Licence MPCI, 2e année
Algèbre Générale

Devoir Maison
A rendre pour le Mercredi 24 avril

Exercice 1 (Entiers de Gauss)**.**

On définit le sous-ensemble de $\mathbb{C}$ suivant :

$$\mathcal{A} = \{a + ib \,|\, a, b \in \mathbb{Z}\}$$

(1) Montrer que $(\mathcal{A}, +)$ est un groupe abélien.

On montre que $\mathcal{A}$ est un sous-groupe de $\mathbb{C}$.
— $0 = 0 + 0i \in \mathcal{A}$.
— Soit $z = a + ib$ et $z' = a' + ib'$ dans $\mathcal{A}$. Alors $z + z' = (a + a') + i(b + b') \in \mathcal{A}$.
— De même $-z = -a + i(-b) \in \mathcal{A}$.
Comme $\mathbb{C}$ est abélien, tout sous-groupe de $\mathbb{C}$ est abélien. Donc $\mathcal{A}$ est un groupe abélien.

(2) Justifier que $\mathcal{A}$ est stable par multiplication. Déterminer $\mathcal{A}^*$, l'ensemble des inversibles de $(\mathcal{A}, \times)$.

Soit $z = a + ib$ et $z' = a' + ib'$ dans $\mathcal{A}$. On a

$$zz' = (aa' - bb') + i(ab' + ba') \in \mathcal{A}$$

Donc $\mathcal{A}$ est stable par multiplication. Un élément $z = a + ib$ est inversible si il existe $z' = a' + ib'$ tel que $zz' = 1$. On remarque que $|zz'|^2 = |z|^2|z'|^2 = 1$. Or $|z|^2 = a^2 + b^2 \in \mathbb{Z}$. Donc un élément inversible est de norme 1. On en déduit que si z est inversible alors $z \in \{1, i, -1, -i\}$. Réciproquement, ces quatres éléments sont inversibles. Donc $\mathcal{A}^* = \{1, i, -1, -i\}$.

(3) Soit $z \in \mathcal{A}$ un élément non-inversible. On dit que z est *réductible* dans $\mathcal{A}$, si il existe $x, y \in \mathcal{A}$ non-inversibles tels que $z = xy$. Sinon on dit que z est irréductible dans $\mathcal{A}$. (Remarque : par convention, un élément inversible sera dit réductible)
Justifier que 3 est irréductible dans $\mathcal{A}$ alors que 5 est réductible dans $\mathcal{A}$.

On montre d'abord que 5 est réductible dans $\mathcal{A}$. En effet, $5 = (2 + i)(2 - i)$.
Pour montrer que 3 est irréductible on suppose qu'il existe z, z' non inversibles tels que $zz' = 3$. On en déduit que $|z|^2|z'|^2 = 9$. Or $|z| \neq 1$ et $|z'| \neq 1$. Donc $|z|^2 = |z'|^2 = 3$. Or $|z|^2 = a^2 + b^2$. Or on ne peut pas trouver $a, b \in \mathbb{Z}$ tels que $a^2 + b^2 = 3$. Donc 3 est irréductible dans $\mathcal{A}$.

(4) Soit $x, y \in \mathcal{A}$ avec $y \neq 0$. Montrer qu'il existe $q \in \mathcal{A}$ tel que $|\frac{x}{y} - q| \leq \frac{1}{\sqrt{2}}$.
En déduire qu'il existe $r \in \mathcal{A}$ tels que $x = qy + r$ et $|r| < |y|$.

On utilise un petut raisonnement géométrique. Tout point du plan $\mathbb{R}^2$ appartient à un carré de la forme $[j, j + 1] \times [k, k + 1]$ avec $j, k \in \mathbb{Z}$. Tout point du carré est à distance inférieure à $\frac{1}{\sqrt{2}}$ de l'un des sommets du carré. (Le maximum est atteint pour le point au centre du carré).
Si $x, y \in \mathcal{A}$ alors, on considère le nombre complèxe $p = x/y$ que l'on place sur le plan complexe. Il est à distance inférieure à $\frac{1}{\sqrt{2}}$ d'un point à coordonnées entières, c'est à dire un élément $q \in \mathcal{A}$.
On pose ensuite $r = x - qy$, et on a immédiatement $|r| = |x - qy| = |y||\frac{x}{y} - q| \leq \frac{|y|}{\sqrt{2}} < |y|$.

