Exs: Invariant factor decomp $\longrightarrow$ Elem. div. decomp.

1) $G = \mathbb{Z}_{36} \times \mathbb{Z}_{12} \times \mathbb{Z}_3$

Scratch: $36^2 = 2^4 \cdot 3^4$,

Want to write

$G = G_1 \times G_2$, $|G_1| = 2^4$, $|G_2| = 3^4$,

then further decompose

G_1, G_2 into products

of cyclic groups.

$\cong (\mathbb{Z}_4 \times \mathbb{Z}_9) \times (\mathbb{Z}_4 \times \mathbb{Z}_3) \times \mathbb{Z}_3$

$\cong \underbrace{(\mathbb{Z}_4 \times \mathbb{Z}_4)}_{G_1} \times \underbrace{(\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3)}_{G_2}$

Note: If $m, n \in \mathbb{N}$, $(m,n) = 1$,

then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

2) General case is similar...

Elem. div. decomp. $\longrightarrow$ Invariant factor decomp

1) $\mathbb{Z}_{256} \times (\mathbb{Z}_{81} \times \mathbb{Z}_{27} \times \mathbb{Z}_3) \times (\mathbb{Z}_{25} \times \mathbb{Z}_5)$

$\cong \underbrace{\mathbb{Z}_{2^8 3^4 5^2}}_{``n_1"} \times \underbrace{\mathbb{Z}_{3^3 5^1}}_{``n_2"} \times \underbrace{\mathbb{Z}_{3^1}}_{``n_3"}$

2) General case is similar...

It follows from these examples that the two versions of the FTFGAG are equiv. to each other.

We'll prove (the finite version of) the elementary divisor decomp:

Thm (FTFGAG, Elementary divisor decomposition):

If G is an Abelian gp., $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k} < \infty$, $p_1 < p_2 < \cdots < p_k$ distinct primes, $\alpha_1, \dots, \alpha_k \in \mathbb{N}$. Then:

i) $G \cong G_1 \times \cdots \times G_k$, with $|G_i| = p_i^{\alpha_i}$.

ii) $\forall 1 \le i \le k$, $\exists\, t_i \ge 1$, $\beta_{i1} \ge \beta_{i2} \ge \cdots \ge \beta_{it_i} \ge 1$, s.t.

$$G_i \cong \mathbb{Z}_{p_i^{\beta_{i1}}} \times \mathbb{Z}_{p_i^{\beta_{i2}}} \times \cdots \times \mathbb{Z}_{p_i^{\beta_{it_i}}}.$$

iii) This decomp. is unique.

Something we will use in the proof.

Thm (Cauchy's theorem): If G is a finite group, p is a prime, and $p \mid |G|$, then G contains an element of order p.

Pf: (due to James MacKay):

Let $S = \{(g_1, \dots, g_p) : g_1, \dots, g_p \in G,\ g_1 \cdots g_p = e\}$.

Define $\sim$ on S as follows:

$x \sim y$ iff x and y are cyclic permutations of each other

i.e: $(g_1, \dots, g_p) \sim (g_2, \dots, g_p, g_1) \sim \cdots \sim (g_p, g_1, \dots, g_{p-1})$

This is an equiv. rel.

Calculate $|S|$ in 2 ways.

- There are 2 types of equiv. classes. Classes with 1 element (e.g. $(e, \dots, e)$), and classes with p different elements. So:

$$|S| = 1 \cdot \underbrace{\#\{\text{of equiv. classes w/ one elem.}\}}_{=k} + p \cdot \underbrace{\#\{\text{equiv. classes w/ } p \text{ elems.}\}}_{=l}$$

$= k + pl$. (note $k \geq 1$).

- $S = \{(g_1, \ldots, g_p) : g_1, \ldots, g_p \in G,\ g_1 \cdots g_p = e\}$.

$= \{(g_1, \ldots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}) : g_1, \ldots, g_{p-1} \in G\}$

$\Rightarrow |S| = |G|^{p-1} = p^{p-1} \cdot m$ $\quad (p \mid |G|)$

Compare the formulas:

$$k + pl = p^{p-1} m \Rightarrow p \mid k \Rightarrow k > 1$$

$$\Rightarrow \exists g \in G \setminus \{e\} \text{ s.t. } g^p = e \Rightarrow |g| = p. \ \boxtimes$$

Pf. of part i of FTFGAG (elem. div. decomp.):

$|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $p_1 < \cdots < p_k$ primes, $\alpha_i \in \mathbb{N}$,

Want to show that $G \cong G_1 \times \cdots \times G_k$, $|G_i| = p_i^{\alpha_i}$.

Pf: First let's show that $\forall\, 1 \le i \le k$, G has a unique subgroup G_i of order $p_i^{\alpha_i}$.

Assuming we can do this:

$$\forall\, 1 \le i < j \le k, \qquad G_i \cap G_j \le G_i, G_j$$

$$\Rightarrow |G_i \cap G_j| \mid p_i^{\alpha_i}, p_j^{\alpha_j}$$

$$\Rightarrow G_i \cap G_j = \{e\}$$

Then, by our discussion of internal direct products:

$$\left.\begin{array}{l} \bullet\ |G_1 \cdots G_k| = |G_1| \cdots |G_k| = |G| \\ \bullet\ G_1 \cdots G_k \cong G_1 \times \cdots \times G_k \end{array}\right\} \Rightarrow G \cong G_1 \times \cdots \times G_k.$$

Let $G_i = \{g \in G : |g| \mid p_i^{\alpha_i}\}$.

- G_i is a group: $e \in G_i \Rightarrow G_i \neq \emptyset$ ✓

  Suppose $g, h \in G_i$. Then $|h^{-1}| = |h| \mid p_i^{\alpha_i}$

  $\Rightarrow |gh^{-1}| \mid \operatorname{lcm}(|g|, |h^{-1}|) \mid p_i^{\alpha_i}$

  $\Rightarrow gh^{-1} \in G_i$. (G is Abelian)

- $|G_i| = p_i^{a_i}$ for some $0 \le a_i \le \alpha_i$.

  By Lag's thm. $|G_i| \mid |G|$

  $\Rightarrow |G_i| = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, $0 \le a_i \le \alpha_i$

  If $j \neq i$ but $a_j > 0$ then $p_j \mid |G_i|$

  $\Rightarrow G_i$ has an elem. of order p_j,

  but this contradicts the def of G_i.

- Can't have $|G_i| = p_i^{a_i}$ for $a_i < \alpha_i$.

  If it were, consider $\overline{G_i} = G/G_i$.

  Then $|\overline{G_i}| = \dfrac{|G|}{|G_i|} \Rightarrow p_i \mid |\overline{G}_i|$

  $\Rightarrow \overline{G_i}$ has an elem. of order p_i,

  call it gG_i.

  Now $(gG_i)^{p_i} = G_i \Rightarrow p_i \mid |g| \Rightarrow |g| = p_i^j q$,

  where $j \ge 1$, $p_i \nmid q$.

Then $|g^q| = \dfrac{|g|}{\gcd(|g|, q)} = p_i^j$

$\Rightarrow g^q \in G_i$, by def.

$\Rightarrow |gG_i| \mid q \Rightarrow p_i \nmid |gG_i|$, contr..

Conclusion: $|G_i| = p_i^{r_i}$. $\blacksquare$

(uniqueness follows easily from the def. of G_i)