théorème. *Soit A un anneau principal, $a_1, ..., a_r \in A$ non-nuls non-inversible avec $r \geq 2$ et on pose $a = a_1...a_r$, $b_i = \frac{a}{a_i}$. Si les $a_1, ..., a_r$ sont premiers entre eux, alors*

$$\begin{array}{rccl} \overline{\phi} & : & A/\langle a_1, ..., a_r\rangle & \rightarrow & A/\langle a_1\rangle \times ... \times A/\langle a_1\rangle \\ & & x \ mod \ a & \rightarrow & (x \ mod \ a_1, ..., x \ mod \ a_r) \end{array}$$

est un isomoprhisme d'anneaux. De plus il existe $u_1, ..., u_r \in A$ tels que $\sum_{i=1}^r u_i b_i = 1$,

$$\overline{\phi}^{-1}(x_1 \ mod \ a_1, ..., x_r \ mod \ a_r) = \sum_{i=1}^r x_i u_i b_i \ mod \ a$$

Démonstration. *Soit*

$$\begin{array}{rccl} \phi & : & A & \rightarrow & A/\langle a_1\rangle \times ... \times A/\langle a_1\rangle \\ & & x & \rightarrow & (x \ mod \ a_1, ..., x \ mod \ a_r) \end{array}$$

ϕ st un morphisme d'anneaux car les projections $x \rightarrow x \ mod \ a_i$ le sont.
$Ker(\phi) = \{x \in A |\ \forall i \in \{1, ..., r\},\ x = 0 \ mod \ a_i\} = \cap_{i=1}^r a_i A = ppcm(a_1, ..., a_r)A$. Or les A_i sont premiers entre eux donc $ppcm(a_1, ...a_r) = a$. Donc d'après le premier théorème d'isomorphisme, $\overline{\phi}$ est bien définit et injectif. Voyons qu'il est surjectif.

Soit $(x_1 \ mod \ a_1, ..., x_r \ mod \ a_r) \in A/\langle a_1\rangle \times ... \times A/\langle a_1\rangle$. Voyons que les éléments $b_1, ..., b_r$ sont premiers ente eux dans leur ensemble. En effet supposons par l'absurde que ce ne soit pas le cas, alors il existe $p \in A$ premier tel que $\forall i \in \{1, ..., r\},\ p|b_i$ donc en particulier $p|a_2...a_r$. D'après le lemme d'Euclide il existe a_{i_0} tel que $p|a_{i_0}$ Or $p|b_{i_0}$ donc par le même argument il existe $a_{i_1} \neq a_{i_0}$ tel que $p|a_{i_1}$ et donc $p|pgcd(a_{i_0}, a_{i_1}) = 1$ donc p est inverible, contradiction.

Ainsi d'après le théorème de Bézout il existe $u_1, ..., u_r$ tel que $\sum_{i=1}^r u_i b_i = 1$. Soit $x = \sum_{i=1}^r u_i b_i x_i$. Pour tout $i \neq j$ $a_i|b_j$ donc $u_i b_i x_i = 0 \ mod \ a_j$ et $u_i b_i = 0 \ mod \ a_j$ donc

$$1 = \sum_{i=1}^r u_i b_i = u_j b_j \ mod \ a_j$$

$$\sum_{i=1}^r u_i b_i x_i = u_j b_j x_j \ mod \ a_j$$

$$x = x_j \ mod \ a_j$$

Finalement $\overline{\phi}(x \ mod \ a) = \phi(x) = (x_1 \ mod \ a_1, ..., x_r \ mod \ a_r)$

Application. *Cherchons $P \in \mathbb{Z}/5\mathbb{Z}[X]$ de degré minimal tel que $P(0) = 2,\ P(1) = 0,\ P(2) = 1$. Cela revient à résoudre*

$$\left\{ \begin{array}{ll} P = 2 & mod \ X - 0 \\ P = 0 & mod \ X - 1 \\ P = 1 & mod \ X - 2 \end{array} \right.$$

$\mathbb{Z}/5\mathbb{Z}[X]$ étant principal, et $X,\ X-1,\ X-2$ étant premier entre eux et non-nuls, non-inversibles. Il existe une solution de la forme $P = 2U_0(X-1)(X-2) + 0U_1X(X-2) + 1U_2X(X-1)$. Or $P = 2 \ mod \ X$ donc $2U_02 = 2 \ mod \ X$, $U_0 = 3 \ mod \ X$. De même $P = 1 \ mod \ X - 2$ donc $1 = U_2X(X-1) \ mod \ X - 2$. Or $X(X-1) = (X+1)(X-2)+2$ donc $X(X-1) = 2 \ mod \ X-2$, $1 = 2U_2 \ mod \ X-2$, et donc $U_2 = 3 \ mod \ X-2$. Pour $U_0 = U_2 = 3$, $P = (X-1)(X-2) + 3X(X-1)$ est bien solution du système. Les autre solutions sont de la forme $P + \alpha X(X-1)(X-2), \alpha \in \mathbb{Z}/5\mathbb{Z}[X]$ et donc sont de degré > 2, P est bien la solution degré minimale.