(5) (***) Soit $I \subset \mathcal{A}$ un sous-groupe de $(\mathcal{A}, +)$. On suppose que pour tout $x \in I$ et tout $y \in \mathcal{A}$, on a $xy \in I$. (On dit que I est un idéal de $\mathcal{A}$.) Montrer qu'il existe $m \in \mathcal{A}$ tel que

$$I = m\mathcal{A} = \{ma \,|\, a \in \mathcal{A}\}$$

(Indication : On s'inspirera de la démonstration sur les sous-groupes de $\mathbb{Z}$.)

La démonstration sur les sous-groupes de $\mathbb{Z}$ repose sur la division euclidienne. La question précédente montre qu'il existe une forme de division euclidienne dans $\mathcal{A}$.
On considère l'ensemble $E = \{|z|^2, z \in I\}$ qui est un sous-ensemble de $\mathbb{N}$. Si cet ensemble est réduit à 0 alors $I = \{0\} = 0\mathcal{A}$. On suppose donc $E \neq \{0\}$. L'ensemble $E \setminus \{0\}$ est donc non-vide et admet un minimum. Soit $m \in I$ tel que $|m|^2$ est le minimum. Montrons $I = m\mathcal{A}$.
On montre d'abord que $m\mathcal{A} \subset I$. En effet, comme $m \in I$, on en déduit que pour tout $a \in \mathcal{A}, ma \in I$ (c'est la propriété d'être un idéal).
Maintenant, soit $z \in I$. Il existe $q, r \in \mathcal{A}$ tel que $z = qm + r$ avec $|r| < |m|$. Alors l'élément $r = z - qm \in I$. Par minimalité de $|m|$ on en déduit que $r = 0$. Donc $z = qm \in m\mathcal{A}$.

(6) Soit z un élément irreductible de $\mathcal{A}$ et I un idéal de $\mathcal{A}$. Montrer que si $z\mathcal{A} \subset I$ alors ($I = \mathcal{A}$ ou $I = z\mathcal{A}$.) .

Soit I un ideal de A tel que $z\mathcal{A} \subset I$. Alors il existe $m \in \mathcal{A}$ tel que $I = m\mathcal{A}$. On en déduit que $z \in m\mathcal{A}$, donc il existe $n \in \mathcal{A}$ tel que $z = mn$. Or z est irréductible donc m ou n est inversible. Si m est inversible, alors $m\mathcal{A} = \mathcal{A}$. Si n est inversible, alors $m = n^{-1}z \in z\mathcal{A}$ et donc $z\mathcal{A} = m\mathcal{A}$.

(7) Soit $x, y, z \in \mathcal{A}$. Montrer que si z est irreductible et $xy \in z\mathcal{A}$, alors $x \in z\mathcal{A}$ ou $y \in z\mathcal{A}$.

On considère l'ensemble $I_x = \{a \in \mathcal{A} | xa \in z\mathcal{A}\}$. Cet ensemble est un idéal. On sait que $y \in I_x$ et de plus $z\mathcal{A} \subset I$. Donc d'après la question précédente $I_x = \mathcal{A}$ ou $I_x = z\mathcal{A}$. Si $I_x = z\mathcal{A}$ on a $y \in z\mathcal{A}$. Sinon on a $I_x = \mathcal{A}$, et en particulier $1 \in I_x$ et donc $x = 1x \in z\mathcal{A}$.

Exercice 2 (Polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.)**.**

Soit $p > 2$ un nombre premier. On définit l'ensemble des polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ de façon formelle.

$$\mathbb{Z}/p\mathbb{Z}[X] = \{\overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n \,|\, \overline{a_i} \in \mathbb{Z}/p\mathbb{Z}, n \in \mathbb{N}\}$$

On peut défnir l'addition et la multiplication de deux polynômes exactement de la même façon que les polynômes usuels. Le degré d'un tel polynôme est toujours défini comme l'indice le plus grand pour lequel $\overline{a_i} \neq \overline{0}$ (et par convention $\deg P = -\infty$ si P est le polynôme nul, noté 0).

