3.3 Anneaux principaux

Définition : Un anneau A est principal ssi :

(i) A est intègre;

(ii) tout idéal de A est principal.

La condition (ii) signifie que pour tout idéal I de A il existe $a \in A$ tel que $I = (a)$.

Remarque : dans un anneau principal qui n'est pas un corps on a, si $p \neq 0$: p est irréductible $\Leftrightarrow$ (p) est maximal parmi les idéaux propres de A $\Leftrightarrow$ (p) maximal dans l'ensemble des idéaux propres de A (puisque tout idéal est principal).

Donc, dans un anneau principal si p est non nul on a : p irréductible $\Leftrightarrow$ (p) maximal $\Leftrightarrow$ (p) premier (d'après la proposition du 3.2).

Théorème : Un anneau principal est factoriel.

Démonstration : montrons la propriété (E).

Supposons qu'il existe un élément $a_1 \in A - \{0\}$ n'admettant pas de décomposition. Alors a_1 n'est ni inversible ni irréductible. Il existe a_2 et b_2 dans A tels que $a_1 = a_2 b_2$; a_1 n'ayant pas de décomposition il en est de même de a_2 ou de b_2. Supposons que ce soit a_2; on a donc $(a_1) \not\subset (a_2)$. Reprenant le raisonnement pour a_2 on voit qu'on peut construire par récurrence une suite $(a_1) \not\subset (a_2) \not\subset ... \not\subset (a_n) \not\subset ...$ strictement croissante d'idéaux de A. Il est clair que $I = \bigcup_{k \in N} (a_k)$ est un idéal de A. A étant principal il existe $d \in A$ tel que $I = (d)$. Comme $d \in I$, il existe $p \in \mathbb{N}$ tel que $d \in (a_p)$. On a donc $(d) \subset (a_p)$. L'inclusion inverse étant vraie on en déduit que $(d) = (a_p)$. Comme $(a_p) \subset (a_q) \subset (d)$ pour $q \geq p$ la suite (a_k) est stationnaire à partir de p ce qui n'est pas. A vérifie donc (E).

Pour montrer que A vérifie la propriété (U) il suffit de montrer que $p \in A - \{0\}$ est irréductible ssi l'idéal (p) est premier (d'après la proposition du 3.2) ce qui résulte de la remarque précédente.

La réciproque du théorème est fausse : par exemple $\mathbb{Z}[X]$ est factoriel d'après le théorème de Gauss mais pas principal (on voit facilement que l'idéal $(2, X)$ engendré par 2 et X n'est pas principal).

Proposition : Dans un anneau principal A, si a et b appartiennent à $A - \{0\}$ on a :

(i) $(a) + (b) = (\text{pgcd}(a, b))$.

(ii) a et b sont premiers entre eux ssi $(a) + (b) = A$ ssi $\exists (u, v) \in A \times A \ / \ au + bv = 1$ (*Relation de Bezout*).

On retrouve par conséquent la situation de $\mathbb{Z}$.

Démonstration :

(i) démonstration analogue à celle de l'exercice 7 de « groupes »;

(ii) clair.

Remarquons que *la relation de Bezout est fausse en général* si on ne suppose pas l'anneau principal : par exemple dans $\mathbf{K}[X, Y]$ les éléments X et Y sont premiers entre eux mais $(X) + (Y) \neq \mathbf{K}[X, Y]$ (car $(X) + (Y)$ est constitué des polynômes P tels que $P(0, 0) = 0$).

Le paragraphe suivant fournit un exemple important d'anneau principal.