(黃皜文的解答)

1(d) Let G be a finite abelian group. Show that if G is not cyclic, then G is decomposable. (Hint. $G =< a > \times K$ for some $a \in G$.)

Proof. We proceed by induction on the order of G. Let a be an element of maximal order m in G. Let $A = \langle a \rangle$. Now we prove the following statements.

(i) For $g \in G$, the order of g divides m.

(ii) Show that there exists a nontrivial subgroup C of G such that $A \cap C = \{1\}$.

(iii) Show that $aC \in G/C$ has order m in G/C. Hence aC is an element of maximal order in G/C.

If G/C is cyclic then $G = A \times C$. Otherwise, by induction hypothesis,

$$G/C = \langle aC \rangle \times Q/C$$

for some subgroup $Q < G$ containing C. Then it is routine to check that $G = A \times Q$. □

Proof of (i). Suppose there exists an element $g \in G$ of order n such that $n \not| m$. If $(n, m) = 1$, then the element ga has order nm and it contradicts the maximality of m. Otherwise, there exists a prime p such that $p^s | n$, $p^{s-1} | m$ and $p^s \not| m$ for some s. Let $h := g^{\frac{n}{p^s}}$ and $b := a^{p^{s-1}}$. Note that h and b have orders p^s and $\frac{m}{p^{s-1}}$ respectively. Since $(p^s, \frac{m}{p^{s-1}}) = 1$, the element hb has order pm and we also obtain a contradiction to the maximality of m. The proof completes. □

Proof of (ii). Choose an element c which has the smallest order among those element in $G - A$. Let the order of c be n. Claim that n is a prime. Suppose not. Let p be a prime factor of n. Since the order of c^p is less than n, we have $c^p = a^i \in A$ for some i. Note that p is also a prime factor of m by (i). Hence

$$1 = c^m = (c^p)^{m/p} = (a^i)^{m/p} = a^{im/p}.$$

Since the order of a is m, we have $p|i$. Let $b := a^{-i/p}c$. Then $b^p = a^{-i}c^p = a^{-i}a^i = 1$. Moreover $b \notin A$ since $c \notin A$. This is a contradiction to the choice for c. Thus, n is a prime and this implies that $\langle c \rangle \cap A = \{1\}$. □

Proof of (iii). Let the order of aC be r. It suffices to show that m divides r. Since $a^r \in C \cap A$ and by (ii), $a^r = 1$ and hence $m|r$. □