Théorème des restes chinois

Cf Lang, Algèbre p 101

95.1 Théorème des restes chinois

Soit A un anneau commutatif.
Soit $(a_i)_{i\in[\![1..n]\!]}$ une famille d'idéaux de A.
Si $\forall (i,j)\in[\![1..n]\!]^2,\ i\neq j \Rightarrow a_i + a_j = A$
alors $\forall (x_i)_{i\in[\![1..n]\!]}\in A^n,\ \exists x\in A,\ \forall i\in[\![1..n]\!]\quad x\equiv x_i \mod(a_i)$

Preuve : Si $n=2$. On a $a_1+a_2=A$, donc il existe $(a_1,a_2)\in a_1\times a_2$ tel que $a_1+a_2=1$. Soit $(x_1,x_2)\in A^2$ fixés.
On pose $x = x_2\times a_1 + x_1\times a_2$.
$x - x_2 a_1 = x_1 a_2 \in a_2$ donc $x\equiv x_2 a_1 \mod(a_2)$
Or $x_2 a_1 = x_2(1-a_2) = x_2 - x_2 a_2$ soit $x_2 a_1 - x_2 = x_2 a_2 \in a_2$
Donc $x_2 a_1 \equiv x_2 \mod(a_2)$, par transitivité $x\equiv x_2 \mod(a_2)$
On montre de même que $x\equiv x_1 \mod(a_1)$.

Si $n\geq 2$. Soit $k\in[\![1..n]\!]$.
Pour $i\in[\![1..n]\!]_{\setminus\{k\}}$ $1\in A = a_i + a_k$ donc $1 = a_i + b_i$ où $a_i\in a_k$ et $b_i\in a_i$
Alors $1 = \prod_{\substack{i=1\\ i\neq k}}^{n} (a_i+b_i)$

$$= \sum_{\substack{(I,J)\text{ partition}\\ \text{de }[\![1..n]\!]\setminus\{k\}}} \prod_{i\in I} a_i \times \prod_{j\in J} b_j$$

$$= \sum_{\substack{(I,J)\text{ partition}\\ \text{de }[\![1..n]\!]\setminus\{k\}\\ k\in I\neq\emptyset}} \underbrace{\prod_{i\in I} \underbrace{a_i}_{\in a_k} \times \prod_{j\in J} b_j}_{\in a_k} + \prod_{\substack{j=1\\ j\neq k}}^{n} \underbrace{b_j}_{\in a_j}$$

$$\in a_k + \sum_{\substack{i=1\\ i\neq k}}^{n} a_i$$

Donc $a_k + \sum_{\substack{i=1\\ i\neq k}}^{n} a_i = A$ et d'après le cas $n=2$ traité ci-avant il existe $y_k\in A$ tel que $\begin{cases} y_k \equiv 1 \mod(a_k) \\ y_k \equiv 0 \mod\left(\sum_{\substack{i=1\\ i\neq k}}^{n} a_i\right)\end{cases}$
Or $\sum_{\substack{i=1\\ i\neq k}}^{n} a_i \subset \bigcap_{\substack{i=1\\ i\neq k}}^{n} a_i$, donc $\forall i\in[\![1..n]\!]_{\setminus\{k\}}$ $y_k\in a_i$ soit $y_k\equiv 0 \mod(a_i)$

Considérant les $(y_k)_{k\in[\![1..n]\!]}$ ainsi construits et les $(x_k)_{k\in[\![1..n]\!]}$ fixés on pose $x = \sum_{k=1}^{n} x_k y_k$.

Alors pour tout $k\in[\![1..n]\!]$ on a $x \equiv \sum_{i=1}^{n} x_i y_i \mod (a_k)$
$\equiv \sum_{i=1}^{n} x_i \delta_{k,i} \mod (a_k)$
$\equiv x_k \mod (a_k)$.

95.2 Plaçons nous sous les hypothèses du théorème.
Pour $i\in[\![1..n]\!]$ on note π_i la projection canonique de A sur A/a_i.
On introduit alors $f = \left(\begin{array}{ccc} A & \longrightarrow & \prod_{i=1}^{n} A/a_i \\ a & \longmapsto & (\pi_i(a))_{i\in[\![1..n]\!]} \end{array}\right)$.
f est un morphisme d'anneau de A vers l'anneau produit $\prod_{i=1}^{n} A/a_i$, car chaque π_i est un morphisme d'anneau.

Le théorème des restes chinois dit exactement que si $\forall (i,j)\in[\![1..n]\!]^2, i\neq j \Rightarrow A = a_i + a_j$, alors f est surjective, car $a \equiv x_i \mod (a_i)$ se réécrit $\pi_i(a) = x_i$.

95.3 Cor $\forall (i,j)\in[\![1..n]\!]^2, i\neq j \Rightarrow a_i + a_j = A$
alors $A/\bigcap_{i=1}^{n} a_i \underset{\text{isomorphisme d'anneaux}}{\simeq} \prod_{i=1}^{n} A/a_i$

En effet l'isomorphisme est donné par le théorème de factorisation :

$$\begin{array}{ccc} A & \xrightarrow{f} & \prod_{i=1}^{n} A/A_i \\ \downarrow & \nearrow_{\bar{f}} & \\ A/\mathrm{Ker} f & & \end{array}$$

sachant que $\mathrm{Ker}(f) = \{x\in A \mid \forall i\in[\![1..n]\!]\ \pi_i(x)=0\}$
$= \bigcap_{i=1}^{n} \mathrm{Ker}(\pi_i)$
$= \bigcap_{i=1}^{n} a_i$.