

Racines $p^{\text{èmes}}$ de l'identité

Partie 1 : Théorème de Bezout

Soient a et b deux entiers naturels non nuls.

Les entiers a et b sont dits premiers entre eux si $\text{pgcd}(a, b) = 1$. Le but de cette partie est d'établir le théorème de Bezout :

Théorème 1 :

Les entiers a et b sont premiers entre eux si et seulement si il existe des entiers u et v tels que $au + bv = 1$.

1. Montrer que s'il existe des entiers relatifs u et v tels que $au + bv = 1$ alors a et b sont premiers entre eux.

Correction : Soit $d \in \mathbb{N}^*$ un diviseur commun à a et b . Alors d divise $au + bv = 1$ par compatibilité de la division avec les combinaisons linéaires entières et $d \leq 1$.

Donc $d = 1$, le seul diviseur commun à a et b est 1. Les entiers a et b sont premiers entre eux.

2. On prouve la réciproque de cette propriété.

On suppose donc que a et b sont premiers entre eux et on considère l'ensemble $\mathcal{E}$ des entiers relatifs de la forme $au + bv$ où u et v sont des entiers relatifs,

$$\text{i.e. } \mathcal{E} = \{au + bv, (u, v) \in \mathbb{Z}^2\}.$$

- (a) Montrer que l'ensemble $\mathcal{E} \cap \mathbb{N}^*$ admet un plus petit élément que l'on notera n_0 .

Correction : Comme a est non nul, $1 \times a + 0 \times b$ ou $-1 \times a + 0 \times b$ appartiennent à $\mathcal{E} \cap \mathbb{N}^*$ qui est donc une partie non vide de $\mathbb{N}$ donc admet un plus petit élément n_0 i.e.

$$\exists (n_0, u_0, v_0) \in \mathbb{N}^* \times \mathbb{Z}^2, au_0 + bv_0 = n_0 \in \mathcal{E} \cap \mathbb{N}^*.$$

- (b) On note r (respectivement r') le reste de la division euclidienne de a (respectivement b) par n_0 . Montrer que r et r' appartiennent à $\mathcal{E}$.

Correction : On sait qu'il existe un (unique) couple $(q; r_0) \in \mathbb{Z}^2$ tel que :

$$\begin{aligned} a &= qn_0 + r_0 \text{ et } 0 \leq r_0 < n_0 \\ r &= a - qn_0 \\ &= a - q(au_0 + bv_0) \\ &= \underbrace{(1 - qu_0)}_{\in \mathbb{Z}} a + \underbrace{-qv_0}_{\in \mathbb{Z}} b \in \mathcal{E}. \end{aligned}$$

Le raisonnement est identique pour r' .

(c) En déduire que $r = r' = 0$.

Correction : Si r (ou r') était différent de 0 alors $r \in \mathcal{E} \cap \mathbb{N}^*$ et $r < n_0$ ce qui contredirait la définition de n_0 .

Donc $r = r' = 0$ i.e. n_0 est un diviseur commun à a et b . Il divise donc $\text{pgcd}(a; b) = 1$ et $n_0 = 1 \in \mathcal{E}$.

Il existe donc bien un couple d'entiers relatifs $(u; v)$ tel que $au + bv = n_0 = 1$.

3. Conclure.

Correction : Conclusion, a et b premiers entre eux $\iff \exists (u, v) \in \mathbb{Z}^2, au + bv = 1$.

Partie 2 : Racines de l'identité

Soient $n \in \mathbb{N}^*$ et p un entier supérieur ou égal à 2. On note

$$\mathcal{R}_n(p) = \{A \in \mathcal{M}_n(\mathbb{C}), A^p = I_n\}.$$

1. Soit $P \in \mathcal{M}_n(\mathbb{C})$ inversible.

Montrer que si $A \in \mathcal{R}_n(p)$ alors $P^{-1}AP \in \mathcal{R}_n(p)$.

Correction : Soit $P \in \mathcal{M}_n(\mathbb{C})$ inversible et soit $A \in \mathcal{R}_n(p)$. On a ainsi $A^p = I_n$. Dès lors, on peut écrire

$$\begin{aligned} (P^{-1}AP)^p &= \underbrace{(P^{-1}AP)(P^{-1}AP)(P^{-1}AP) \dots (P^{-1}AP)(P^{-1}AP)}_{p \text{ fois}} \\ &= P^{-1}A(PP^{-1})A(PP^{-1})AP \dots P^{-1}A(PP^{-1})AP \\ &= P^{-1} \underbrace{A \dots A}_p P = P^{-1}A^p P = P^{-1}I_n P = P^{-1}P = I_n. \end{aligned}$$

Commentaires : Ou à démontrer plus rigoureusement par récurrence. Si on ne vous demande pas de le faire ainsi, vu la simplicité du résultat, vous pouvez écrire directement qu'il est clair que $(P^{-1}AP)^p = P^{-1}A^p P$ pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$.

