Licence MPCI, 2e année
Algèbre Générale

Devoir Maison
A rendre pour le Mercredi 24 avril

Le but du DM est de manipuler des anneaux sans avoir défini ce que c'est. Les deux premiers exercices sont indépendants. Le troisième exercice montre une très jolie conséquence des deux premiers exercices, et n'est donc pas du tout indépendant. Le troisième exercice est facultatif.

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.

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

(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 $\mathcal{A}$.

(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 $|r| < |y|$.

(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 $\mathbb{Z}$.)

(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 $I = z\mathcal{A}$.) .

(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 $y \in z\mathcal{A}$.

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 $(\overline{2}X^2 + \overline{4}X + \overline{4})(\overline{3}X^2 + \overline{4}X + \overline{1}) = X^4 + \overline{4}$.

(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 ...)

(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(R) < deg(B). (Indication : si vous savez le faire dans $\mathbb{R}[X]$, vous savez le faire ici)

(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.

(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 $\frac{p-1}{2}$.

(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 $P(\overline{k}) = \overline{0}$.

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

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 $p \equiv 1 \bmod(4)$

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

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

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

(5) Conclure