This implies that M_{tor} is the direct sum of modules of the form $A/p_i^{n_{i,j}}$, for some primes $p_i \in A$.

To prove uniqueness, observe that the p_i-primary component of M_{tor} is the direct sum

$$(A/p_i^{n_{i,1}}A)^{m_{i,1}} \oplus \cdots \oplus (A/p_i^{n_{i,s_i}}A)^{m_{i,s_i}},$$

and these are uniquely determined. Since $n_{i,1} < \cdots < n_{i,s_i}$, we have

$$p_i^{n_{i,s_i}}A \subseteq \cdots \subseteq p_i^{n_{i,1}}A \neq A,$$

Proposition 35.30 implies that the irreducible elements p_i and $n_{i,j}$, s_i, and $m_{i,j}$ are unique. □

In view of Theorem 35.38, we make the following definition.

Definition 35.13. Given a finitely generated module M over a PID A as in Theorem 35.38, the ideals $p_i^{n_{i,j}}A$ are called the *elementary divisors* of M, and the $m_{i,j}$ are their *multiplicities*. The ideal (0) is also considered to be an elementary divisor and r is its multiplicity.

Remark: Theorem 35.38 shows how the elementary divisors are obtained from the invariant factors: the elementary divisors are the prime power factors of the invariant factors.

Conversely, we can get the invariant factors from the elementary divisors. We may assume that M is a torsion module. Let

$$m = \max_{1 \leq i \leq t}\{m_{i,1} + \cdots + m_{i,s_i}\},$$

and construct the $t \times m$ matrix $C = (c_{ij})$ whose ith row is the sequence

$$\underbrace{n_{i,s_i}, \ldots, n_{i,s_i}}_{m_{i,s_i}}, \ldots, \underbrace{n_{i,2}, \ldots, n_{i,2}}_{m_{i,2}}, \underbrace{n_{i,1}, \ldots, n_{i,1}}_{m_{i,1}}, 0, \ldots, 0,$$

padded with 0's if necessary to make it of length m. Then, the jth invariant factor is

$$\alpha_j A = p_1^{c_{1j}} p_2^{c_{2j}} \cdots p_t^{c_{tj}} A.$$

Observe that because the last column contains at least one prime, the α_i are not units, and $\alpha_m \mid \alpha_{m-1} \mid \cdots \mid \alpha_1$, so that $\alpha_1 A \subseteq \cdots \subseteq \alpha_{m-1}A \subseteq \alpha_m A \neq A$, as desired.

From a computational point of view, finding the elementary divisors is usually practically impossible, because it requires factoring. For example, if $A = K[X]$ where K is a field, such as $K = \mathbb{R}$ or $K = \mathbb{C}$, factoring amounts to finding the roots of a polynomial, but by Galois theory, in general, this is not algorithmically doable. On the other hand, the invariant factors can be computed using elementary row and column operations.

It can also be shown that A and the modules of the form $A/p^n A$ are indecomposable (with $n > 0$). A module M is said to be *indecomposable* if M cannot be written as a direct