HW due Mon Feb 5

Tao Ju

February 3, 2014

Problem 4
Let G be a finite abelian group. Prove that the following are equivalent
1) For every subgroup H of G there is a subgroup K of G with $HK = G$ and $H \cap K = \{e\}$. (Complementation Property)
2) Every element of G has square-free order.

Proof:
Let's prove two easier statements first:

a) $C_p \times C_p \times \cdots \times C_p = nC_p$ has CP where there're n C_p's for $n \in \mathbb{N}^*$ and p prime.

Firstly, it is clear that C_p has CP.
Suppose $\exists n \in \mathbb{N}^*$ s.t. nC_p has CP, let's consider $(n+1)C_p$.
Let H be an arbitrary subgroup of $(n+1)C_p$. If $H = (n+1)C_p$, then take $K = \{e\}$, we've got $HK = (n+1)C_p$ and $H \cap K = \{e\}$. Then assume $H \neq (n+1)C_p$, then $\exists x \in (n+1)C_p$ and $x \notin H$, as a result $x \neq e$. Since every element except e in $(n+1)C_p$ is of order p, $|x| = p$. It is clear that $H \cap \langle x \rangle = \{e\}$. Define the group homomorphism:

$$f : (n+1)C_p \to (n+1)C_p/\langle x \rangle, \quad a \mapsto a^* = a + \langle x \rangle.$$

Since $|(n+1)C_p/\langle x \rangle| = |(n+1)C_p|/|\langle x \rangle| = p^n$ and $|a^*| \leq |a| \leq p$ for every $a^* \in (n+1)C_p/\langle x \rangle$, so $(n+1)C_p/\langle x \rangle$ can be decomposed to

$$(n+1)C_p/\langle x \rangle \cong nC_p,$$

which has CP according to our assumption. Notice that $H^* = f(H)$ is a subgroup of $(n+1)C_p/\langle x \rangle$, so we have another subgroup K^* s.t. $H^*K^* = (n+1)C_p/\langle x \rangle$ and $H^* \cap K^* = \{e^*\}$. Pull back K^* we get $K = f^{-1}(K^*)$ which is a subgroup of $(n+1)C_p$. And it is clear that $H \cap K = \{e\}$ since $H \cap K \subset f^{-1}(H^* \cap K^*) = f^{-1}(e^*) = \langle x \rangle$ and $H \cap \langle x \rangle = \{e\}$.
Consider $f|_H : H \to H^*$, $\forall a \in \ker(f|_H)$, $f(a) = a + \langle x \rangle = \langle x \rangle$, so $a \in \langle x \rangle$, $a = \{e\}$. Thus $f|_H$ is bijection and then $|H| = |H^*|$. We have $|HK| = |H||K| = |H^*||K^*||\langle x \rangle| = |(n+1)C_p/\langle x \rangle||\langle x \rangle| = |(n+1)C_p|$, so $HK = (n+1)C_p$. Therefore, we've shown $(n+1)C_p$ has CP.
By induction, we get our goal that $\forall n \in \mathbb{N}^*$, nC_p has CP.

b) Let $|G|$ and $|H|$ be relatively prime. Prove that if both G and H have CP, then $G \times H$ has CP.

Claim any subgroup of $G \times H$ is of form $R \times S$ where R and S are subgroups of G and H respectively.
Let M be the subgroup of $G \times H$. Let $R = \{g \in G : \exists (g,h) \in M \text{ for some } h \in H\}$, $S = \{h \in H : \exists (g,h) \in M \text{ for some } g \in G\}$, it is clear that $M \subset R \times S$ and R, S are subgroups of G, H respectively.. $\forall r \in R$, $\exists h \in H$ s.t. $(r,h) \in M$. Let $k = |r|$ and $l = |h|$, since $\gcd(|G|, |H|) = 1$, $\gcd(k,l) = 1$, then $\exists s, t \in \mathbb{Z}$ s.t. $sk + tl = 1$. So $(r,h)^{tl} = (r^{1-sk}, h^{tl}) = (r,e) \in M$. Thus $R \times \{e\} \subset M$, similarly, $\{e\} \times S \subset M$. Therefore $R \times S = (R \times \{e\}) \cdot (\{e\} \times S) \subset M$, as to say $M = R \times S$.

Next, prove statement b):
For any subgroup $R \times S$ of $G \times H$ where R, S are subgroups of G, H respectively, since G, H have CP, we can find subgroups P, Q of G, H respectively s.t. $RP = G$, $R \cap P = \{e\}$ and $SQ = H$, $S \cap Q = \{e\}$. Thus $P \times Q$ is a subgroup of $G \times H$ and $(P \times Q) \cap (R \times S) = \{e\}$, $(P \times Q) \cdot (R \times S) = G \times H$, which indicates that $G \times H$ has CP.

Now, let's prove the original problem.
1) $\Rightarrow$ 2):
Let G be a finite abelian group with at least one element whose order isn't square-free, so there is some prime p and element x s.t. $|\langle x \rangle| = p^2$. Suppose G has CP, take $H = \langle x^p \rangle$, there exists a subgroup K of G s.t. $HK = G$ and $H \cap K = \{e\}$. Let $P = K \cap \langle x \rangle$ which is a subgroup of G, then it is clear that $H \cap P = \{e\}$ and $HP = \langle x \rangle$. Then $\exists x^{np} \in H, x^m \in P$ s.t. $x = x^{np} \cdot x^m = x^{np+m}$, so $(m, p^2) = 1$. Thus $\exists \alpha, \beta \in \mathbb{Z}$ s.t. $\alpha m + \beta p^2 = 1$. Then $(x^m)^\alpha = x^{1-\beta p^2} = x \in P$, then $P = \langle x \rangle \supset H$, contradiction.
Therefore G must be square-free if G has CP.

2) $\Rightarrow$ 1):
If G is square-free and $|G| = p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n}$ where $p_1 < p_2 < \cdots < p_n$ are prime, then

$$G \cong i_1 C_{p_1} \times i_2 C_{p_2} \times \cdots \times i_n C_{p_n}.$$

By a), $i_k C_{p_k}$ has CP for all k. Then by b) and induction, we get G has CP.

Till now, we've shown G has CP iff G is square-free.