date: wednesday, january 17, 2024

Fundamental Theorem of Finite Abelian Groups III

Lemma 1: Suppose G is an abelian group with $|G| = p_1^{a_1} \cdots p_r^{a_r}$ (p_i distinct). For $i = 1, \ldots, r$, set

$$G_i = \{g \in G \mid |g| = p_i^{\alpha_i} \text{ for some } \alpha_i\}.$$

Then each G_i is a p_i-group and G is the internal direct product of $G_1, \ldots, G_r$.

Recall: Internal direct product definition: ① $G = G_1 \cdots G_r$
② $G_i \cap (\bigcup_{i \neq j} G_j) = \{e\}$
free since G is abelian $\longrightarrow$ ③ $g_i g_j = g_j g_i$ for all $g_i \in G_i$ and $g_j \in G_j$

Proof

First show each G_i is a p_i-group. They are subgroups because

- $e \in G_i$ since $|e| = 1 = p_i^0$
- Let $a, b \in G_i$. So $|a| = p_i^t$ and $|b| = p_i^s$. Then $|ab| = \operatorname{lcm}(|a|, |b|) = \operatorname{lcm}(p_i^t, p_i^s) = p_i^{\max(t,s)}$.

  So $ab \in G_i$.
- Let $a \in G_i$. So $|a| = |a^{-1}| = p_i^s$. So $a^{-1} \in G_i$.

This is a p_i-group since every element has order prime power.
We now check conditions ① and ② of direct product.
We do ②. Let $g \in G_i \cap (\bigcup_{i \neq j} G_j)$. So $g \in G_i \Rightarrow |g| = p_i^s$. But $g \in (\bigcup_{i \neq j} G_j)$ so $g \in G_j$ for some j. So $|g| = p_j^t$. So $p_i^s = p_j^t \Leftrightarrow s = t = 0 \Leftrightarrow |g| = 1 \Leftrightarrow g = e$.
To show $G = G_1 \cdots G_r = \{g_1 \cdots g_r \mid g_i \in G_i\}$, enough to show $G_1 \cdots G_r \supseteq G$. Let $g \in G$, so $|g| \mid |G| = p_1^{a_1} \cdots p_r^{a_r}$. So $|g| = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ with $0 \le b_i \le a_i$.
Let $\alpha_i = \frac{|g|}{p_i^{b_i}}$. So $\gcd(\alpha_1, \alpha_2, \ldots, \alpha_r) = 1$. There exists $c_1, \ldots, c_r$ such that $c_1\alpha_1 + \cdots + c_r\alpha_r = 1$. So

$$g = g^1 = g^{c_1\alpha_1 + \cdots + c_r\alpha_r} = g^{c_1\alpha_1} g^{c_2\alpha_2} \cdots g^{c_r\alpha_r}$$

Consider $(g^{c_i\alpha_i})$. Then,

$$(g^{c_i\alpha_i})^{p_i^{b_i}} = g^{c_i\alpha_i p_i^{b_i}} = g^{c_i|g|} = g^{|g|c_i} = e.$$

So, $|g^{c_i\alpha_i}| \mid p_i^{b_i} \Rightarrow$ So $g^{c_i\alpha_i} \in G_i$. Thus, $g = (g^{c_1\alpha_1}) \cdots (g^{c_r\alpha_r}) \in G_1 \cdots G_r$. $\square$

Lemma 2: Let G be a finite abelian p-group and let $g\in G$ with maximal order (ie. $|g|=p^m$, and $|h|\leq p^m$ for all other h). Then,

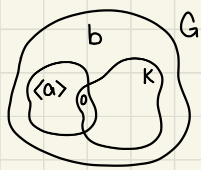
$$G\simeq\langle a\rangle\times K\simeq\mathbb{Z}_{p^m}\times K$$

where K is also a p-group.

Proof

Assume $|G|=p^\alpha$ and let $|a|=p^n$ be the element of largest order. Let K be the largest subgroup of G such that $\langle a\rangle\cap K=\{0\}$ (there is at least one, $K=\{0\}$ so K exists).

Goal is to prove $G=\langle a\rangle+K$ (this then implies G is the internal direct product of $\langle a\rangle$ and K).



Suppose $b\in G\setminus(\langle a\rangle+K)$. Let k be the smallest integer such that $p^kb=\underbrace{b+\cdots+b}_{p^k}\in\langle a\rangle+K$ (since $p^\alpha b=0$ for some α since $b\in G$ and G is a p-group, $p^\alpha b=0\in\langle a\rangle+K$, so such a k exists).

So $c=p^{k-1}b\notin\langle a\rangle+K$ but $pc=p^kb\in\langle a\rangle+K$. So $\boxed{pc=ta+k}$ (*) for some $t\in\mathbb{Z}$, $k\in K$. Since $|a|=p^n$, $p^nx=0$ for all $x\in G$ since a has the largest order. Thus,

$$0=p^nc=p^{n-1}(pc)=p^{n-1}(ta+k)=p^{n-1}ta+p^{n-1}k.$$

So

$$p^{n-1}ta=-p^{n-1}k\in\langle a\rangle\cap K=\{0\}\Rightarrow p^{n-1}ta=0.$$

Since $|a|=p^n$ and $(p^{n-1}t)a=0$, $p^n\mid p^{n-1}t\Rightarrow p\mid t\Rightarrow t=mp$.

Hence,

$$pc=ta+k=mpa+k$$
$$\Leftrightarrow k=pc-mpa=p(c-ma).$$

Set $\boxed{d=c-ma}$ (**). So $pd=k\in K$. On the other hand, $d\notin K$ because that would give $c=ma+d\in\langle a\rangle+K$.

Fact: Let $H=\{x+zd\mid x\in K, z\in\mathbb{Z}\}$. Then H is a subgroup of G that properly contains K.

Let $0\neq w\in\langle a\rangle\cap H$. Hence, $\boxed{w=sa=k_1+rd}$ (***) with $k_1\in K$, $r\in\mathbb{Z}$.

Claim: $p\nmid r$. If $p\mid r$, we have $r=py$ and since $pd\in K$, we have $0\neq w=sa=k_1+y(pd)\in\langle a\rangle\cap K=\{0\}$ (contradiction). Since $p\nmid r$, $\gcd(p,r)=1\Rightarrow pu+rv=1$ for some u,v.

$$
\begin{aligned}
c = c\cdot 1 = c(pu+rv) &= u(pc)+vrc \\
&= u(ta+k)+vr(d+ma) && (*)\ \&\ (**) \\
&= u(ta+k)+v(rd+mra) \\
&= u(ta+k)+v(sa-k_1+rma) && (***) \\
&= \underbrace{(ut+vs+vrm)}_{\in\langle a\rangle}a+\underbrace{uk-vk_1}_{\in K} \in \langle a\rangle + K
\end{aligned}
$$

A contradiction. So no such b.

□