I. On utilise la notion usuelle P' pour la dérivée d'un polynôme $P \in \mathbf{R}[X]$. Considérons les sous-ensembles de $\mathbf{R}[X]$

$$A = \{P \in \mathbf{R}[X] \mid P(0) = 0\},$$
$$B = \{P \in \mathbf{R}[X] \mid P'(0) = 0\},$$
$$C = \{P \in \mathbf{R}[X] \mid P(0) = P'(0) = 0\}.$$

(a) Est-ce que A, B et C sont des idéaux de $\mathbf{R}[X]$? Si oui, quels seraient leurs générateurs ? Expliquer

(b) Est-ce que A, B et C sont des sous-anneaux [redacted] de $\mathbf{R}[X]$? Expliquer

a) • I : idéal de l'anneau A

① $(I, +)$ sous-groupe $(A, +)$

② $\forall x \in I, a \in A$, $\begin{cases} x \cdot a \in I \\ a \cdot x \in I \end{cases}$

• $A = \{P \in \mathbb{R}[X] : P(0) = 0\}$.

① $(A, +)$ sous-groupe de $(\mathbb{R}[X], +)$.

• $e_G \in H$

• $\forall x, y \in H$, $x * y^{-1} \in H$.

Soit $P, Q \in A$

$(P + Q^{-1})(0)$

$= (P - Q)(0)$

$= P(0) - Q(0)$

$= 0 - 0 = 0$

donc $P * Q^{-1} \in A$

2. Soit $P \in A$, $Q \in \mathbb{R}[x]$

$(PQ)(0) = P(0)\,Q(0)$

$= 0 \times Q(0)$

$= 0$. donc $PQ \in A$.

donc A est un idéal de $\mathbb{R}[X]$.

③ $P = \sum_{k=0}^{n} a_k X^k$

$P(0) = a_0 = 0$

donc $P = a_1 X + a_2 X^2 + \dots + a_n X^n$

$= X(a_1 + a_2 X + \dots + a_n X^{n-1})$

$= X \underbrace{Q}_{\deg\, n-1}$

et si $P = XQ$ alors $P(0) = 0$ et $P \in A$

$P \in A \iff X \mid P \iff P \in \langle X \rangle$

Donc $A = \langle X \rangle$.

5) $A = \langle X \rangle \neq \mathbb{R}[X]$

donc $\underset{\mathbb{R}[X]}{1} \notin A$.

$1 \in I \Rightarrow I =$ anneau

donc A n'est pas un sous-anneau de $\mathbb{R}[X]$.

$(A, +, \times)$ anneau et $B \subset A$.

on dit que B sous-anneau de A si $(B, +)$ sous-groupe.
et $(B, \times)$ stable

- $1_A \in B$
- $\forall x, y \in B, \; x - y \in B$
- $\forall x, y \in B, \; x \times y \in B$

- A idéal on a $(A, +)$ sous-groupe de $(\mathbb{R}[X], +)$

- Soit $P, Q \in A$

$(PQ)(0) = P(0) \times Q(0) = 0 \times 0 = 0$

donc $P \times Q \in A$.

ok mais
pas sous-anneau

II. Considérons la permutation $\sigma \in S_6$ donnée par $\sigma = (1\,2\,3)\,(3\,5\,4\,1)\,(2\,4\,3)$.

(a) Ecrire σ comme un produit de cycles à supports disjoints.

(b) Quel est l'ordre de σ ? Quelle est la signature $\varepsilon(\sigma)$ de σ ? H.W

III. (a) L'application $i\colon \mathbf{R}^* \to \mathbf{R}$ avec formule $i(x) = x$ (l'inclusion de $\mathbf{R}^*$ dans $\mathbf{R}$) est-elle un morphisme de groupes ? Quel ~~serait son~~ noyau ?

(b) L'application $f\colon \mathbf{R}^* \to \mathbf{R}$ avec formule $f(x) = \ln|x|$ est-elle un morphisme de groupes ? Quel serait son noyau ?

IV. Soit $\phi\colon G \to H$ un morphisme de groupes. Démontrer que ϕ *est injectif si et seulement si on a* $\ker\phi = \{e\}$. ✓

exercice 3 :

$\forall\, x, y \in (G, *)$ et

$\phi : (G, *) \longrightarrow (H, \Delta)$

$\phi(x * y) = \phi(x)\, \Delta\, \phi(y)$

a) $i : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}, +)$

$x \longmapsto x$

brouillon :

$$i(x \times y) = xy$$

$$i(x) + i(y) = x + y$$

$$\Rightarrow \quad xy = x + y$$

$$\underbrace{2 \times 3}_{6} = \underbrace{2 + 3}_{5}$$

Non car $i(2 \times 3) = 6$ et $i(2) + i(3) = 5$, donc

$$i(2 \times 3) \neq i(2) + i(3)$$

donc i n'est pas un morphisme de groupe.

3) $f : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}, +)$

$$x \longmapsto \ln|x|$$

Soit $x, y \in (\mathbb{R}^*, \times)$

$$f(x \times y) = \ln|x \times y|$$

$$= \ln|x| + \ln|y|$$

$$= f(x) + f(y).$$

donc f est un morphisme de groupe.

$$\ker(f) = \{x \in \mathbb{R}^*,\ \ln|x| = 0\}$$

$$= \{-1 ; 1\}.$$

- $g : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$

$$x \longmapsto \exp(x)$$

Soit $x, y \in (\mathbb{R}, +)$

$$g(x+y) = e^{x+y}$$

$$= e^x \times e^y$$

$$= g(x) \times g(y)$$

donc g est un morphisme de groupe

$$\ker(g) = \{ x \in \mathbb{R} : \exp(x) = 1 \}$$

$$= \{0\}.$$

V. Quels sont les 2 derniers chiffres (de dizaines et d'unités) dans le développement décimal de 30303^{444} ?

. $30\,303 \equiv 3 \mod 100$

donc

$$30\,303^{444} \equiv 3^{444} \mod 100$$

Théorème Euler :

si $\mathrm{pgcd}(a,n) = 1$, alors

$$a^{\varphi(n)} \equiv 1 \mod n$$

Théorème Fermat :

si p premier et $\mathrm{pgcd}(a,p) = 1$
alors

$$a^{p-1} \equiv 1 \mod p$$

car pgcd $(3; 100) = 1$,

donc d'après le théorème d'Euler on a :

$$3^{\boxed{\varphi(100)}} \equiv 1 \mod (100).$$

$$100 = 2^2 \times 5^2$$

$$\varphi(100) = \varphi(2^2) \times \varphi(5^2)$$

$$= (2^2 - 2^1) \times (5^2 - 5^1)$$

$$= 100 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$

Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ p_i premier

alors $\varphi(n) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$

$$= n \times \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

$$\varphi(100) = 2 \times 20 = 40$$

donc $3^{40} \equiv 1 \mod (100)$

$$444 = 40 \times 11 + 4$$

Ainsi :

$$3^{444} = 3^{40 \times 11 + 4}$$

$$= \left(3^{40}\right)^{11} \times 3^4$$

$$\equiv 3^4 \mod 100$$

$$\equiv 81 \mod 100$$

exercice :

2 derniers chiffres de

$70\,707^{222}$