(1) Exemple : Dans $\mathbb{Z}/5\mathbb{Z}[X]$, justifier que $(\overline{2}X^2 + \overline{4}X + \overline{4})(\overline{3}X^2 + \overline{4}X + \overline{1}) = X^4 + \overline{4}$.

On calcule
$$\begin{aligned}(\overline{2}X^2 + \overline{4}X + \overline{4})(\overline{3}X^2 + \overline{4}X + \overline{1}) &= \overline{6}X^4 + \overline{8}X^3 + \overline{2}X^2 + \overline{12}X^3 + \overline{16}X^2 + \overline{4}X + \overline{12}X^2 + \overline{16}X + \overline{4} \\ &= \overline{6}X^4 + \overline{20}X^3 + \overline{30}X^2 + \overline{20}X + \overline{4} \\ &= X^4 + \overline{4}\end{aligned}$$

(2) Soit $P, Q \in \mathbb{Z}/p\mathbb{Z}[X]$. Montrer que deg(PQ) = deg(P) + deg(Q). (Si vous n'avez pas utilisé l'hypothèse sur p, c'est qu'il manque quelque chose ...)

Si $P = 0$ alors $PQ = 0$ et donc $\deg(\mathrm{PQ}) = -\infty = -\infty + \deg(\mathrm{Q}) = \deg\mathrm{P} + \deg\mathrm{Q}$.
On suppose maintenant que $P, Q \neq 0$. On note deg(P) = n et deg(Q) = m de sorte que $P = \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n$ et $Q = \overline{b_0} + \overline{b_1}X + \cdots + \overline{b_m}X^m$ avec $\overline{a_n} \neq \overline{0}$ et $\overline{b_m} \neq \overline{0}$. Alors $PQ = \overline{a_n}\overline{b_m}X^{m+n} + ... + \overline{a_0}\overline{b_0}$. Il faut maintenant justifier que $\overline{a_n}\overline{b_m} \neq \overline{0}$. Comme $\overline{a_m} \neq \overline{0}$ et que p est premier, on en déduit que $\overline{a_n}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$. Supposons que $\overline{a_n}\overline{b_m} = \overline{0}$, alors $\overline{b_m} = \overline{0}\overline{a_n}^{-1} = \overline{0}$. Contradiction. Donc $\overline{a_n}\overline{b_m} \neq \overline{0}$. Ce qui prouve donc que $\deg(\mathrm{PQ}) = \mathrm{m} + \mathrm{n} = \deg(\mathrm{P}) + \deg(\mathrm{Q})$.

(3) Montrer qu'il y a une division euclidienne dans $\mathbb{Z}/p\mathbb{Z}[X]$. C'est à dire pour tout $A, B \in \mathbb{Z}/p\mathbb{Z}[X]$ avec $B \neq 0$, il existe un couple $(Q, R) \in \mathbb{Z}/p\mathbb{Z}[X]$ tels que $A = BQ + R$ et $\deg(\mathrm{R}) < \deg(\mathrm{B})$. (Indication : si vous savez le faire dans $\mathbb{R}[X]$, vous savez le faire ici)

On fait une récurence sur $k = \deg(\mathrm{A}) - \deg(\mathrm{B})$.
— Pour $k < 0$, il suffit de choisir $Q = 0$ et $R = A$ et on a le résultat voulu.
— Supposons que le résultat est vrai pour un certain $k \in \mathbb{Z}$. Soient A et B tels que $\deg(\mathrm{A}) - \deg(\mathrm{B}) = \mathrm{k} + 1$. On note $A = \overline{a_n}X^n + \cdots + \overline{a_0}$ et $B = \overline{b_m}X^m + \cdots + \overline{b_0}$ avec $m - n = k + 1$. On pose $Q_0 = \overline{a_n}\overline{b_m}^{-1}X^{m-n}$ et $R_0 = A - Q_0B$.
On a alors que R_0 est de degré inférieur à k. D'après l'hypothèse de récurence, il existe Q_1, R_1 tels que $R_0 = Q_1B + R_1$ avec $\deg(\mathrm{R}_1) < \deg(\mathrm{B})$. On a alors

