Direct Sum is Cancelative for Finite Groups

Daniel Kelsall

November 9, 2016

On Problem Sheet 5, Q.3.(b) we proved the following result,

Proposition 1. *If A and B are finite abelian groups with $A \oplus A \cong B \oplus B$, then $A \cong A$.*

However, the proof of Proposition 1 was unsatifactory as it used the Fundamental Theorem of Finite Abelian Groups. Here we give an alternative proof that does not require the Fundamental Theorem and proves the more general result below,

Theorem 2. *If A and B are finite groups with $A \times A \cong B \times B$, then $A \cong B$.*

Before giving a proof of Theorem 2, we begin with two useful properties of group homorphisms.

Lemma 3. *If A, B and G are groups then there exists a bijection*

$$\mathrm{Hom}(G, A \times B) \longleftrightarrow \mathrm{Hom}(G, A) \times \mathrm{Hom}(G, B).$$

Where $\mathrm{Hom}(X, Y)$ *is the collection of homorphisms from X to Y.*

Proof. Observe that we have the following homorphisms

$$\begin{aligned} \pi_A &: A \times B \to A \\ &: (a, b) \mapsto a \end{aligned} \qquad\qquad \begin{aligned} \pi_B &: A \times B \to B \\ &: (a, b) \mapsto b \end{aligned}$$

Now for any map $\phi \in \mathrm{Hom}(G, A \times B)$ we obtain homomorphisms

$$\pi_A \circ \phi : G \to A \qquad\qquad \pi_B \circ \phi : G \to B$$

Converseley, given maps $\psi_A \in \mathrm{Hom}(G, A)$ and $\psi_B \in \mathrm{Hom}(G, B)$, we obtain a homorphism

$$\begin{aligned} \psi &: G \to A \times B \\ &: (a, b) \mapsto (\psi_A(a), \psi_B(b)) \end{aligned}$$

This establishes the desired bijection. $\square$

Lemma 4. *If A and B are groups, then there exists a bijection*

$$\mathrm{Hom}(A, B) \longleftrightarrow \bigsqcup_{N \trianglelefteq A} \mathrm{Mon}(A/N, B).$$

Where $\mathrm{Mon}(A, B)$ *is the collection of all monomorphisms from A to B.*

Proof. It is clear that the union is disjoint. The bijective correspondance is given by the following. For a map $\phi \in \mathrm{Hom}(A, B)$ there exists a monomorphism $\overline{\phi} \in \mathrm{Mon}(A/\ker(\phi), B)$, by the First Isomorphism Theorem.

On the other hand, given a monomorphism $\psi \in \mathrm{Mon}(A/N, B))$, for some $N \trianglelefteq A$, composing with the quotient map $\pi : A \to A/N$ produces a homorphism $\psi \circ \pi \in \mathrm{Hom}(A, B)$. Moreover, since ψ is injective, we have that

$$\ker(\psi \circ \pi) = \ker(\pi) = N.$$

Thus we have established the desired bijection. $\square$

We are now in a position to give the proof of Theorem 2.

Proof of Theorem 2. Let G be a finite group. By Lemma 3 we have that

$$|\operatorname{Hom}(G, A)|^2 = |\operatorname{Hom}(G, A \times A)| = |\operatorname{Hom}(G, B \times B)| = |\operatorname{Hom}(G, B)|^2$$

and hence $|\operatorname{Hom}(G, A)| = |\operatorname{Hom}(G, B)|$.

Next we adopt an induction hypothesis of $|\operatorname{Mon}(G, A)| = |\operatorname{Mon}(G, B)|$ when $|G| < k$ and consider the case $|G| = k$. By Lemma 4 we have that

$$\sum_{N \trianglelefteq G} |\operatorname{Mon}(G/N, A)| = |\operatorname{Hom}(G, A)| = |\operatorname{Hom}(G, B)| = \sum_{N \trianglelefteq G} |\operatorname{Mon}(G/N, B)|.$$

and by our induction hypothesis $|\operatorname{Mon}(G/N, A)| = |\operatorname{Mon}(G/N, B)|$ when $|G/N| < k$, that is when $N \neq \{1\}$. Therefore we have

$$\begin{aligned}
|\operatorname{Mon}(G, A)| &= |\operatorname{Hom}(G, A)| - \sum_{\{1\} \neq N \trianglelefteq G} |\operatorname{Mon}(G/N, A)| \\
&= |\operatorname{Hom}(G, B)| - \sum_{\{1\} \neq N \trianglelefteq G} |\operatorname{Mon}(G/N, B)| \\
&= |\operatorname{Mon}(G, B)|
\end{aligned}$$

proving our induction hypothesis to be true.

Now taking $G = A$, yields that $|\operatorname{Mon}(A, A)| = |\operatorname{Mon}(A, B)|$, moreover we have that $|\operatorname{Mon}(A, A)| \geq 1$ since it contains the identity map. Thus there exists a monomorphism from A to B. Similarly, taking $G = B$ shows that there exists a monomorphism from B to A.

Thus, by the First Isomorphism Theorem, A is isomorphic to a subgroup of B. Similarly, B is isomorphic to a subgroup of A. Hence $A \cong B$, as desired. □