

## DM 29 : ensembles multiplicatifs.

**Il s'agit d'un sujet supplémentaire pour votre travail personnel.**

**Il n'est pas à rendre.**

**Un corrigé sera fourni à la fin des vacances.**

On dira qu'un sous-ensemble  $S$  d'un anneau  $A$  est multiplicatif si et seulement si, pour tout  $(r, s) \in S^2$ ,  $rs \in S$ .

Pour tout entier  $n \geq 1$ , on note  $S_n(A)$  l'ensemble des éléments  $x$  de l'anneau  $A$  qui peuvent s'écrire sous la forme  $x = x_1^2 + \cdots + x_n^2$ , avec  $x_1, \dots, x_n$  dans  $A$ .

Si  $k$  est un sous-corps de  $\mathbb{C}$ ,  $k[X]$  et  $k(X)$  désignent respectivement l'anneau des polynômes et le corps des fractions rationnelles à coefficients dans  $k$ .

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$  ont les significations habituelles.

### Partie I

1°) Soient  $x, y, z, t$  quatre éléments d'un sous-anneau  $B$  du corps  $\mathbb{R}$  des réels. En écrivant que

$$(*) \quad |x + iy|^2 \cdot |z + it|^2 = |(x + iy)(z + it)|^2,$$

démontrer que  $S_2(B)$  est un ensemble multiplicatif.

2°) L'égalité  $(*)$  peut être regardée comme une identité dans l'anneau  $B$  en les lettres  $x, y, z, t$ . Enoncer cette identité et la démontrer dans un anneau commutatif quelconque  $A$ . En déduire que  $S_2(A)$  est un ensemble multiplicatif.

3°)

a) Montrer que le carré d'un entier relatif est congru à 0 ou à 1 modulo 4.

b) Supposons qu'il existe  $(x_1, x_2, x_3) \in \mathbb{Z}^3$  tel que  $15 = x_1^2 + x_2^2 + x_3^2$ .

Montrer que  $x_1, x_2$  et  $x_3$  sont impairs.

c) Montrer que  $15 \notin S_3(\mathbb{Z})$  et en déduire que  $S_3(\mathbb{Z})$  n'est pas un ensemble multiplicatif.

4°) On note  $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{7}$  les huit éléments de l'anneau  $E = \mathbb{Z}/8\mathbb{Z}$ . Donner sans justification la liste des éléments de chacun des trois ensembles  $S_1(E)$ ,  $S_2(E)$  et  $S_3(E)$ .

5°) Soient  $a, b, c, d$  dans  $\mathbb{Z}$  tels que  $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{8}$ .

Déduire de la question précédente que ces quatre nombres sont tous pairs.

6°) En déduire que, si  $n \in \mathbb{Z}$  est congru à  $-1$  modulo 8, alors  $n$  n'appartient ni à  $S_3(\mathbb{Z})$ , ni à  $S_3(\mathbb{Q})$ .

7°) L'ensemble  $S_3(\mathbb{Q})$  est-il multiplicatif?

8°) Soit  $f \in \mathbb{R}[X]$  tel que, pour tout  $x \in \mathbb{R}$ ,  $f(x) \geq 0$ .

a) Si  $f$  est de degré 2, montrer que  $f \in S_2(\mathbb{R}[X])$ .

b) Pour  $f$  de degré quelconque, montrer que les racines réelles de  $f$  sont de multiplicités paires, puis montrer que  $f \in S_2(\mathbb{R}[X])$ .

c) Montrer que  $S_2(\mathbb{R}[X]) = \{g \in \mathbb{R}[X] / \forall x \in \mathbb{R} \ g(x) \geq 0\}$ .

9°) Démontrer que pour tout  $n \geq 3$ , on a  $S_n(\mathbb{R}[X]) = S_2(\mathbb{R}[X])$ .

A-t-on aussi  $S_n(\mathbb{R}(X)) = S_2(\mathbb{R}(X))$ ?

## Partie II

Dans cette partie,  $k$  désigne un corps commutatif quelconque. On notera 0 et 1 ses éléments neutres.

◇ On appelle caractéristique de  $k$  et on note  $\text{car}(k)$  le plus petit entier  $n \geq 1$  tel que  $n.1 = 0$ , si un tel entier  $n$  existe. Dans le cas contraire, on pose  $\text{car}(k) = 0$ .

◇ On appelle niveau de  $k$  et on note  $s(k)$  le plus petit entier  $n \geq 1$  tel que  $-1 \in S_n(k)$ , si un tel entier  $n$  existe. Dans le cas contraire, on pose  $s(k) = +\infty$ .

**On admet pour la suite du problème que, si  $k$  est un corps commutatif de caractéristique nulle, et si  $n$  est une puissance de 2, alors  $S_n(k)$  est un ensemble multiplicatif.**

1°) Calculer la caractéristique et le niveau des corps  $\mathbb{R}$  et  $\mathbb{C}$ .

2°) a) Si  $p$  est un nombre premier, calculer la caractéristique du corps  $\mathbb{Z}/p\mathbb{Z}$ .

b) Quel est le niveau d'un corps de caractéristique 2? d'un corps de caractéristique 5?

3°) On pose  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , où  $p$  est un nombre premier  $\geq 3$ .

a) Quel est le noyau du morphisme  $x \mapsto x^2$  du groupe multiplicatif  $\mathbb{F}_p^*$  des éléments non nuls du corps  $\mathbb{F}_p$  dans lui-même?

b) Notons  $A = \{\bar{1}, \bar{2}, \dots, \overline{\left(\frac{p-1}{2}\right)}\}$ .

Montrer que  $A$  et  $-A$  constituent une partition de  $\mathbb{F}_p^*$  (où  $-A = \{-x/x \in A\}$ ).