$$A = Q_0B + R_0 = Q_0B + Q_1B + R_1 = (Q_0 + Q_1)B + R_1$$

(4) Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$ et $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$. Montrer que si $P(\overline{k}) = \overline{0}$ alors il existe $Q \in \mathbb{Z}/p\mathbb{Z}[X]$ tel que $P = (X - \overline{k})Q$. En déduire qu'un polynôme de degré n a au plus n racines distinctes.

On effectue la division euclidiennet de P par $(X - \overline{k})$. Il existe Q, R tels que $P = (X - \overline{k})Q + R$ avec $\deg\mathrm{R} < 1$. Donc R est un polynôme constant. On calcule $R(\overline{k}) = P(\overline{k}) - (\overline{k} - \overline{k})Q(k) = \overline{0}$. Donc $P = (X - \overline{k})Q$.
Supposons P a m racines distinctes, $\overline{k_1}, \ldots, \overline{k_m}$ alors il existe Q tel que $P = (X - \overline{k_1})(X - \overline{k_2}) \cdots (X - \overline{k_m})Q$. Or

$$\deg(\mathrm{P}) = \deg(\mathrm{X} - \overline{\mathrm{k}_1}) + \deg(\mathrm{X} - \overline{\mathrm{k}_2}) + \cdots + \deg(\mathrm{X} - \overline{\mathrm{k}_\mathrm{m}}) + \deg(\mathrm{Q}) = \mathrm{m} + \deg(\mathrm{Q}) \geq \mathrm{m}$$

(5) On note $\mathcal{C}_p$ l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$, c'est à dire

$$\mathcal{C}_p = \left\{\overline{k} \in \mathbb{Z}/p\mathbb{Z} \,|\, \exists \overline{a} \in \mathbb{Z}/p\mathbb{Z}, \overline{k} = (\overline{a})^2\right\}$$

Montrer que $\mathcal{C}_p$ est de cardinal $\frac{p-1}{2}$.

Il y avait une erreur dans l'énoncé. L'ensemble $\mathcal{C}_p$ est l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$. (Sinon, il faut rajouter $+1$ car 0 est un carré)
On considère l'application $\psi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ définie par $\psi(\overline{k}) = \overline{k}^2$. On vérifie facilement que c'est un morphisme de $(\mathbb{Z}/p\mathbb{Z})^*$. Soit $\overline{k} \in \mathrm{Ker}(\psi)$. Alors $\overline{k}^2 = \overline{1}$, c'est à dire $(\overline{k} - \overline{1})(\overline{k} + \overline{1}) = \overline{0}$
Comme p est un nombre premier, cela implique que $\overline{k} = \overline{1}$ ou bien $\overline{k} = \overline{-1}$. Donc $|\mathrm{Ker}(\psi)| = 2$. D'après le théorème d'isomorphisme $|\mathrm{Im}(\psi)| = |(\mathbb{Z}/\mathrm{p}\mathbb{Z})^2|/2 = \frac{\mathrm{p}-1}{2}$.

(6) On considère le polynôme $P = X^{\frac{p-1}{2}} + \overline{-1}$. Montrer que pour tout $\overline{k} \in \mathcal{C}_p$ on a $P(\overline{k}) = \overline{0}$.

Soit $\overline{k} \in \mathcal{C}_p$ Il exite $\overline{j} \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $\overline{k} = \overline{j}^2$. Donc $P(\overline{k}) = (\overline{j}^2)^{\frac{p-1}{2}} + \overline{-1} = \overline{j}^{p-1}$. Or d'après le petit théorème de Fermat $\overline{j}^{p-1} = \overline{1}$, donc $P(\overline{k}) = \overline{0}$.

(7) En déduire que $\overline{-1} \in \mathcal{C}_p$ si et seulement si $\frac{p-1}{2}$ est pair.