Application. *Résolvons dans $\mathbb{Z}$*

$$\left\{ \begin{array}{ll} k = 2 & mod \ 4 \\ k = 3 & mod \ 5 \\ k = 1 & mod \ 9 \end{array} \right.$$

Commencons par expliciter la relation de Bézout pour 4×5, 4×9 et 5×9. $pgcd(20, 36) = 4 = 36\times(-1)+20\times2$. $pgcd(20, 36, 45) = pgcd(4, 45) = 1 = 45 \times 1 + 4 \times (-11)$ donc $1 = 45 \times 1 + 36 \times 11 + 20 \times (-22)$. Soit $k_0 = 45+36\times11\times3-20\times22\times1 = 838$, d'après le théorème Chinois, en remarquant $838 = 118 \ mod \ 4\times5\times9 = 180$ les solution sont $118 + 180\mathbb{Z}$

théorème. *Soit f un endomorphisme de E, $P = p_1...p_r \in \mathbb{K}[X]$ avec $P_1, ..., P_r$ premiers entre eux. Alors $ker\ P(f) = \bigoplus_{i=1}^{r} ker\ P_i(f)$*

Démonstration. *Par récurrence sur $r \geq 2$. Soit $P = P_1P_2$ avec $pgcd(P_1, P_2) = 1$. Alors par le théorème de Bézout, il existe U et V dans $\mathbb{K}[X]$ tel que $UP_1 + VP_2 = 1$. Montrons que $ker\ P(f) = ker\ P_1(f) \oplus ker\ P_2(f)$. Soit $x \in ker\ P_1(f) \cap ker\ P_2(f)$. Par la relation de Bézout $(UP_1 + VP_2)(f)(x) = x$.*
Donc $x = U(f)(x) \circ P_1(f)(x) + V(f)(x) \circ P_2(f)(x) = 0$. Soit $x \in ker\ P(f)$. $(UP_1 + VP_2)(f)(x) = x$. Voyon que $UP_1(f)(x) \in ker\ P_2(f)$. $P_2(f)(UP_1(f)(x)) = P_2UP_1(f)(x)$. Ce sont des polynomes en f donc ils commutent. Ainsi $P_2(f)(UP_1(f)(x)) = UP_1P_2(f)(x) = UP(f)(x) = 0$. Par le même argument $VP_2(f)(x) \in ker\ P_1(f)$. Ainsi $x = UP_1(f)(x) + Vp_2(f)(x) \in ker\ P_1(f) + ker\ P_2(f)$ d'où la somme directe.

On suppose qu'il existe $r \geq 2$ tel que pour tout polynome $P = P_1...P_r \in \mathbb{K}[X]$ avec $P_1, ..., P_r$ premiers entre eux, $ker\ P(f) = \bigoplus_{i=1}^{r} ker\ P_i(f)$. Soit $Q = Q_1...Q_{r+1} \in \mathbb{K}[x]$ avec $Q_1, ..., Q_{r+1}$ premiers entre eux. En particulier $Q' = Q_1...Q_r$ et Q_{r+1} sont premier entre eux. Donc par le cas $r = 2$ $ker\ Q(f) = ker\ Q'(f) \oplus ker\ Q_{r+1}(f)$ puis par hypothèse de récurrence $ker\ Q(f) \bigoplus_{i=1}^{r} ker\ Q_i(f) \oplus ker\ Q_{r+1}(f) = \bigoplus_{i=1}^{r+1} ker\ P_i(f)$

Application. *Soit f un endomorphisme de E $P = P_1...P_r \in \mathbb{K}[X]$ avec $P_1, ..., P_k$ deux à deux premiers entre eux. Alors pour tout $i \in \{1, ..., \}$, la projection de $ker\ P(f)$ sur $ker\ P_i(f)$ parallèlement à $\bigoplus_{j \neq i} ker\ P_j(f)$ est un polynome en f*

Démonstration. *On se place dans $Ker\ P(f)$ Comme $P_1, ..., P_r$ sont deux à deux premiers entre eux, P_i et $\prod_{j \neq i} P_j$ sont premiers entre eux. Il existe donc U_i, $V_i \in \mathbb{K}[X]$ tels que $1 = U_iP_i + V_i \prod_{j \neq i} P_j$. Posons $p_i = (V_i \prod_{j \neq i} P_j)(f)$, on a $U_iP_i(f)(x) + p_i(x) = x$. Montrons que p_i est le projecteur de $ker\ P(f)$ sur $ker\ P_i(f)$ prallèlement à $\bigoplus_{j \neq i} ker\ P_j(f)$.*

D'abord $Im\ p_i = Ker\ P_i(f)$. En effet

- *$\forall x \in ker\ P_i(f)$, $x = U_iP_i(f)(x) + p_i(x) = p_i(x)$ donc $ker\ P_i(f) \subset Im\ p_i$*
- *$\forall y \in im\ p_i$ il existe $x \in ker\ P(f)$ tel que $P_i(f)(y) = P_i(f)(p_i(x)) = P_i(f) \circ (V_i \prod_{j \neq i}^{k} P_j)(f)(x) = (V_i \prod_{j=1}^{k} P_j)(f)(x)$ d'où $P_i(f)(y) = (V_i \circ P)(f)(x) = 0$. Ainsi $Im\ p_i = ker\ P_i(f)$*

D'autre part, $ker\ p_i = \bigoplus_{j \neq i} ker\ P_j(f)$. En effet

- *Soit $x \in \bigoplus_{j \neq i} ker\ P_j(f)$ Alors par définition de p_i, $p_i(x) = 0$*
- *Par le théorème du rang, $dim(ker\ p_i) + rg(p_i) = dim(ker\ P(f)) = dim(\bigoplus_{j \neq i} ker\ P_j(f)) + dim(ker\ P_i(f))$ Or comme $Im\ p_i = ker\ P_i(f)$ on à l'égalité des dimensions de $ker\ p_i$ et $\bigoplus_{j \neq i} ker\ P_j(f)$ d'où l'égalitée des espace*

$p_i^2(x) = p_ip_i(x) = (p_i \circ (Id - U_iP_i))(f))(x) = p_i(x) - (U_iP_i(f) \circ p_i)(x) = p_i(x)$ p_i est donc bien un projecteur sur $ker\ P_i(f)$ paralèllement à $\bigoplus_{j \neq i} ker\ P_j(f)$.