On note  $E$  l'image du morphisme étudié au 3.a.

Montrer que l'application 
$$\begin{array}{ccc} A & \longrightarrow & E \\ x & \longmapsto & x^2 \end{array}$$
 est une bijection.

c)  $T$  désignant l'ensemble des éléments de  $\mathbb{F}_p$  de la forme  $-1 - y$

avec  $y \in S_1(\mathbb{F}_p) = E \cup \{0\}$ , démontrer que l'intersection  $T \cap S_1(\mathbb{F}_p)$  n'est pas vide.

d) En déduire que  $s(\mathbb{F}_p) \leq 2$ .

4°) On suppose que  $k$  est un corps (fini ou infini) de caractéristique  $n$  non nulle.

a) Montrer que l'application  $\bar{h} \mapsto h.1$  est un morphisme d'anneaux injectif

de  $\mathbb{Z}/n\mathbb{Z}$  dans  $k$ .

b) En déduire que  $n$  est un nombre premier.

c) Montrer que  $s(k) \leq 2$ .

5°) On suppose, dans cette question, que le corps  $k$  est de caractéristique nulle et de niveau  $s \neq +\infty$ . Il existe donc  $x_1, \dots, x_s$  dans  $k$  tels que  $-1 = x_1^2 + \dots + x_s^2$ .

Soit  $n$  la plus grande puissance de 2 telle que  $n \leq s$  et soit  $x = x_1^2 + \dots + x_n^2$ .

Etablir que  $x \neq 0$ , puis successivement que  $-x, -x^2$  et  $-1$  appartiennent à  $S_n(k)$ .

6°) Démontrer que le niveau d'un corps commutatif quelconque est égal ou bien à  $+\infty$  ou bien à une puissance de 2.

## Partie III

Dans cette partie,  $k$  désigne un sous-corps de  $\mathbb{C}$ . On note  $A = k[X]$  et  $K = k(X)$ , de sorte que  $k \subset A \subset K$ .

1°) Démontrer que  $S_1(A) = A \cap S_1(K)$ .

2°) On fixe un entier  $n$  avec  $n \geq 2$ .

Soient  $a_1, \dots, a_{n-1}, b$  dans  $K$ . Simplifier l'expression  $(b+1)^2 + \sum_{i=1}^{n-1} (a_i(b-1))^2$  lorsque

$$\sum_{i=1}^{n-1} a_i^2 = -1.$$

3°) En déduire que, s'il existe  $n \geq 2$  tel que  $-1 \in S_{n-1}(k)$ , alors  $S_n(k) = k$ ,  $S_n(A) = A$  et  $S_n(K) = K$ .

4°) Pour quels entiers  $n \geq 1$  les ensembles  $S_n(\mathbb{C}(X))$  sont-ils multiplicatifs?

5°) Soit  $n$  un entier tel que  $n \geq 2$  et  $-1 \notin S_{n-1}(k)$ .

Soient  $R_1, \dots, R_n$  des polynômes dans  $A$ .

Démontrer que si  $R_1^2 + \dots + R_n^2 = aX$  avec  $a \in k$ , alors  $R_1, \dots, R_n$  sont tous nuls.

6°) Soient  $P, Q, P_1, \dots, P_n, Q_1, \dots, Q_n$  dans  $A$ , où on a encore  $n \in \mathbb{N}$  avec  $n \geq 2$ .

On pose  $S = P - \sum_{i=1}^n Q_i^2$ ,  $T = PQ - \sum_{i=1}^n P_i Q_i$ ,  $Q' = 2T - QS$  et  $P'_i = 2Q_i T - P_i S$  pour tout  $i \in \{1, \dots, n\}$ .

a) Démontrer que, si l'on a l'égalité :

$$(1) \quad Q^2 P = \sum_{i=1}^n P_i^2,$$

alors on a aussi les deux égalités :

$$(2) \quad Q'^2 P = \sum_{i=1}^n P_i'^2 \text{ et}$$

$$(3) \quad QQ' = \sum_{i=1}^n (P_i - QQ_i)^2.$$

b) On suppose, outre l'égalité (1), que  $-1 \notin S_{n-1}(k)$ , que  $Q \neq 0$  et que  $Q' = 0$ . Prouver l'égalité :

$$(4) \quad P = \sum_{i=1}^n Q_i^2.$$

*Indication* : on pourra utiliser la question 5 avec  $a = 0$ .

7°) Soit  $n \geq 2$  tel que  $-1 \notin S_{n-1}(k)$  et soient  $P, Q, P_1, \dots, P_n$  dans  $A$  vérifiant l'égalité (1) ci-dessus et les conditions

$$(5) \quad PQ \neq 0 \text{ et } \deg(Q) \geq 1.$$

Démontrer que l'on peut trouver  $Q'', P_1'', \dots, P_n''$  dans  $A$  vérifiant

$$(6) \quad Q''^2 P = \sum_{i=1}^n P_i''^2 \text{ et}$$

$$(7) \quad PQ'' \neq 0 \text{ et } \deg(Q'') < \deg(Q).$$

*Indication* : on pourra utiliser la question précédente en prenant pour  $Q_i$  le quotient de la division euclidienne de  $P_i$  par  $Q$ .

8°) Démontrer que, pour tout  $n \geq 1$ , on a  $S_n(A) = A \cap S_n(K)$ .

9°) a) Démontrer que les corps  $k$  et  $K$  ont le même niveau.

b) En supposant que ce niveau commun  $s$  est fini, démontrer que  $S_s(K) \neq S_{s+1}(K)$ .

10°) Etablir que, si  $n$  est une puissance de 2, alors l'ensemble  $S_n(A)$  est multiplicatif.