5 Extension à un nombre fini d'entiers

■ PGCD de n entiers $n \geq 2$

Théorème 1 : Associativité de $\wedge$

Pour tous $a, b, c \in \mathbb{Z}$: $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, quantité que l'on peut donc noter $a \wedge b \wedge c$.

Démonstration. Notons $d_1 = (a \wedge b) \wedge c$ et $d_2 = a \wedge (b \wedge c)$ et montrons que $d_1 = d_2$.
On sait que $d_1 \mid a \wedge b$ et que $d_1 \mid c$. Ainsi : $d_1 \mid a$, $d_1 \mid b$ et $d_1 \mid c$.
Puisque $d_1 \mid b$ et $d_1 \mid c$, on sait par théorème que $d_1 \mid b \wedge c$.
Dès lors, puisque $d_1 \mid a$ et $d_1 \mid b \wedge c$, le même théorème assure que $d_1 \mid a \wedge (b \wedge c)$ *i.e.* $d_1 \mid d_2$.
On montre de même que $d_2 \mid d_1$.
Ainsi, d_1 et d_2 sont associés et sont par ailleurs positifs donc ils sont égaux. □

• **Conséquence.** La propriété d'associativité donne un sens à $a \wedge b \wedge c$ puis (par récurrence) à $a_1 \wedge \cdots \wedge a_n$ pour tout entier $n \geq 2$. Cette dernière quantité est appelée PGCD de $a_1, \ldots a_n$.

Par récurrence sur n, on peut étendre les propriétés vues pour deux entier dont :

Théorème 2 : Généralisation des propriétés du PGCD

1. *PGCD et diviseurs communs :* Les diviseurs communs à $a_1, \ldots, a_n$ sont les diviseurs de leur PGCD *i.e.* pour tout $d \in \mathbb{Z}$: $(\forall i \in [\![1, n]\!],\ d \mid a_i) \iff d \mid (a_1 \wedge \cdots \wedge a_n)$
2. *Relation de Bézout :* il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que : $\sum_{i=1}^{n} a_i u_i = a_1 \wedge \cdots \wedge a_n$.

■ Entiers premiers entre eux dans leur ensemble

Définition 1

Les entiers $a_1, a_2 \ldots a_n$ sont dits premiers entre eux dans leur ensemble si : $a_1 \wedge \cdots \wedge a_n = 1$,
ou encore si leur seul diviseur positif commun est 1.

On dispose encore de la caractérisation de Bézout :

Théorème 3

Soient $a_1, \ldots, a_n \in \mathbb{Z}$. Les deux propositions suivantes sont équivalentes :

i) $a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble.

ii) Il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que $\sum_{i=1}^{n} a_i u_i = 1$.

☢ **Attention** ☢ Ne pas confondre les propriétés suivantes :

- Les a_i sont premiers entre eux dans leur ensemble : $a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1$.
- Les a_i sont deux à deux premiers entre eux : si $i \neq j$ alors $a_i \wedge a_j = 1$.

Schématiquement :

« deux à deux premiers entre eux » $\implies$ « premiers entre eux dans leur ensemble »

mais la réciproque est fausse.
Par exemple 6, 10 et 15 sont premiers entre eux dans leur ensemble (leur seul diviseur positif commun est 1) mais 6 et 10 ne sont pas premiers entre eux, 6 et 15 non plus, ni 10 et 15.