L5

No.

Date

→ re:

由这个例子可知：Abel + $A\cap B=\{e\}$ 为核心条件

例：$G=(\mathbb{Z}_{15},+)$，$A=\langle 3\rangle$ $B=\langle 5\rangle$；$G\cong A\times B$ direct product

一般情况下 $|G|=|A|\times|B|$，$A\le G$ $B\le G$ $A\cap B=\{e\}$ ⇔ $G\cong A\times B$ 是否成立？"⇐"✓ "⇒"✗

"⇒" $\varphi:(a,b)\to a\times b$

$a_1b_1=a_2b_2$，$a_1^{-1}a_2=b_1b_2^{-1}\in A\cap B=\{e\}$ ∴ $a_1=a_2$ $b_1=b_2$ φ injective

$A\cap B=\{e\}$ $\forall ab\in G$ 且 inj，$|G|=|A|\times|B|$ ∴ φ surjective

$\varphi(a_1b_1)\times\varphi(a_2b_2)=a_1\times b_1\times a_2\times b_2\neq\varphi((a_1,b_1)(a_2,b_2))=a_1a_2\times b_1b_2$ ∴ φ 不一定满足 homo

⇓

再加条件 "$A\trianglelefteq G$ $B\trianglelefteq G$" + $A\cap B=\{e\}$ ⇒ "$\forall a\in A, b\in B$ $a\times b=b\times a$"

Th：$HK=G$，$H\trianglelefteq G$，$K\trianglelefteq G$ then：

(1) $\Phi: H\times K\to G$ $(h,k)\to hk$ isomorphism (2) $H\cap K=\{e\}$ (1)⇔(2)

HK 先得是群

"⇒" 只用 injective 即可

"⇐" injective + surjective 同上，

$ab=b\times a$ ⇔ $ab(ba)^{-1}=aba^{-1}b^{-1}=e$ ⇐ $aba^{-1}b^{-1}\in A\cap B=\{e\}$ "◁"

Th：G group of order p^2，p is prime number；则 $G\cong\mathbb{Z}_{p^2}$，or $G\cong\mathbb{Z}_p\times\mathbb{Z}_p$ （G is Abel）

后面 L10 会证必定 Abel P34

$\forall g\in G$ $g\neq e$ $\langle g\rangle\le G$

$o(g)\mid|G|$ ∴ $o(g)=p$ or $o(g)=p^2$

(1)：$\exists x\in G$，$o(g)=p^2$，$G=\langle x\rangle=\{x^0,x^1,\cdots x^{p^2-1}\}\cong\mathbb{Z}_{p^2}$，G is Abel

(2)：$\forall x\in G$ $o(g)=p$：$\langle x\rangle=\{x^0,x^1,\cdots x^{p-1}\}\cong\mathbb{Z}_p$

take $y\in G\setminus\langle x\rangle$，$\langle y\rangle=\{y^0,y^1,\cdots y^{p-1}\}\cong\mathbb{Z}_p$ ∴ $\langle x\rangle\times\langle y\rangle\cong\mathbb{Z}_p\times\mathbb{Z}_p$

define $\varphi:\langle x\rangle\times\langle y\rangle\to G$

φ surjective and injective

这种情况下一定需要 Abel 证明 homo：$\varphi(x^i,y^j)\varphi(x^{i'},y^{j'})=x^iy^j\times x^{i'}y^{j'}=x^ix^{i'}y^jy^{j'}$

def：Sym(Ω) 的子群称为 permutation group；$G\le$ Sym(Ω)，G is transitive on Ω

if $\forall\alpha\beta\in\Omega$ $\exists r\in G$，$\alpha^r=\beta$

KOKUYO

即：任找一个 m 阶循环群 $\langle k\rangle = \langle e, k, k^2, \cdots k^{m-1}\rangle$ 均可满足 $|k|=m$，$\langle k\rangle \cap H = \{e\}$ 这即所需

不行

②: consider: $K=\{k\in G: k^m=e\}$；已知 $\forall h\in H$, $|h|=p^r$ some r

证明过程记下来：$x\in K\cap H$ $x^m = x^{p^r} = e$ $\therefore |\langle x\rangle| \mid m$, $|\langle x\rangle| \mid p^r \Rightarrow |\langle x\rangle| = 1$ $x=e$