Le polynôme P est de degré $\frac{p-1}{2}$. On en déduit que P a au maximum $\frac{p-1}{2}$ racines distinctes. Tous les éléments de $\mathcal{C}_p$ sont racines de P, donc les racines de P sont exactement les éléments de $\mathcal{C}_p$.
On en déduit que $\overline{-1} \in \mathcal{C}_p$ si et seulement si -1 est racine de P. Si $\frac{p-1}{2}$ est pair, on a directement $\overline{-1}^{\frac{p-1}{2}} = \overline{-1}^{2q} = \overline{1}$ et donc $\overline{-1}$ est racine de P. Et si $\frac{p-1}{2}$ est impair on a $\overline{-1}^{\frac{p-1}{2}} = \overline{-1}$ et donc $\overline{-1}$ n'est pas racine de P.

Exercice 3 (Facultatif)**.**

Le but est de montrer le théorème suivant :

Théorème (des deux carrés)**.**

Soit $p > 2$ un nombre premier.
Le nombre p s'écrit comme la somme de deux carrés (c'est à dire qu'il existe $a, b \in \mathbb{Z}$ tels que $a^2 + b^2 = p$) si et seulement si $p \equiv 1 \bmod(4)$

(1) Montrer que si p s'écrit comme la somme de deux carrés, alors $p \equiv 1 \bmod(4)$.

Supposons $p = a^2 + b^2$. Comme p est impair, on en déduit que a est pair et b est impair (ou inversement). Donc $a = 2k$ et $b = 2j + 1$. Donc $p = 4k^2 + 4j^2 + 4j + 1 = 4(k^2 + j^2 + j) + 1$. Donc $p \equiv 1 \bmod(4)$.

(2) Montrer que p est réductible dans $\mathcal{A}$ si et seulement si p s'écrit comme la somme de deux carrés.

Supposons que p est réductible dans $\mathcal{A}$. Alors il existe $z = a + ib, z' = a' + ib' \in \mathcal{A}$ non-inversibles tels que $p = zz'$. On a alors $p^2 = |p|^2 = |z|^2|z'|^2$. Or $|z|^2$ et $|z'|^2$ sont des entiers, différents de 1. Comme p est un nombre premier, on en déduit que $|z|^2 = |z'|^2 = p$. Donc $p = a^2 + b^2$.

(3) On suppose maintenant que $p \equiv 1 \bmod(4)$. Montrer que dans ce cas il existe $a \in \mathbb{Z}$ tel que $(a + i)(a - i) \in p\mathcal{A}$.

Si $p \equiv 1 \bmod(4)$ alors $\frac{p-1}{2}$ est pair, et donc -1 est un carré dans $(\mathbb{Z}/p\mathbb{Z})^2$. Donc il existe $\overline{a}$ tel que $\overline{a}^2 = -\overline{1}$. Donc $\overline{a}^2 + \overline{1} = \overline{0}$. On en déduit que $(a+i)(a-i) = a^2+1 \in p\mathbb{Z} \subset p\mathcal{A}$.

(4) En déduire que si p est irreductible dans $\mathcal{A}$ alors p divise 4.

Si p est irréductible dans $\mathcal{A}$ et $(a + i)(a - i) \in p\mathcal{A}$ alors d'après la question (7) de l'exercice 1, on a $(a + i) \in p\mathcal{A}$ ou $(a - i) \in p\mathcal{A}$. Si $(a + i) \in p\mathcal{A}$, alors $a - i = \overline{a + i} \in \overline{p}\mathcal{A} = p\mathcal{A}$. Donc à la fois $a + i$ et $a - i$ sont dans $p\mathcal{A}$.
Donc p divise $a + i$ et $a - i$. Donc p divise $(a + i) - (a - i) = 2i$. On en déduit que p divise 4.

(5) Conclure

On en déduit que si $p > 2$ est un nombre premier tel que $p \equiv 1 \bmod(4)$, et est irréductible alors p divise 4. Ce qui est une contradiction. Donc p n'est pas irréductible. Donc p s'écrit comme la somme de deux carrés.
En utilisant la question (1), le théorème est donc prouvé.