

Théorèmes de Bezout

Propriété

C'est la relation de **Bezout** dans sa forme la plus générale. Soient a et b deux entiers relatifs. Alors il existe deux entiers relatifs u et v tels que $au + bv = a\Lambda b$

Preuve

La preuve s'appuie sur l'algorithme d'euclide dit étendu.

Restreignons nous au cas où $0 \leq b < a$

Nous avons déjà montré l'existence de deux familles $(r_0, r_1, r_2 \dots r_N)$ et $(q_2, q_3 \dots q_{N-1})$ telles que :

- les premiers termes sont définis par : $(r_0, r_1) = (a, b)$ avec q_2 défini par $a = bq_2 + r_2 \Leftrightarrow r_0 = r_1q_2 + r_2$
- La relation de récurrence s'écrit $r_k = r_{k+1}q_{k+2} + r_{k+2}$ avec $0 \leq r_{k+1} < r_k$

Nous rappelons ici l'existence d'un N tel que $r_N = 0$. (voire démonstration PGCD)

Définissons deux suites $(U_k)_{0 \leq k \leq N}$ et $(V_k)_{0 \leq k \leq N}$

Telles que $(U_0, V_0) = (1, 0)$ et $(U_1, V_1) = (0, 1)$ et $\begin{cases} U_{k+2} = U_k - q_{k+2}U_{k+1} \\ V_{k+2} = V_k - q_{k+2}V_{k+1} \end{cases}$

Nous allons montrer que $\forall n \text{ tq } 0 \leq n \leq N \text{ alors } aU_n + bV_n = r_n$

Par récurrence :

Procédons d'abord à l'initialisation :

$$\begin{cases} aU_0 + bV_0 = a = r_0 \\ aU_1 + bV_1 = b = r_1 \end{cases}$$

Hérédité :

Supposons $\begin{cases} aU_k + bV_k = r_k \\ aU_{k+1} + bV_{k+1} = r_{k+1} \end{cases}$ alors nous avons :

$$aU_{k+2} + bV_{k+2} = a(U_k - q_{k+2}U_{k+1}) + b(V_k - q_{k+2}V_{k+1})$$

$$\Leftrightarrow aU_{k+2} + bV_{k+2} = aU_k + bV_k - q_{k+2}(aU_{k+1} + bV_{k+1})$$

$$\Leftrightarrow aU_{k+2} + bV_{k+2} = r_k - q_{k+2}(r_{k+1}) = r_{k+2}$$

Il suffit maintenant d'appliquer cette formule pour $k = N - 1$

$aU_{N-1} + bV_{N-1} = r_{N-1}$ donc $a\Lambda b = r_{N-1} = aU_{N-1} + bV_{N-1}$ Nous avons trouvé notre u et notre v .

Dans le cas où $0 \leq a < b$ il suffit de permuter les rôles de a et de b dans la démonstration précédente et le tour est joué. Dans le cas où $b = a$. Nous avons $a\Lambda b = a$ et il paraît clair que $2a - a = a$

Il nous reste à élargir la démonstration au cas où a ou b seraient négatifs.

Supposons que ce soit a . Rétablissons la démonstration sur $-a$

Il existe deux entiers relatifs u et v tels que $(-a)u + bv = (-a)\Lambda b$ soit $a(-u) + bv = a\Lambda b$ (car $(-a)\Lambda b = a\Lambda b$). La encore l'existence de ces deux entiers relatifs est démontrée. Par symétrie le cas où b serait négatif est démontré aussi.

Exemple

Déterminons dans un premier temps le PGCD de 255 et 141

$$255 = 1 \times 141 + 114$$

$$141 = 1 \times 114 + 27$$

$$114 = 4 \times 27 + 6$$

$$27 = 4 \times 6 + 3$$

$$6 = 2 \times 3 + 0$$

Nous avons donc $\text{PGCD}(255, 141) = 3$

$$3 = 27 - 4 \times 6$$

$$3 = 27 - 4 \times (114 - 4 \times 27)$$

$$3 = 27 - 4 \times 114 + 27 \times 16$$

$$3 = 17 \times 27 - 4 \times 114$$

$$3 = 17 \times (141 - 114) - 4 \times 114$$

$$3 = 17 \times 141 - 21 \times 114$$

$$3 = 17 \times 141 - 21 \times (255 - 141)$$

$$3 = 141(17 + 21) - 21 \times 255$$

$$3 = 141 \times 38 - 21 \times 255$$

Remarque

Attention ce couple (u, v) n'est pas unique.

En effet si au lieu de 38 et de -21 nous proposons $38 + k \times 255$ et $-21 - k \times 141$ avec k entier relatif alors $141(38 + k \times 255) - 255(21 + k \times 141) = 141 \times 38 - 255 \times 21 = 3$

Théorème	Généralisons la propriété précédente. Soient $a_1, a_2, \dots, a_n$ n entiers relatifs alors il existe $u_1, u_2, \dots, u_n$ entiers relatifs tels que $u_1 a_1 + u_2 a_2 + \dots + u_n a_n = a_1 \wedge a_2 \dots \wedge a_n$
Preuve	
Par récurrence. Dans le cas $n = 2$ c'est déjà démontré. Supposons que ce soit vrai dans le cas $n = p$ $\text{div}(a_1 \wedge a_2 \dots \wedge a_{p+1}) = \text{div}(a_1) \cap \text{div}(a_2) \cap \dots \cap \text{div}(a_{p+1}) = \{\text{div}(a_1) \cap \text{div}(a_2) \cap \dots \cap \text{div}(a_p)\} \cap \text{div}(a_{p+1})$ Donc $a_1 \wedge a_2 \dots \wedge a_{p+1} = (a_1 \wedge a_2 \dots \wedge a_p) \wedge a_{p+1}$ La relation de Bezout dans le cas de deux nombres nous donne donc l'existence de u et v entiers naturels tels que $a_1 \wedge a_2 \dots \wedge a_{p+1} = u(a_1 \wedge a_2 \dots \wedge a_p) + v a_{p+1}$ D'après l'hypothèse de récurrence $a_1 \wedge a_2 \dots \wedge a_p = u_1 a_1 + u_2 a_2 + \dots + u_p a_p$ Il vient $a_1 \wedge a_2 \dots \wedge a_{p+1} = u(u_1 a_1 + u_2 a_2 + \dots + u_p a_p) + v a_{p+1} = u u_1 a_1 + u u_2 a_2 + \dots + u u_p a_p + v a_{p+1}$ L'hérédité est donc démontrée.	
Exemple	Nous avons $18 \wedge 27 \wedge 6 = 3$ $18 \wedge 27 = 9$ $9 = 1 * 27 - 1 * 18$ $9 \wedge 6 = 3$ $3 = 1 * 9 - 1 * 6 = 1 * (1 * 27 - 1 * 18) - 1 * 6 = 1 * 27 - 1 * 18 - 1 * 6$ L'existence de trois entiers u, v, w tels que $3 = 18u + 27v + 6w$ est donc démontrée.