Th: G: finite Abel group of order n, $n=p_1^{t_1}\cdots p_r^{t_r}$, p_i 均为质数，then:

(1): $G = G_1 \times \cdots G_r$, $|G_i| = p_i^{t_i}$ (2) G is a direct product of cyclic groups

(1): let $n = m\times p^t$, $p=p_i$ $t=t_i$ some i, p coprimes with m

$H = \{g^m : g\in G\}$

G Abel: $g_1^m g_2^m = (g_1 g_2)^m \in H$ $\therefore H$ is subgroup 注意 $g_1^m g_2^m = (g_1 g_2)^m$ 不恒等成立！

$\forall h\in H$ $h = g^m$ some m, $o(h)=k$

$(g^m)^k = e$, $mk \mid mp^t$ $\therefore k$ is p-power since $k\mid p^t$，即每个元素在H均有 p^n 阶

又 $\forall h\in H$ $o(h) \mid |H|$, $|H|$ is p-power

(1)用(2)证：$|HK| = \frac{|H|\cdot|K|}{|H\cap K|} = |H|\times|K| \neq 1$

$\Rightarrow |H| = p^t$ ---① ✓

$\exists K\leq G, |K|=m, K\cap H = \{e\}$ ---② ?

→CAA P217

Th2: G finite Abel group, $m \mid |G|$, then G has a subgroup of order m

induct on $|G|=n$

$n=1$, then $m=1$ subgroup $=G$

$n\neq 1$: let prime p: $p\mid m$ ($p=m$ 也行)

by Th1: G has a subgroup K of order p

G/K is Abelian with order $n\div p$, and $m\div p \mid |G/K|$

Inn 5/7

P183 CAA　product = internal direct product：$G=HK$ 是一对充且 homo 3

distinguish "$G=HK$" 集合意义的相等，$G=H\times K$：还要加上 $\phi: H\oplus K\to G$ 这D

$G=H\oplus K$ 直和 (h,k)，有时候会混用 "×"；自己不要这么写，知道就好

Th1 CAA P212 (fundamental theorem of Finite Abelian group):

∀ finite Abel group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product, and the order of the cyclic groups, are uniquely determined the group.

已知一个阶为 n 的循环群 $\langle g\rangle=\{g^0,g^1,\cdots g^{n-1}\}\cong \mathbb{Z}_n$

Any finite Abel group $\cong \mathbb{Z}_{p_1^{n_1}}\oplus \mathbb{Z}_{p_2^{n_2}}\oplus\cdots\mathbb{Z}_{p_k^{n_k}}$

⇒CAA P218

Lem1: G is finite Abel group of order p^nm; p is prime, p, m coprime; then:

$G=H\times K$, where $H=\{x\in G: x^{p^n}=e\}$, $K=\{x\in G: x^m=e\}$; $|H|=p^n$, $|K|=m$

G Abel, $H\le G$, $K\le G$ 易知　3组等前提　Cauchy

(1) ☆：在 Abel 情况下，$G=H\times K\Leftrightarrow H\cap K=\{e\}$, $G=HK$ "①+②"

$\gcd(p^n,m)=1$ ∴∃ s,t∈ℤ, $sp^n+tm=1$　这重要

$\forall x\in G$, $x=x^1=x^{sp^n}\cdot x^{tm}\in HK$ since $x^{sp^n}\in K$, $x^{tm}\in H$ ∴ $G\subseteq HK$

$HK\subseteq G\Rightarrow HK=G$ …①

设 $x\in H\cap K$, $x^{p^n}=e=x^m$ ∴ $|x|\mid p^n$, $|x|\mid m$ ∴ $|x|=1$ $x=e$ …③

(2): $|G|=p^nm=|HK|=\frac{|H|\cdot|K|}{|H\cap K|}$　K也 finite Abel，否则 K 有 p 阶元素了 同④矛盾

代入：$p^nm=|H|\cdot|K|$ ∴ $|H|=p^n$ since $p\nmid|K|$ … P182 CAA

Cauchy lem1.1: G is finite Abel, p is prime $p\mid|G|$; ∃g∈G o(g)=p

对 |G| 进行归纳，$|G|=2$，易知结论成立 …①'

