DOMAINE : Algèbre
NIVEAU : Intermédiaires
CONTENU : Exercices

AUTEUR : Pierre BERTIN
STAGE : Grésillon 2011

Nombres complexes en algèbre

Exercice 1 Soit $P \in \mathbb{C}[X]$ un polynôme à coefficients complexes. Montrez que P admet une racine dans $\mathbb{C}$.

Exercice 2 Calculez en fonction de n la somme suivante :

$$\sum_{k \equiv 1[4]} \binom{n}{k}$$

Exercice 3 Montrez que pour tout $n \geqslant 3$, il existe un couple d'entiers impairs (x_n, y_n) tel que

$$x_n^2 + 7y_n^2 = 2^n$$

Exercice 4 Pour tout $t > 0$, on considère la somme $S = r_1^2 + r_2^2 + r_3^2 + r_4^2$, où r_1, r_2, r_3, r_4 sont les racines du polynôme

$$P_t[X] = \frac{1}{t}X^4 + \left(1 - \frac{10}{t}\right)X^3 - 2X^2 + \sqrt[3]{2t}X + \arctan(t)$$

Quelle est la valeur minimale de $|S|$ et en quel t est-elle atteinte ?

Exercice 5 Soient x, y, z trois réels qui vérifient

$$\frac{\sin(x) + \sin(y) + \sin(z)}{\sin(x+y+z)} = \frac{\cos(x) + \cos(y) + \cos(z)}{\cos(x+y+z)} = a$$

Montrez que

$$\cos(x+y) + \cos(y+z) + \cos(z+x) = a$$

Exercice 6 Montrez la formule de Moivre :

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$$

En déduire que si $\cos(\theta)$ et $\sin(\theta)$ sont rationnels, alors $\cos(n\theta)$ et $\sin(n\theta)$ sont eux aussi rationnels.

Exercice 7 (Entiers de Gauss) Les entiers de Gauss $\mathbb{Z}[i]$ sont tous les nombres de la forme

$$a = a_1 + ia_2\ ,\ a_1, a_2 \in \mathbb{Z}$$

On définit la norme de a par $N(a) = a_1^2 + a_2^2$, et on appelle les éléments de $\mathbb{Z}[i]$ de norme 1 les unités.

1. Vérifiez que $N(ab) = N(a)N(b)$.
2. Prouvez l'existence d'une division euclidienne : Soient a et b deux entiers de Gauss, montrez que l'on peut trouver deux entiers de Gauss q et r (pas forcément uniques) tels que
   – $a = bq + r$
   – $N(r) < N(b)$
   En déduire le théorème de Bezout pour les entiers de Gauss.
3. On définit les deux concepts suivants :
   – on dit que p est *irréductible* si ses seuls diviseurs sont 1 et lui-même (à une unité près)
   – on dit que q est *premier* si $q|ab \Rightarrow q|a$ ou $q|b$.
   Montrez que dans $\mathbb{Z}[i]$, p premier $\Leftrightarrow$ p irréductible. (Indication : un sens est facile et l'autre sens utilise Bezout)
4. Démontrez l'existence et l'unicité de la décomposition en facteurs premiers dans $\mathbb{Z}[i]$.
5. Montrez qu'un entier de Gauss a est premier ssi l'un de ces cas est vérifié
   – $N(a) = 2$ ou $N(a) = p$ avec p un entier premier $\equiv 1[4]$
   – $N(a) = q^2$ avec q un entier premier $\equiv 3[4]$

- Correction -

Solution de l'exercice 1 On prend $P \in \mathbb{C}[X]$, et on considère $Q(X) = P(X)\overline{P}(X)$. Pour tout $x \in \mathbb{R}$, on a alors $Q(x) = P(x)\overline{P(x)} = |P(x)|^2 \in \mathbb{R}$. Donc Q est à valeurs réelles sur $\mathbb{R}$, on en déduit que $Q(X)$ est un polynôme à coefficient réel. D'après le théorème de D'Alembert-Gauss, Q a donc au moins une racine

$z \in \mathbb{C}$. Donc $Q(z) = P(z)\overline{P}(z) = 0$: soit $P(z) = 0$ et on a une racine, soit $\overline{P}(z) = 0$ et dans ce cas $P(\overline{z}) = 0$.

