2.22 Proof of the Chinese remainder theorem

Theorem 2.28. *(Chinese remainder theorem) Let $\mathbb{A}$ be a PID and let $d \in \mathbb{A}$.*

$$\textit{Assume} \qquad d = pq \qquad \textit{with} \qquad \gcd(p,q) = 1.$$

Then there exist $r, s \in A$ such that $1 = pr + qs$ and

$$\begin{array}{ccc} \dfrac{\mathbb{A}}{d\mathbb{A}} & \stackrel{\sim}{\longrightarrow} & \dfrac{\mathbb{A}}{p\mathbb{A}} \oplus \dfrac{\mathbb{A}}{q\mathbb{A}} \\ pr + pq\mathbb{A} & \mapsto & (0 + p\mathbb{A}, 1 + q\mathbb{A}) \\ qs + pq\mathbb{A} & \mapsto & (1 + p\mathbb{A}, 0 + q\mathbb{A}) \\ 1 + pq\mathbb{A} & \mapsto & (1 + p\mathbb{A}, 1 + q\mathbb{A}) \end{array} \qquad \textit{is an } \mathbb{A}\textit{-module isomorphism.}$$

Proof. Let $r, s \in \mathbb{A}$ such that $pr + sq = 1$. Then

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & pq \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -qs & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ qs & pq \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -qs & 1 \end{pmatrix} \begin{pmatrix} pr + qs & 0 \\ qs & pq \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -qs & 1 \end{pmatrix} \begin{pmatrix} p & q \\ 0 & q \end{pmatrix} \begin{pmatrix} r & -q \\ s & p \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -qs & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix} \begin{pmatrix} r & -q \\ s & p \end{pmatrix} \\ &= P \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix} Q, \qquad \text{where} \quad P = \begin{pmatrix} 1 & 1 \\ -qs & 1 - qs \end{pmatrix} \quad \text{and} \quad Q = \begin{pmatrix} r & -q \\ s & p \end{pmatrix}. \end{aligned}$$

The $\mathbb{A}$-module $\frac{\mathbb{A}}{d\mathbb{A}}$ is given by generators m_1, m_2 with relations $1 \cdot m_1 = 0$ and $dm_2 = 0$. Then let

$$b_1 = rm_1 - qm_2, \qquad b_2 = sm_1 + pm_2 \qquad \text{so that} \qquad m_1 = pb_1 + qb_2, \qquad m_2 = -sm_1 + rm_2.$$

Then

$$pb_1 = prm_1 - pqm_2 = 0 - dm_2 = 0 \qquad \text{and} \qquad qb_2 = -qsm_1 + qpm_2 = 0 + dm_2 = 0$$

so that b_1, b_2 are generators of the module $\frac{\mathbb{A}}{p\mathbb{A}} \oplus \frac{\mathbb{A}}{q\mathbb{A}}$. Thus

$$\frac{\mathbb{A}}{p\mathbb{A}} \oplus \frac{\mathbb{A}}{q\mathbb{A}} \cong \frac{\mathbb{A}}{1 \cdot \mathbb{A}} \oplus \frac{\mathbb{A}}{pq\mathbb{A}} = 0 \oplus \frac{\mathbb{A}}{pq\mathbb{A}} = \frac{\mathbb{A}}{pq\mathbb{A}}.$$

□