

II. ESSAIS ET VARIÉTÉS

ESSAI D'UNE THÉORIE DU P.G.C.D. ET DU P.P.C.M., INSPIRÉ PAR LES MÉTHODES DE L'ALGÈBRE MODERNE

I. — On appelle « idéal » un ensemble (I) d'entiers relatifs tels que :

1° si α et $\alpha' \in (I)$, $\alpha + \alpha' \in (I)$;

2° si $\alpha \in (I)$, et si k est un entier relatif quelconque, $k\alpha \in (I)$.

PROPRIÉTÉS.

1° Si $\alpha \in (I)$, $-\alpha \in (I)$.

2° Si $\alpha \in (I)$, $\alpha' \in (I)$, $k\alpha + k'\alpha' \in (I)$, k et k' étant des entiers relatifs quelconques.

3° $0 \in (I)$.

4° Parmi tous les nombres positifs de (I), il en existe un qui est inférieur à tous les autres, soit Δ . Si $\alpha \in (I)$ nous pouvons diviser α par Δ :

$$\alpha = \Delta Q + R \quad 0 \leq R < \Delta.$$

D'après 1° $R = \alpha - \Delta Q \in (I)$ donc $R \geq \Delta$, ou $R = 0$. Il y a contradiction, sauf si $R = 0$.

THÉORÈME. — *Tous les entiers relatifs non nuls d'un même Idéal sont les multiples de l'un d'entre eux, l'entier positif qui a la plus petite valeur absolue.*

Réciproquement, on vérifie sans peine que tous les entiers relatifs de la forme $k\Delta$, Δ donné, k entier relatif quelconque, constituent un idéal.

Remarque. — Le groupe additif d'un idéal est isomorphe au groupe additif des entiers relatifs.

II. — Soient a et b deux entiers relatifs donnés. Nous cherchons tous les diviseurs communs à a et b . Il est clair qu'un tel diviseur divise tous les entiers relatifs $\alpha = ax + by$, x et y étant des entiers relatifs quelconques. Soient deux nombres de cette forme :

$$\alpha = ax + by \quad \alpha' = ax' + by',$$

les nombres

$$\alpha + \alpha' = a(x + x') + b(y + y'),$$

$$k\alpha = a.kx + b.ky \quad (k \text{ entier quelconque}),$$

ont encore la même forme. Par suite, les nombres de la forme $\alpha = ax + by$ constituent un Idéal (Iab) . a et b font partie de (Iab) .

Soit Δ le plus petit nombre positif de (Iab) . Tous les nombres de (Iab) sont multiples de Δ . En particulier a et b admettent Δ comme diviseur. Tout diviseur de Δ est un diviseur commun à a et b .

Réciproquement, comme $\Delta \in (Iab)$, on a :

$$\Delta = ax_0 + by_0,$$

et tout diviseur commun à a et b divise ax_0 et by_0 , donc leur somme algébrique Δ .

THÉORÈME. — *Tous les diviseurs communs à deux entiers relatifs sont les diviseurs du plus grand d'entre eux, Δ , appelé le P.G.C.D.*

COROLLAIRES.

1° Δ et $-\Delta$ sont les seuls nombres de (Iab) qui divisent a et b . En effet, tout autre entier non nul de (Iab) est supérieur à Δ en valeur absolue, il ne peut être diviseur commun à a et b , car il serait alors diviseur de Δ , ce qui est contradictoire.

2° Si $\Delta = 1$, on a $1 = ax_0 + by_0$, a et b n'ont aucun autre diviseur commun que 1 et -1 , ils sont *premiers entre eux*. (Iab) se confond alors avec l'anneau des entiers relatifs. Nous pouvons alors énoncer :

THÉORÈME DE BEZOUT. — *Pour que deux entiers relatifs a et b soient premiers entre eux, il faut et il suffit qu'il existe deux entiers relatifs x et y tels que*

$$ax + by = 1.$$

Remarque. — Dans $\Delta = ax_0 + by_0$, x_0 et y_0 sont premiers entre eux. En effet, s'il n'en est pas ainsi $x_0 = kx'_0$, $y_0 = ky'_0$

$$\text{et } \Delta = k(ax'_0 + by'_0); \quad \frac{\Delta}{k} = ax'_0 + by'_0$$

et Δ ne serait pas le plus petit nombre positif de (Iab).

