Example of the 2nd Iso Thm

The 2nd Iso Thm is very useful to group theorists but is somewhat notorious for being hard to motivate.

Here is one interesting application.

Example let $n, m$ be two integers. Then

$$\gcd(n, m) \cdot \text{lcm}(n, m) = nm$$

**Proof:**

Consider the subgroups $n\mathbb{Z}$ and $m\mathbb{Z}$ of $\mathbb{Z}$. (abstractly, assume.)

We have

$$n\mathbb{Z} + m\mathbb{Z} = \gcd(n, m)\mathbb{Z} \quad \text{? check!}$$

$$n\mathbb{Z} \cap m\mathbb{Z} = \text{lcm}(n, m)\mathbb{Z}$$

$$\langle n\mathbb{Z} \rangle + \langle m\mathbb{Z} \rangle = \langle \gcd(n, m)\mathbb{Z} \rangle$$

$$n\mathbb{Z} \cap m\mathbb{Z} = \langle \text{lcm}(n, m)\mathbb{Z} \rangle$$
so \( \gcd(n, m)^2 = n^2 \frac{2}{\text{can}(n, m)^2} \)

In particular,
\[
\left| \frac{\gcd(n, m)^2}{m^2} \right| = \left| \frac{n^2}{\text{can}(n, m)^2} \right|
\]

\[
\frac{m}{\gcd(n, m)}
\]

(\text{check: if } d \ln \left| \frac{dZ}{\sqrt{Z}} \right| = \frac{n}{2} \)

So \( \gcd(n, m) \text{can}(n, m) = nm \)

\text{Cauchy's Theorem}

Our goal is the following.

Then (Cauchy, 1845)

let \( G \) be a group with \(|G| < \infty \) and \( p \) be a prime. Then \( G \) contains an
element of order $p$.

Let's first do the abelian case.

**Proof**

Let $G$ be a finite abelian group with $p | |G|$. Then $G$ contains an element of order $p$.

**Proof**

We have $|G| = pm$, $m \geq 1$.

If $m = 1$ then $G$ is cyclic, $G = \langle x \rangle$

close $x$ has order $p$.

We now prove the result by induction on $m$.

Let $x \neq 1 \in G$. Let $n = |x|$. If $p | n$ then $x^{\frac{n}{p}}$ has order $p$.

(Pf: obviously $x^{\frac{n}{p}} \cdot p = 1 \Rightarrow \frac{n}{p} | |G| \Rightarrow p | |G|$)

But $p$ is prime!)

div alg: $r \leq |x^{\frac{n}{p}}| + 1$
So in this case we are done.

Now assume $n=|x|$ does not divide $p$.

$G$ abelian $\Rightarrow$ all subgroups are normal, so consider $G/<x>$

$|G/<x>| = |G|/|n| = \frac{p^m}{n} = p \binom{m}{n}$

Since $n \nmid p$, $n | m$ and $\frac{m}{n} < m$.

"**Induction Hypothesis**: Assume claim holds for all finite groups of order $p^n$, $s.t. \frac{m}{n} < m$.

So by induction the claim holds for $G/<x>$, i.e. $3 \exists y \in G/<x>$, $|y| = p$.

The quotient hom $\phi: G \rightarrow G/<x>$ is

Surjective, let $\phi(y) = \bar{y}$ (i.e. $\bar{y} = y<x>$)
What's the order of \( y \)?

\[ \phi(y^p) = \phi(\chi)^p = 0 \] so \( y^p \in \ker \phi \) i.e. \( y^p \in \langle x \rangle \).

\[ y^p \in \langle x \rangle. \]

On the other hand \( y \notin \langle x \rangle \) (or else \( y = 1 \)).

