L25: Existence of Invariant factor decomposition

Existence proof v2

As before we have $A \cong \mathbb{Z}^N / E \qquad E \leq \mathbb{Z}^N$. ($\gcd(M_{ij})$ from before)

Induction on N. $N = 0 : \checkmark$. $N > 0$.

We set $a := \min \{ \sum \lambda_i e_i \mid (e_1, \dots, e_N) \in E, (\lambda_1, \dots, \lambda_N) \in \mathbb{Z}^N \} \cap \mathbb{N}^{>0}$

If no such min exists we are done ($A \cong \mathbb{Z}^N$)

Let the min be achieved by $e = (e_1, \dots, e_N)$

Claim $\exists\, U \in \mathrm{Mat}_{N \times N}(\mathbb{Z})$ st. $U^{-1} \in \mathrm{Mat}_{N \times N}(\mathbb{Z})$ and

$U \begin{pmatrix} e_1 \\ \vdots \\ e_N \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ for some integer d $\qquad (= \gcd(e_1, \dots, e_N))$

Pf Exactly as in Euclidean algorithm $\square$ claim

Claim Using U as base change we can assume $e = (d, 0, \dots, 0)$

(while keeping a, in part $a = d$)

Pf bookkeeping & $\sum \lambda_i e_i = (\lambda_1, \dots, \lambda_N) \begin{pmatrix} e_1 \\ \vdots \\ e_N \end{pmatrix} = (\lambda_1, \dots, \lambda_N) U^{-1} U \begin{pmatrix} e_1 \\ \vdots \\ e_N \end{pmatrix}$ $\square$ claim

Note that for any $f = (f_1, \dots, f_N) \in E$ we have $d \mid f_1$. Otherwise $(d, f_1) < d$,

but $(d, f_1) = ad + bf_1$ for $a, b \in \mathbb{Z}$ $\qquad (\ast)$

$$= (ae + bf)_1 = \sum \lambda_i \underbrace{(ae + bf)_i}_{\in E} \quad \text{for } (\lambda_1, \dots, \lambda_N) = (1, 0, \dots, 0).$$

Claim $\quad E = d\mathbb{Z} \oplus (\{0\} \times \mathbb{Z}^{N-1} \cap E)$

Pf $\supseteq : \checkmark$

$\subseteq : \; f \in E : \quad f = \underbrace{\frac{f_1}{d}}_{\in \mathbb{Z}} \underbrace{(d, 0, \dots, 0)}_{\in E} + \underbrace{(0, f_2, \dots, f_N)}_{\in E}$ $\; \Rightarrow$ $\qquad \square$ claim

Claim $\quad \varphi : \mathbb{Z}^N / E \to \mathbb{Z}/d\mathbb{Z} \times \underbrace{\frac{\{0\} \times \mathbb{Z}^{N-1}}{\{0\} \times \mathbb{Z}^{N-1} \cap E}}_{A'}$

$(f_1, \dots, f_N) \mapsto (\bar{f}_1, [(f_2, f_3, \dots, f_N)])$

is a group isom.

Pf We start with $\tilde{\varphi} : \mathbb{Z}^N \to \mathbb{Z}/d\mathbb{Z} \times A'$ and show that $E = \ker \tilde{\varphi}$.

But $\ker \tilde{\varphi} = d\mathbb{Z} \oplus \{0\} \times \mathbb{Z}^{N-1} \cap E$ thus it follows from previous claim. $\square$ claim

We conclude using the induction hypothesis on A' that

$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^{N-k}$

A similar argument to $(\ast)$ shows $d_1 \mid d_2 \mid \dots \mid d_k$ (or use chinese remainder theorem to reassemble). $\square$ Proof