Sylow-1 阿贝尔 设 $|G|<n$，结论均成立 …②'

$|G|=n$，设 $o(x)=q$ for some prime q; 设 $p=q$ finished

(claim: 任何 group 均有 prime 阶元素，

证：设 $o(x)=t$, $t=q\times\cdots$，分解质因数 $o(x^{\cdots})=q$)

设 $p\neq q$, ∀subgroup in Abel group is normal,

∴ construct $G/\langle x\rangle$, which is also Abel

$|G/\langle x\rangle|=|G|/|\langle x\rangle|=n/q$ (找格式用的)　∴ $p\mid|G/\langle x\rangle|$

②' → ∃ $y\langle x\rangle\in G/\langle x\rangle$, $o(y\langle x\rangle)=p$

$(y\langle x\rangle)^p=y^p\langle x\rangle=\langle x\rangle$ (e)　最小的 $|x|=q$

∴ $y^p\in\langle x\rangle$　$y^{pq}=e$

∴ $y^{\cdots}$ has order q

{ CAAP80 coro3: $|a|=n, \langle a^i\rangle=\langle a^j\rangle \Leftrightarrow \gcd(n,i)=\gcd(n,j)=1$; $|\langle a\rangle|=|\langle a^i\rangle| \Leftrightarrow \gcd(n,i)=1$
P78 th: $|\langle a\rangle|=n$, $k\in\mathbb{N}^+$, then $\langle a^k\rangle=\langle a^{\gcd(n,k)}\rangle$ $|\langle a^k\rangle| = n\div\gcd(n,k)$ ⇒ 证明此右面

Lem2直接可知 ↓

Lem3: A finite Abelian group of prime-power order is an internal direct product of cyclic groups

Lem1说明: 任Abel group G with $|G|=p_1^{r_1}p_2^{r_2}\cdots p_n^{r_n}$

$G=G_1\times G_2\times\cdots G_n$, $|G_i|=p_i^{r_i}$ 比如, some $G_1, G_2\cdots$ (G_i不唯一)

现在要说明的是每个G_i均可以写成 cyclic group 的内直积, 继续分解G

Lem2: G: finite Abel group of prime-power order, a为G中阶最大的元素, 则:

$G=\langle a\rangle\times K$, $K\leq G$.

Induct on $|G|$, $|G|=1$ 时 $G=\langle e\rangle\times\langle e\rangle$ (并不是要找阶=p的, 而是不在$\langle a\rangle$中的)

设结论对于 $\forall k\leq n$, $|G|=p^k$ 成立, ↓

$|G|=p^n$ 时: 设 $O(a)=p^m$ is the maximum order; $G=\langle a\rangle$ finished

$G\neq\langle a\rangle$. Let $b\in G$ $b\notin\langle a\rangle$, 有最小的order

接下来说明最小阶为p: $|b^p|=|b|\div p$ ∴ $b^p\in\langle a\rangle$ 不然b^p是$\langle a\rangle$外order最小的

$b^p=a^i$,

$O(b)<O(a)=p^m$ ∴ $b^{p^m}=b^{p\cdot p^{m-1}}=(a^i)^{p^{m-1}}$ ∴ $|a^i|\leq p^{m-1}$

CAAP80 ↓ ∴ a^i不为$\langle a\rangle$的生成元, $\langle a^i\rangle\neq\langle a\rangle$

∴ $\gcd(p^m,i)\neq 1$,

∴ $p\mid i$ 因为p^m只有p这个因数, Let $i=pj$

∴ $b^p=a^i=a^{pj}$

考虑 $c=a^{-j}b$, $c\neq\langle a\rangle$, $c^p=a^{-jp}b^p=e$

$\langle b^k\rangle=\langle b\rangle$ 可以由P80 coro3推出右面 $\gcd(k,p)=1$ 或 $O(b)=p$, 如下步骤 $b^k\neq e$

∴ 在$\langle a\rangle$外找到一个元素 c, $O(c)=p$ ⇒ $b=c$

∴ $\langle a\rangle\cap\langle b\rangle=\{e\}$ 否则 $x=b^k=a^k$, 用x所生成$\langle b\rangle$:

