Françoise et Étienne TRABBIA, lycée de VINCENDO et IREM de la Réunion, 1999/2000

ACTIVITÉS SUR LES POLYNÔMES

Activité 4

Entiers de Gauss

On considère l'ensemble G des nombres complexes de forme algébrique $x + iy$, où x et y sont des entiers relatifs ; G est appelé l'ensemble des entiers de Gauss.
Pour tout élément α de G, on note $n(\alpha)$ l'entier naturel égal au carré du module de α (si $\alpha = x + iy$; $n(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = x^2 + y^2$).
Soient α et β éléments de G, avec $\beta \neq 0$, on dit que β est un diviseur de α dans G, ou que α est un multiple de β dans G, lorsque $\frac{\alpha}{\beta}$ appartient à G.

1) a) Montrer que pour tout α élément non nul de G, α est un diviseur de $n(\alpha)$ dans G.
b) Montrer que si β divise α dans G, alors $n(\beta)$ divise $n(\alpha)$ dans $\mathbb{N}$.
c) Soit $\alpha = 5 + 3i$ et $\beta = 4 + i$; montrer que $n(\beta)$ divise $n(\alpha)$ dans $\mathbb{N}$. A-t-on β diviseur de α dans G ? Que dire de la propriété réciproque du b) ?

2) On veut déterminer les diviseurs β de 1 dans G ; ils doivent donc vérifier : $n(\beta)$ diviseur de 1 dans $\mathbb{N}$, c'est-à-dire $n(\beta) = 1$.
a) Déterminer tous les couples d'entiers relatifs (x, y) tels que $x^2 + y^2 = 1$.
b) Écrire la liste des diviseurs de 1 dans G. Ces éléments sont appelés les « éléments unitaires » de G. Ce sont les seuls éléments de G dont l'inverse appartient à G.

3) a) Déterminer tous les éléments de G vérifiant $n(\alpha) = 2$.
b) Faire de même pour $n(\alpha) = 5$ et pour $n(\alpha) = 13$.

4) a) Déterminer tous les diviseurs dans G de $1 + i$.
b) Faire de même pour $2 + 3i$ et $-4 + 7i$.
(Indication : utiliser 1) b) et les éléments unitaires ; $1 + i$ et $2 + 3i$ possèdent chacun huit diviseurs dans G, et $-4 + 7i$ en possède seize.)

5) Si α et β sont deux éléments non nuls de G, et si β est un diviseur de α dans G, on dit que β est un diviseur strict de α dans G lorsque $n(\beta)$ est un diviseur strict de $n(\alpha)$ dans $\mathbb{N}^*$.
On dit que α est premier dans G s'il n'admet aucun diviseur strict, sinon il est dit composé dans G.
Exemples :
• $1 + i$ est premier car il n'admet aucun diviseur strict.
• $3 - i$ n'est pas premier, car $3 - i = (1 + i)(1 - 2i)$ est le produit de deux diviseurs stricts de $3 - i$; comme $1 + i$ et $1 - 2i$ sont premiers, on dit que l'on a décomposé $3 - i$ en produit de facteurs premiers dans G.
Remarque : chaque facteur premier d'une décomposition est défini à un facteur unitaire près.
a) Décomposer $-4 + 7i$ en produit de facteurs premiers dans G.
b) Faire de même pour $3 + 4i$ et $9 + 7i$.

Commentaires sur G = $\mathbb{Z}$[i], anneau des entiers de Gauss :

• On peut montrer que la recherche des éléments α premiers dans G se ramène à la recherche des nombres $n(\alpha)$ premiers dans $\mathbb{N}^*$ s'écrivant comme somme des carrés de deux entiers, c'est à dire pour $n(\alpha) > 2$; $n(\alpha)$ premier dans $\mathbb{N}$ et de la forme $4k + 1$.

• On peut définir une division euclidienne dans G, avec pour grandeur euclidienne le module. Il n'y a pas unicité du quotient et du reste. Exemple :

$$-2 + 5i = (3 + i)(2i) - i \text{ avec } |-i| < |3 + i|$$
$$-2 + 5i = (3 + i)\, i + (-1 + 2i) \text{ avec } |-1 + 2i| < |3 + i|.$$