_{g\in G}o(g)$. 则对任何 $x\in G$ 有 $o(x)\mid o(a)$. [提示：如果 $o(x)\nmid o(a)$ 则有素数 p 及 $0\leqslant\alpha<\beta$ 使得 $o(a)=p^\alpha m$ 且 $o(x)=p^\beta n$, 其中 m 与 n 都不被 p 整除.]

证：设 $o(a)=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ ($p_1\cdots p_n$ 为不同所有素因数 $\alpha_i\geqslant 0$)

$o(x)=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$

若 $\forall i$ $\beta_i\leqslant\alpha_i$ 则 $o(x)\mid o(a)$

若 $o(x)\nmid o(a)$ 则 $\exists i$ s.t. $\beta_i>\alpha_i$

设 $o(a)=p_i^{\alpha_i}m$ $o(x)=p_i^{\beta_i}m$ ($\beta_i>\alpha_i\geqslant 0$)

由(1)对 $y=a^{p^{\alpha_i}}x^n$ 有 $o(y)>o(a)$ 与 $o(a)=\max_{g\in G}o(g)$ 矛盾 故 $o(x)\mid o(a)$

(3) 假如对任何正整数 m, 方程 $x^m=e$ 在 G 中解数不超过 m. 证明 G 必为循环群. [提示：利用 (2)]

设 $o(a)=\max_{g\in G}o(g)$

令 $m=o(a)$

$\because \forall x\in G$ $o(x)\mid o(a)=m$

$\therefore \forall x\in G$ $x^m=e$ 即 $\forall g\in G$ g 为 $x^m=e$ 的解.

又 $x^m=e$ 在 G 中解的不超过 m

故 $|G|\leqslant m$.