On a ainsi $(P^{-1}AP)^p = I_n$ donc $P^{-1}AP \in \mathcal{R}_n(p)$.

2. Soit $A \in \mathcal{R}_n(p)$.

Montrer que A est inversible et exprimer A^{-1} en fonction de A . En déduire que $A^{-1} \in \mathcal{R}_n(p)$.

Correction : Soit $A \in \mathcal{R}_n(p)$. On a $A^p = I_n$ que l'on peut réécrire

$$AA^{p-1} = A^{p-1}A = I_n.$$

Donc A est inversible d'inverse $A^{-1} = A^{p-1}$.

Il s'ensuit

$$(A^{-1})^p = (A^{p-1})^p = A^{p(p-1)} = (A^p)^{p-1} = I_n^{p-1} = I_n.$$

Donc, $A^{-1} \in \mathcal{R}_n(p)$.

3. Montrer que l'ensemble des matrices diagonales de $\mathcal{R}_n(p)$ forme un ensemble fini dont on déterminera le cardinal.

Correction : Soit $A = \text{diag}(a_1, \dots, a_n) \in \mathcal{M}_n(\mathbb{C})$ une matrice diagonale.

$$\begin{aligned} A \in \mathcal{R}_n(p) &\iff A^p = I_n \iff \begin{pmatrix} a_1^p & & \\ & \ddots & \\ & & a_n^p \end{pmatrix} = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \iff \begin{cases} a_1^p = 1 \\ \vdots \\ a_n^p = 1. \end{cases} \\ &\iff \forall i \in \llbracket 1; n \rrbracket, a_i \in \mathbb{U}_p. \end{aligned}$$

Donc l'ensemble des matrices diagonales de $\mathcal{R}_n(p)$ est l'ensemble des matrices diagonales dont les coefficients diagonaux sont des racines $p^{\text{èmes}}$ de l'unité au nombre de p .

C'est donc un ensemble fini de cardinal p^n .

4. On considère q un entier naturel supérieur ou égal 2 et on note $d = \text{pgcd}(p; q)$.
(a) Montrer que $\mathcal{R}_n(d) \subset \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$.

Correction : Soit $A \in \mathcal{R}_n(d)$ i.e. $A^d = I_n$.

On a $d|p$ et $d|q$ donc il existe deux entiers p' et q' tels que $p = dp'$ et $q = dq'$.

$$\begin{aligned} \text{D'où, } A^p &= A^{dp'} = (A^d)^{p'} = I_n^{p'} = I_n \text{ donc } A \in \mathcal{R}_n(p) \\ \text{et } A^q &= A^{dq'} = (A^d)^{q'} = I_n^{q'} = I_n \text{ donc } A \in \mathcal{R}_n(q). \end{aligned}$$

Conclusion, $A \in \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$ i.e. $\mathcal{R}_n(d) \subset \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$.

- (b) Justifier qu'il existe deux entiers u et v tels que $pu + qv = d$.

Correction : Comme $d = \text{pgcd}(p; q)$, il existe deux entiers p' et q' premiers entre eux tels que $p = dp'$ et $q = dq'$.

D'après le théorème de Bezout, il existe deux entiers u et v tels que $p'u + q'v = 1$.

En multipliant cette relation par d , il vient

$$dp'u + dq'v = d \iff pu + qv = d.$$

- (c) En déduire que $\mathcal{R}_n(d) = \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$.

Correction : Montrons $\mathcal{R}_n(d) = \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$ par double inclusion.

On a déjà établi $\mathcal{R}_n(d) \subset \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$ à la question (4a).

Réciproquement, soit $A \in \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$ i.e. $A^p = I_n$ et $A^q = I_n$.

D'après la question (4b), il existe deux entiers u et v tels que $d = pu + qv$.

On peut alors réécrire :

$$A^d = A^{pu+qv} = A^{pu} A^{qv} = (A^p)^u (A^q)^v = I_n^u I_n^v = I_n \iff A \in \mathcal{R}_n(d).$$

On a ainsi établi $\mathcal{R}_n(p) \cap \mathcal{R}_n(q) \subset \mathcal{R}_n(d)$.

Finalement, $\mathcal{R}_n(p) \cap \mathcal{R}_n(q) = \mathcal{R}_n(d)$.