PROPRIÉTÉS DU P.G.C.D. DE DEUX NOMBRES.

1° Soit Δ le P.G.C.D. de a et b . Si k est un entier quelconque, $k\Delta$ divise ka et kb . D'autre part :

$$\begin{aligned} \Delta &= ax_0 + by_0, \text{ donc :} \\ k\Delta &= (ka)x_0 + (kb)y_0. \end{aligned}$$

D'après le corollaire 1° ci-dessus, $k\Delta$ est le P.G.C.D. de ka et kb .

2° Si k est un diviseur de Δ , il est un diviseur commun à a et b , et on démontrerait de même que $\frac{\Delta}{k}$ est le P.G.C.D. de $\frac{a}{k}$ et $\frac{b}{k}$. En particulier si $k = \Delta$, $\frac{\Delta}{k} = 1$.

THÉORÈME. — *Pour que Δ , diviseur commun à a et b soit leur P.G.C.D., il faut et il suffit que $\frac{a}{\Delta}$ et $\frac{b}{\Delta}$ soient premiers entre eux.*

3° Supposons que c est premier avec a , et divise ab . Nous avons :

$$\begin{aligned} 1 &= ax + cy \quad (\text{théorème de Bezout}), \\ \text{donc} \quad b &= abx + bcy, \end{aligned}$$

c divise ab , donc abx , il divise bcy , il divise donc leur somme b .

THÉORÈME FONDAMENTAL DE LA DIVISIBILITÉ. — *Si un nombre divise un produit de deux facteurs, et est premier avec l'un d'eux, il divise l'autre.*

Les théorèmes suivants sur la divisibilité se démontrent ensuite comme dans les méthodes classiques.

Remarque. — Les restes successifs obtenus par la méthode de l'algorithme d'Euclide appartiennent tous à (Iab).

CAS DE PLUSIEURS ENTIERs RELATIFS a, b, c, d .

La méthode précédente se généralise. Les diviseurs communs cherchés divisent tous les nombres de la forme :

$$ax + by + cz + dt.$$

Ces nombres constituent un idéal (Iabcd), et cet idéal comprend les nombres a, b, c, d . Le P.G.C.D. de a, b, c, d est le plus petit nombre positif de cet idéal. Tous les diviseurs communs à a, b, c, d sont les diviseurs de

$$\Delta = ax_0 + by_0 + cz_0 + dt_0.$$

En particulier, pour que a, b, c, d soient premiers entre eux dans leur ensemble, il faut et il suffit qu'il existe des entiers relatifs x, y, z, t , tels que :

$$ax + by + cz + dt = 1.$$

Dans le cas général $\frac{a}{\Delta}, \frac{b}{\Delta}, \frac{c}{\Delta}, \frac{d}{\Delta}$ sont premiers entre eux dans leur ensemble, et cette propriété caractérise le P.G.C.D.

III. — Soient a et b deux entiers relatifs. Nous recherchons leurs multiples communs. Il en existe certainement, puisque (ab) possède cette propriété.

Si M_1 et M_2 sont deux multiples communs :

$$\begin{aligned} M_1 - M_2 &\text{ est un multiple commun,} \\ kM_1 &\text{ est un multiple quelconque.} \end{aligned}$$

THÉORÈME. — *Les multiples communs à deux entiers relatifs constituent un Idéal. Ils sont par suite les multiples de l'un d'entre eux, le multiple positif le plus petit, soit m , m est appelé le P.P.C.M. de a et b .*

Un multiple commun quelconque est : $M = km$, k étant un entier relatif quelconque.

En particulier $ab = km$.

Posons $m = a\alpha = b\beta$. Nous avons :

$$b = k\alpha \quad a = k\beta.$$

k est donc un diviseur commun à a et b , et sa valeur absolue est la plus grande possible pour que m soit le P.P.C.M. Donc k est égal au P.G.C.D., Δ , au signe près et :

$$m = \pm \frac{ab}{\Delta}$$

Les autres propriétés du P.P.C.M. se démontrent comme dans les méthodes classiques.

MULTIPLES COMMUNS A PLUSIEURS ENTIERS RELATIFS.

On montrerait de même que les multiples communs à plusieurs entiers relatifs a, b, c, d constituent un idéal (I_M), et que par suite $M = km$, m étant le P.P.C.M. Mais la méthode pour déterminer m ne se généralise pas.

FRIBOURG (Lycée de Saint-Cloud).