Consider $G/\langle b\rangle$, if $|\langle a\rangle\langle b\rangle|<|\langle a\rangle|=p^{m-t}$

$(a\langle b\rangle)^{p^{m-t}}=a^{p^{m-t}}\langle b\rangle=\langle b\rangle$

∴ $a^{p^{m-t}}\in\langle a\rangle\cap\langle b\rangle=\{e\}$, 与$O(a)=p^m$矛盾

∴ $|a\langle b\rangle|=|\langle a\rangle|=p^m$

∴ $a\langle b\rangle$在$G/\langle b\rangle$中有最大的order p^m

$|G/\langle b\rangle|=p^{n-1}$ 符合归纳假设 ∴ 有$K/\langle b\rangle$ s.t. $G/\langle b\rangle=\langle a\rangle/\langle b\rangle\times K/\langle b\rangle$

No.

Date

G is Abel ∴ $G/\langle b\rangle = \langle a\rangle/\langle b\rangle \times K/\langle b\rangle \Rightarrow \langle a\rangle/\langle b\rangle \cap K/\langle b\rangle = \langle b\rangle$, $\langle a\rangle \cap K = e$

Let $\bar{K} = \{x \in G : x/\langle b\rangle \in K/\langle b\rangle\}$ this is OK for $G = \langle a\rangle \times K$

归纳递推成功

lem1 + lem2 → 3: $G = G_1 \times G_2 \times \cdots G_n = (\langle a_1\rangle \times \cdots \langle a_n\rangle) \times (\langle b_1\rangle \times \cdots \langle b_m\rangle) \cdots \times (\langle f_1\rangle \times \cdots \langle f_n\rangle)$

即 finite Abel group 均可写成 cyclic group 的内直积

上课没讲，再说吧

lem4: 对于上面的 G, $G = H_1 \times H_2 \times \cdots \times H_m$, $G = K_1 \times K_2 \times \cdots \times K_n$, H_i 与 K_i are non-trivial cyclic groups with $|H_1| \geq |H_2| \geq \cdots |H_m|$, $|K_1| \geq \cdots |K_n|$; then $m = n$, $|H_i| = |K_i|$ 长

GAA P78 th: $|\langle a\rangle| = n$, $k \in \mathbb{N}^+$, then $\langle a^k\rangle = \langle a^{\gcd(n,k)}\rangle$; $|\langle a^k\rangle| = n \div \gcd(n,k)$

首先求阶数 证 $|\langle a^k\rangle| = n \div \gcd(n,k) = \mathrm{lcm}(n,k) \div k$; 记 $\mathrm{lcm}(n,k) = l$

$o(a^k) = t$. $a^{kt} = e$

$o(a) = n$ $a^n = e$ ∴ $n \mid kt$

$t = \min\{s : n \mid ks\}$ ∴ $t = \mathrm{lcm}(n,k) \div k = n \div \gcd(n,k)$

$\gcd(n,k) \leq k$ ∴ $\langle a^k\rangle \leq \langle a^{\gcd(n,k)}\rangle$

$|\langle a^k\rangle| = n \div \gcd(n,k) = |\langle a^{\gcd(n,k)}\rangle|$ ∴ $\langle a^k\rangle = \langle a^{\gcd(n,k)}\rangle$

P80 cor 3: $\langle a\rangle = \langle a^i\rangle \Leftrightarrow \gcd(n,i) = 1$; $|\langle a\rangle| = |\langle a^i\rangle| \Leftrightarrow \gcd(n,i) = 1$

↑ 易知；$\Rightarrow$ 用阶数；$\Leftarrow$ 用阶数 + subgroup 关系知 由 Th 易

cor 2: $\langle a^i\rangle = \langle a^j\rangle \Leftrightarrow \gcd(n,i) = \gcd(n,j)$; $|\langle a^i\rangle| = |\langle a^j\rangle| \Leftrightarrow \gcd(n,i) = \gcd(n,j)$

$\Leftarrow$ "$\langle a^i\rangle = \langle a^{\gcd(n,i)}\rangle = \langle a^j\rangle = \langle a^{\gcd(n,j)}\rangle$" ; $\Rightarrow$ "阶数" 易