Solution de l'exercice 2 Fixons $n > 0$, on définit les 4 sommes suivantes :

$$S_i = \sum_{k \equiv i[4]} \binom{n}{k} \quad i \in \{0, 1, 2, 3\}$$

Maintenant on va utiliser la formule $(1+x)^n = \sum \binom{k}{n} x^n$ avec $x = 1, -1$ et i.

$$\begin{aligned} S_0 + S_1 + S_2 + S_3 &= 2^n \\ S_0 - S_1 + S_2 - S_3 &= 0 \\ S_0 - S_2 &= Re((1+i)^n) \\ S_1 - S_3 &= Im((1+i)^n) \end{aligned}$$

Ensuite il suffit d'utiliser que $(1+i)^2 = 2i$ et on a selon les cas suivants :

$$\begin{aligned} n = 4k &: S_1 = 2^{4k-2} \\ n = 4k+1 &: S_1 = 2^{4k-1} + (-1)^k 2^{2k-1} \\ n = 4k+2 &: S_1 = 2^{4k} + (-1)^k 2^{2k} \\ n = 4k+3 &: S_1 = 2^{4k+1} + (-1)^k 2^{2k} \end{aligned}$$

Solution de l'exercice 3 Pour $n = 3$ on a le couple $(1,1)$, pour $n = 4$ le couple $(3,1)$, etc. L'astuce est de considérer les complexes de la forme $a + i\sqrt{7}b$, $a, b \in \mathbb{Z}$, muni de la norme $N(a + i\sqrt{7}b) = a^2 + 7b^2$. Comme il s'agit du carré du module, il est évident que cette norme est multiplicative. Utilisons cette propriété à bon escient pour construire la suite (x_n, y_n) par récurrence :

$$\begin{aligned} N\left((x_n + i\sqrt{7}y_n)(1 + i\sqrt{7})\right) &= N(x_n + i\sqrt{7}y_n)N(1 + i\sqrt{7}) \\ N((x_n - 7y_n) + i\sqrt{7}(x_n + y_n)) &= 2^{n+3} \end{aligned}$$

Mais les deux entiers $x_n - 7y_n$ et $x_n + y_n$ sont pairs alors qu'on veut des entiers impairs. Qu'à cela ne tienne, on les divise par 2 :

$$N\left(\frac{x_n - 7y_n}{2} + i\sqrt{7}\frac{x_n + y_n}{2}\right) = 2^{n+1}$$

Et donc si les entiers $\left(\frac{x_n - 7y_n}{2}, \frac{x_n + y_n}{2}\right)$ sont impairs, on a gagné. S'ils sont pairs, on recommence tout avec $(x_n - i\sqrt{7}y_n)$ à la place, et on se retrouve avec

$\left(\frac{x_n+7y_n}{2}, \frac{x_n+y_n}{2}\right)$. Il es facile de vérifier que parmi ces deux couples, l'un est un couple d'entiers pairs et l'autre un couple d'entiers pairs. On prend le couple impair et on a (x_{n+1}, y_{n+1}).

Solution de l'exercice 4

$$\begin{aligned} S &= r_1^2 + r_2^2 + r_3^2 + r_4^2 \\ &= (r_1 + r_2 + r_3 + r_4)^2 - 2(r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4) \\ &= \left(-\frac{1 - 10/t)}{1/t}\right)^2 - 2\frac{-2}{1/t} \\ &= t^2 - 16t + 100 \end{aligned}$$

Une étude de ce trinôme montre que la valeur minimale de $|S|$ est 36 et est atteinte en $t = 8$.

Solution de l'exercice 5 Écrivons ces deux égalités sous la forme

$$\cos(x)+\cos(y)+\cos(z) = a\cos(x+y+z) \text{ et } \sin(x)+\sin(y)+\sin(z) = a\sin(x+y+z)$$

$$\begin{aligned} e^{ix} + e^{iy} + e^{iz} &= ae^{i(x+y+z)} \\ e^{-i(y+z)} + e^{-i(x+z)} + e^{-i(x+y)} &= a \end{aligned}$$

et en prenant la partie réelle on obtient la formule désirée.

