Cancellation in Direct Products of Finite Groups

Theorem 1. *Let $A, B,$ and C be finite groups. If*

$$A \times B \cong A \times C,$$

then $B \cong C$.

Proof. For finite groups X and Y, let

$$h(X, Y)$$

denote the number of group homomorphisms from X to Y, and let

$$m(X, Y)$$

denote the number of injective homomorphisms (monomorphisms) from X to Y.

Step 1: Equality of homomorphism counts.

Let D be any finite group. A homomorphism

$$\varphi : D \to A \times B$$

is uniquely determined by its coordinate maps

$$\varphi_A : D \to A, \qquad \varphi_B : D \to B,$$

and conversely any pair of homomorphisms (φ_A, φ_B) determines a homomorphism $D \to A \times B$. Therefore,

$$h(D, A \times B) = h(D, A)\, h(D, B).$$

Similarly,

$$h(D, A \times C) = h(D, A)\, h(D, C).$$

Since $A \times B \cong A \times C$, we have

$$h(D, A \times B) = h(D, A \times C),$$

and hence

$$h(D, A)\, h(D, B) = h(D, A)\, h(D, C).$$

Because $h(D, A) \geq 1$ (the trivial homomorphism always exists), it follows that

$$h(D, B) = h(D, C)$$

for every finite group D.

Step 2: Equality of monomorphism counts.

We prove that

$$m(D, B) = m(D, C)$$

for every finite group D, by induction on $|D|$.

Base case. If $|D| = 1$, then there is exactly one homomorphism from D to any group, and it is injective. Thus

$$m(D, B) = 1 = m(D, C).$$

Inductive step. Assume the statement holds for all groups of order strictly less than n, and let D be a group of order n.

By Lemma 1 below,

$$h(D, B) = m(D, B) + \sum_{K} m(D/K, B),$$

and

$$h(D, C) = m(D, C) + \sum_{K} m(D/K, C),$$

where the sums are taken over all nontrivial normal subgroups $K \triangleleft D$.

From Step 1 we know

$$h(D, B) = h(D, C),$$

and by the induction hypothesis,

$$m(D/K, B) = m(D/K, C)$$

for every nontrivial normal subgroup K, since $|D/K| < |D|$.

Therefore,

$$m(D, B) = m(D, C).$$

This completes the induction.

Step 3: Conclusion.

Taking $D = B$ and $D = C$ gives

$$m(B, C) = m(B, B) \geq 1, \qquad m(C, B) = m(C, C) \geq 1.$$

Thus there exist injective homomorphisms

$$B \hookrightarrow C \quad \text{and} \quad C \hookrightarrow B.$$

Since B and C are finite, the existence of mutual injections implies

$$|B| \leq |C| \quad \text{and} \quad |C| \leq |B|,$$

so $|B| = |C|$. An injective homomorphism between finite groups of equal order is bijective, hence an isomorphism. Therefore

$$B \cong C.$$

□

Lemma 1. *Let D and B be finite groups. Then*

$$h(D, B) = m(D, B) + \sum_{K} m(D/K, B),$$

where the sum is taken over all nontrivial normal subgroups $K \triangleleft D$.

Proof. Let $f : D \to B$ be a homomorphism. Either:

- f is injective, contributing to $m(D, B)$, or
- $\ker f = K$ is a nontrivial normal subgroup of D.

In the second case, f factors uniquely through the quotient map $\pi : D \to D/K$, giving a homomorphism

$$g : D/K \to B$$

such that

$$f = g \circ \pi.$$

The kernel of g is trivial, so g is injective.

Conversely, if $g : D/K \to B$ is injective, then

$$f(x) = g(xK)$$

defines a homomorphism $f : D \to B$ with kernel K.

Thus there is a bijection between homomorphisms $f : D \to B$ with kernel K and monomorphisms $g : D/K \to B$.

Summing over all nontrivial normal subgroups K and including the injective homomorphisms gives the stated formula. □