This means \( \langle y^p \rangle \) and \( \langle y \rangle \) must be different groups (the first is contained in \( \langle x \rangle \) while the 2nd is not).

i.e. \( \langle y^p \rangle \neq \langle y \rangle \)

**Fact** (will prove in a minute)

\[ |y^p| = \frac{|y|}{\gcd(|y|, p)} \]

If \( |y| < p \) then we would have \( |y| < p \) \( y \) so we must have \( \gcd(|y|, p) = p \)

\[ \Rightarrow p \mid |y| \text{ by above. But we} \]
already know how to construct elements of order $p$ when this happens ($\frac{\text{ord} X}{\text{gcd}(\text{ord} X, n)}$ when such an elt $D$.

It remains to prove the fact.

Prop (Prop 5.1 pg 57 De F)

Let $X$ be an element of finite order in a group.

Then $|x^n| = \frac{|x|}{\text{gcd}(|x|, n)}$

Proof.

Set $n = |x|$ and $d = \text{gcd}(|x|, n)$ and write

$n = db$, $a = dc$, $b_1 c e \in G$ with $b > 0$.

As $d$ is the gcd of $n$ and $a$, $\gcd(b_1 c e) = 1$ (or else would have bigger divisor). Set $y = x^n$. 
\[ y^b = x^a = x = (x^b)^c = (x^c)^b = 1 \]

\[ \Rightarrow \ l y l \ \text{divides} \ b \quad (\text{by div. alg.}) \]

Next \[ X^a l y l \ (\approx y^b) = 1 \]

\[ \Rightarrow \ n = |x| l a l y l \ i.e. \ dB \mid DC [y] \]

\[ \Rightarrow b \mid c [y] . \ A s \ \gcd(b, c) = 1 \]

\[ \Rightarrow b \mid [y] \Rightarrow b = |y| = |y| \ \text{divide} \ b \]

Which is what we wanted to prove.

The main technique we need is

The Class Equation

Recall G acting on itself: \( g h g^{-1} = g \cdot h \) Conjugation

Orbits under conjugation are called Conjugacy classes.

Generalization \( \mathcal{P}(G) := \Sigma \) Set of Subsets \( S \subseteq G \)

Have conjugation action of \( G \) on \( \mathcal{P}(G) \):
\[ g \cdot S := g \cdot g^{-1} S = \{ g \cdot g^{-1} s \mid s \in S \} \]

By the orbit-stabilizer theorem, the number of orbits (conjugacy classes) under this action is
\[
\left[ G : G_{S} \right] = \left[ G : N_{G}(S) \right]
\]

Stabilizer
\[ \text{Stabilizer} \]
\[ N_{G}(S) = \{ g \in G \mid g \cdot S = S \} \]

If \( s \in G \) is an element
\[ N_{G}(S) = C_{G}(S) = \{ g \in G \mid g \cdot s = S \} \]

Centralizer

We define
\[ \text{the centre} \quad Z(G) := \{ g \in G \mid \forall f \in G, \quad fgf^{-1} = g \} \]

Note that each element in the centre forms its own conjugacy class, as \( g^{-1}fg = S \cdot S \cdot g \cdot S \).
The Class Equation

Assume $|G| < \infty$, let $\Gamma$ be the number of conjugacy classes not contained in the center. Let $g_1, \ldots, g_r$ be representatives for each of these orbits.

Then

$$|G| = |\mathbb{Z}(G)| + \sum_{\iota = 1}^{r} \left[ G : C_G(g_i) \right]$$

**Proof**

Let $\Theta_1, \ldots, \Theta_r$ be the orbits corresponding to $g_1, \ldots, g_r$.

Thus $\mathbb{Z}(G) \cup \Theta_1 \cup \cdots \cup \Theta_r$ gives a partition of $G$.

$$|G| = |\mathbb{Z}(G)| + \sum_{\iota = 1}^{r} |\Theta_{\iota}|$$

$$= (|\mathbb{Z}(G)| \times \sum_{\iota = 1}^{r} \left[ G : C_G(g_i) \right])$$

by the orbit-stabilizer theorem as above.

$\square$