Licence de mathématiques
L3, parcours « enseignement » – arithmétique et groupes
contrôle partiel n° 2 du jeudi 23 novembre
durée 1h30

Ni documents, ni calculatrices, ni téléphones, ni ordinateurs ne sont autorisés.

Exercice 1 a) Soit $c \in \mathbb{R}$. Exprimer en fonction de c le reste de la division euclidienne de $X^4 - X^3 + X^2 - X + 1$ par $X^2 - cX + 1$ dans $\mathbb{R}[X]$.

Le reste est : $(c^3 - c^2 - c)X - c^2 + c + 1$. Ce reste est nul

$$\Leftrightarrow \begin{cases} c^3 - c^2 - c &= 0 \\ -c^2 + c + 1 &= 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} c(c^2 - c - 1) = 0 \\ c^2 - c - 1 = 0 \end{cases}$$

$$\Leftrightarrow c^2 - c - 1 = 0 \Leftrightarrow c = c_1 := \frac{1 - \sqrt{5}}{2} \text{ ou } c = c_2 := \frac{1 + \sqrt{5}}{2} \ .$$

. Donc $X^2 - c_1X + 1$ et $X^2 - c_2X + 1$ divisent $X^4 - X^3 + X^2 - X + 1$.

b) En déduire la factorisation du polynôme $X^4 - X^3 + X^2 - X + 1$ dans $\mathbb{R}[X]$.

Si $c = \frac{1 \pm \sqrt{5}}{2}$, le discriminant de $X^2 - cX + 1$ est $c^2 - 4 = \frac{-5 \pm \sqrt{5}}{2} < 0$. Donc les polynômes $X^2 - c_1X + 1$ et $X^2 - c_2X + 1$ sont irréductibles sur $\mathbb{R}$. Comme $c_1 \neq c_2$, ils sont premiers entre eux donc

$$X^4 - X^3 + X^2 - X + 1 = (X^2 - c_1X + 1)(X^2 - c_2X + 1)$$

est la factorisation dans $\mathbb{R}[X]$.

c) Exprimer les racines complexes de $X^4 - X^3 + X^2 - X + 1$. Soit $x \in \mathbb{C}$. On a :

$$x^4 - x^3 + x^2 - x + 1 = 0 \Leftrightarrow (x^2 - c_1x + 1)(x^2 - c_2x + 1) = 0$$

$$\Leftrightarrow x^2 - c_1x + 1 = 0 \text{ ou } x^2 - c_2x + 1 = 0$$

or,

$$c_1^2 - 4 = \left(i\sqrt{\frac{5 - \sqrt{5}}{2}}\right)^2, \ c_2^2 - 4 = \left(i\sqrt{\frac{5 + \sqrt{5}}{2}}\right)^2,$$

donc

$$x^4 - x^3 + x^2 - x + 1 = 0 \Leftrightarrow x = \frac{1-\sqrt{5}}{2} \pm i\sqrt{\frac{5-\sqrt{5}}{2}} \text{ ou } \frac{1+\sqrt{5}}{2} \pm i\sqrt{\frac{5+\sqrt{5}}{2}}$$

Exercice 2 Trouver deux polynômes à coefficients rationnels $U(X), V(X)$ tels que

$$U(X)(X^5+1) + V(X)(X^4+1) = 1$$

dans $\mathbb{Q}[X]$.

On applique l'algorithme d'Euclide à $P = X^5+1$, $Q = X^4+1$:

$$P = QX - X + 1,\ Q = (-X+1)(-X^3 - X^2 - X - 1) + 2$$

$$\Rightarrow 1 = \frac{1}{2}Q + (-X+1)\frac{X^3+X^2+X+1}{2}$$

$$= \frac{1}{2}Q + (P - QX)\frac{X^3+X^2+X+1}{2}$$

$$= Q(-X\frac{X^3+X^2+X+1}{2} + \frac{1}{2}) + P\frac{X^3+X^2+X+1}{2}$$

$$= Q\underbrace{\frac{-X^4-X^3-X^2-X+1}{2}}_{:=V} + P\underbrace{\frac{X^3+X^2+X+1}{2}}_{:=U}$$