Solution de l'exercice 6 La formule de Moivre est une simple traduction de $(e^{i\theta})^n = e^{in\theta}$. Comme $\cos(n\theta)$ et $\sin(n\theta)$ s'obtiennent comme polynômes à coefficients entiers de $\cos(\theta)$ et $\sin(\theta)$, la propriété est évidente.

Solution de l'exercice 7

1. Comme N est le carré du module, c'est évident.
2. On prouve tout d'abord un petit lemme : pour tout complexe z il existe un entier de Gauss a tel que $|z - a| < 1$. En effet, pour tout point du plan, le plus proche point à coordonnées entières est au plus à distance $\frac{1}{\sqrt{2}}$. Maintenant faisons notre division euclidienne à proprement parler : soient a, b deux entiers de Gauss et soit $z = \frac{a}{b}$. On prend q un entier de Gauss à distance < 1 de z, et $r = a - bq$. On a bien

   $$N(r) = |b(z - q)|^2 = N(b)|z - q|^2 < N(b)$$

   L'existence de l'algorithme d'Euclide et le théorème de Bezout s'ensuivent.

3. Il faut démontrer séparément les deux sens de l'équivalence
   - Soit q un premier. Raisonnons par l'absurde : on suppose que n'est pas irréductible : $q = ab$ avec a, b qui ne sont pas des unités : $1 < N(a), N(b) < N(q)$. Comme q divise q, cela que soit $q|a$, soit $q|b$. Mais ceci est impossible puisque ces deux nombres ont une norme inférieure à celle de q.
   - Soit p irréductible. Supposons que p divise ab mais ni a ni b. Comme p est irréductible, cela implique que PGCD(a, p) =PGCD$(b, p) = 1$. D'après Bezout, on peut trouver $u_a, u_b \in \mathbb{Z}[i]$ tels que

     $$u_a a \equiv u_b b \equiv 1[p]$$

     Et donc $u_a a u_b b \equiv 1[p]$ ce qui en contradiction avec $p|ab$, donc p est bien premier.
4. Quand on a l'équivalence entre premier et irréductible, l'existence et l'unicité de la décomposition en facteurs premiers se fait exactement de la même façon que dans les entiers (par récurrence sur $N(a)$).
5. Pour démontrer ce résultat on va admettre le théorème des deux carrés de Fermat : un entier n peut s'écrire comme somme de deux carrés ssi pour tous les premiers $q \equiv 3[4]$, $\nu_q(n)$ est paire. En particulier, un entier premier p peut s'écrire comme somme de deux carrés ssi $p \equiv 1[4]$ ou $p = 2$.

   Soit a un entier de Gauss, alors si $N(a)$ est un premier il est facile de voir que a est irréductible (si $a = bc$, alors $N(a) = N(b)N(c)$). Maintenant si $N(a) = q^2$ avec q premier $\equiv 3[4]$, supposons que a est composé : $a = bc$. Le seul cas possible est alors $N(b) = N(c) = q$, et $q = b_1^2 + b_2^2$, ce qui est en contradiction avec le théorème des deux carrés.

   La réciproque est une conséquence de l'existence de la factorisation en facteurs premiers et du théorème des deux carrés de Fermat : soit a un entier de Gauss, $N(a)$ est la somme de deux carrés, donc sa décomposition en facteurs premiers est :

   $$N(a) = 2^{\alpha_2} \prod_{p \equiv 1[4]} p^{\alpha_p} \prod_{q \equiv 3[4]} q^{2\beta_q}$$

   Donc, en choisissant pour tout $p \equiv 1[4]$ un couple (x_p, y_p) tq $x_p^2 + y_p^2 = p$

   $$a\overline{a} = (1+i)^{\alpha_2}(1-i)^{\alpha_2} \prod_{p \equiv 1[4]} (x_p + iy_p)^{\alpha_p}(x_p - iy_p)^{\alpha_p} \prod_{q \equiv 3[4]} q^{2\beta_q}$$

et d'après le début de la question, tous les termes de ce produit sont des premiers dans l'anneau des entiers de Gauss. Il s'agit donc de la décomposition en facteurs premiers de $a\overline{a}$. Donc si a avait un facteur premier qui ne soit pas de la forme demandée, il devrait apparaîtrait dans le produit. Comme il n'y en a pas, la réciproque est démontrée.