Exercice 3 a) Quel est l'ordre de 5 dans le groupe $(\mathbb{Z}/64\mathbb{Z}, +)$?64 car 5 est premier avec $64 = 2^6$.

b) Quel est l'ordre du groupe $((\mathbb{Z}/64\mathbb{Z})^*, \cdot)$? Quel est l'ordre de 5 dans $((\mathbb{Z}/64\mathbb{Z})^*, \cdot)$?
$|(\mathbb{Z}/64\mathbb{Z})^*| = \varphi(64) = 2^6 - 2^5 = 32$, et :

$5^2 = 25$, $5^4 = 625 = -15 \bmod 64$, $5^8 = 15^2 = 225 = 33 \bmod 64$, $5^{16} = 1089 = 1 \bmod 64$

donc 5 est d'ordre 16 dans le groupe multiplicatif.

c) Montrer que pour tout $k \in \mathbb{Z}$, $5^k \neq -1 \bmod 64$. *Indication. Raisonner modulo 4.* $5 = 1 \bmod 4 \Rightarrow \forall\, k \in \mathbb{Z},\ 5^k = 1 \bmod 4 \Rightarrow 5^k \neq -1 \bmod 4 \Rightarrow 5^k \neq -1 \bmod 64$ car $4|64$.

d) En déduire que l'application

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \to (\mathbb{Z}/64\mathbb{Z})^*,\ (\epsilon, k) \mapsto (-1)^\epsilon 5^k$$

est un isomorphisme de groupes.

C'est un morphisme bien défini car -1 est d'ordre 2 et 5 d'ordre 16. C'est injectif car $(-1)^\epsilon 5^k = 1 \Leftrightarrow 5^k = (-1)^\epsilon \bmod 64 \Rightarrow 5^k = 1 \bmod 64$ (car $5^k \neq -1$) $\Rightarrow 16|k$ car 5 d'ordre 16 et donc $(-1)^\epsilon = 1 \Rightarrow 2|\epsilon$. D'où $\epsilon = 0 \bmod 2$, $k = 0 \bmod 16$.

e) Le groupe $((\mathbb{Z}/64\mathbb{Z})^*, \cdot)$ est-il cyclique ? *Justifier votre réponse.*

Non car $\forall\ x \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, $16x = 0$ donc l'ordre de x divise 16. Donc $\mathbb{Z}/64\mathbb{Z})^*$ n'a pas d'éléments d'ordre 32.

Exercice 4 a) Rappeler la définition de la signature d'une permutation $\sigma \in \mathfrak{S}_n$.

$\epsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}$.

b) Pour tout diviseur de d de 24, déterminer le nombre d'éléments d'ordre d dans $\mathfrak{S}_4$. Il y a

— 1 élément d'ordre 1,

— 9 d'ordre 2 : les 6 transpositions et les 3 doubles-transpositions,

— 8 d'ordre 3 : les 8 3−cycles,

— 6 d'ordre 4 : les 6 4−cycles.

— 0 élément d'ordre 6, 8, 12 ou 24.

c) Soit $G = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Quel est l'ordre de G ? $|G| = (3^2 - 1)(3^2 - 3) = 48$.

d) Montrer que le morphisme dét : $G \to (\mathbb{Z}/3\mathbb{Z})^*$ est surjectif. $\forall a \in (\mathbb{Z}/3\mathbb{Z})^*$, $\det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a$. En déduire l'ordre du groupe $S = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) = \{g \in G \ :\ \det g = 1\}$. $|G/S| = |(\mathbb{Z}/3\mathbb{Z})^*| = 2 \Rightarrow |S| = 24$.

e) Déterminer l'ordre de la matrice $A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in S$. Les groupes S et $\mathfrak{S}_4$ sont-ils isomorphes ? *Justifier.*

$$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ A^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ A^6 = 1$$

donc A est d'ordre 6. Donc S n'est pas isomorphe à $\mathfrak{S}_4$ qui n'a pas d'élément d'odre 6.