DM n°9

Pour le 1e février.

EXERCICE I —Entiers de Gauss —

Les élèves intéressés, compléteront par l'exercice 38.

Soient $\mathbf{Z}[i]$ l'ensemble des nombres complexes de la forme $u+iv$, avec $(u,v)\in\mathbf{Z}^2$ et l'application. $\varphi\,;\,\mathbf{Z}[i]\to\mathbf{N}\,;\;a\mapsto\bar{a}a$.

1. Montrer que $\mathbf{Z}[i]$ est un sous-anneau du corps $\mathbf{C}$.
2. Déterminer $\mathbf{Z}[i]^*$, ensemble des éléments inversibles de $\mathbf{Z}[i]$.
3. Montrer que pour tout élément a de $\mathbf{Z}[i]$ et tout élément b de $\mathbf{Z}[i]\setminus\{0\}$, il existe un couple (non nécessairement unique) (q,r) d'éléments de $\mathbf{Z}[i]$ tel que $a=bq+r$ et $\varphi(r)<\varphi(b)$. On dit que l'anneau $\mathbf{Z}[i]$ est euclidien pour φ.
4. Montrer que tout idéal de $\mathbf{Z}[i]$ est de la forme $a\mathbf{Z}[i]$, on dit que $\mathbf{Z}[i]$ est principal.
5. Soit a un élément de $\mathbf{Z}[i]$. Montrer que si $\varphi(a)$ est premier, alors a est un élément irréductible de $\mathbf{Z}[i]$.

   Rappelons qu'un élément a d'un anneau intègre est dit irréductible si par définition il n'est pas inversible et si il admet la décomposition $a=bc$, alors a ou b est inversible.

PROBLÈME I —Extentions de corps —

Les élèves intéressés, compléteront par le DM supplémentaire des vacances de Noël.

Première partie : Un exemple d'extension du corps $\mathbf{Q}$

1. Soit P le polynôme X^3-X-1.
   Montrer que P n'a pas de racines rationnelles. En déduire que P est irréductible dans $\mathbf{Q}[X]$.
   Montrer que P a une racine réelle que l'on notera ω.
2. Soit $\mathbf{K}$ le $\mathbf{Q}$-espace vectoriel engendré par $(\omega^i)_{i\in\mathbf{N}}$.
   Montrer que $\mathbf{K}$ est de dimension finie, et donner une base simple de K.
3. Montrer que $\mathbf{K}$ est une $\mathbf{Q}$-sous-algèbre de $\mathbf{R}$, muni de sa structure naturelle de $\mathbf{Q}$-algèbre.
4. Montrer que $\mathbf{K}$ est un sous-corps de $\mathbf{R}$.

Deuxième partie : Cas général d'extension de $\mathbf{Q}$

Soit a un réel.

1. Montrer que tout sous-corps de $\mathbf{R}$ contient $\mathbf{Q}$.
2. Montrer que l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a admet un plus petit élément pour l'inclusion. On le notera dans la suite $\mathbf{Q}(a)$.
3. Montrer que $\phi\;:\;\mathbf{Q}[X]\to\mathbf{R}\,;\;P\mapsto P(a)$ est un morphisme de la $\mathbf{Q}$-algèbres $\mathbf{Q}[X]$ dans la $\mathbf{Q}$ algèbre $\mathbf{R}$. On note $\mathbf{Q}[a]$ son image.
4. Soit $I:=\{P\in\mathbf{Q}\,[X]\,,P\,(a)=0\}$. Montrer que I est un idéal de $\mathbf{Q}[X]$.

5. Le réel a est dit algébrique (sur $\mathbf{Q}$), si, par définition, a est racine d'un polynôme non nul à coefficients entiers.
   Montrer que a est algèbrique si et seulement si I est non réduit à $\{0\}$.
   Dans cette partie on suppose dans la suite que que a est algèbrique, sauf à la dernière question.
6. Montrer qu'il existe un et un seul élément de $\mathbf{Q}[X]$ unitaire, μ_a, tel que $I = \mu_a\mathbf{Q}[X]$.
   Montrer que μ_a est irréductible dans $\mathbf{Q}[X]$. Montrer que si a est irrationnel, alors le degré de μ_a est supérieur ou égal à 2. Déterminer μ_a pour $a = \sqrt{2}$ et pour $a = \sqrt{\frac{1+\sqrt{5}}{2}}$.
7. Montrer que $\mathbf{Q}[a]$ est un corps. Montrer que $\mathbf{Q}(a) = \mathbf{Q}[a]$.
   Montrer que $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension n, où n est le degré de μ_a, dont on donnera une base simple.
8. Si a est non algébrique, montrer qu'alors $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension infinie [1].

PROBLÈME II

Dans tout le problme, p désigne un nombre premier strictement supérieur à 3, $\mathbf{Z}_p$ l'anneau quotient $\mathbf{Z}/p\mathbf{Z}$.

Si A est un anneau fini, d'élément unité e, on appelle ordre d'un élément inversible a de A, le plus petit entier strictement positif ω tel que $a^\omega = e$.

Pour toute matrice carrée M à coefficients dans un corps, on note $\Delta(M)$ son déterminant et $T(M)$ sa trace.

Les 3/2 vérifieront que pour tout élément M de $\mathcal{M}_2(\mathbf{R})$, on a : $\chi_M(M) = 0_2$ (Théorème de Caylay-Hamilton).

I

1. Soit A_p l'ensemble des matrices à coefficient dans $\mathbf{Z}_p$ de la forme

$$R = \lambda M + \mu I,$$

   où

$$\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix},\ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

   et λ et μ sont des éléments de $\mathbf{Z}_p$.
   Montrer que A_p est un anneau commutatif pour l'addition et la multiplication des matrices usuelles.
   Donner le nombre d'éléments de A_p.
2. Calculer $T(R)$ et $\Delta(R)$ pour R dans A_p. Exprimer $T(R^2)$ et $\Delta(R^2)$ en fonction de $T(R)$ et $\Delta(R)$.
3. Montrer que deux quelconques des conditions suivantes impliquent la troisième :
   i. T(R)=0.
   ii. $\Delta(R) = 1$.
   iii. L'ordre de R est 4.
4. On considère la suite d'entiers $(Y_k)_{k\in N}$, définie par

$$Y_0 = 2 \text{ et } Y_{k+1} = 2Y_k^2 - 1.$$

   , Comparer Y_k et $T(M_k)$, pour tout entier naturel k.

1. On pourrait montrer que $\mathbf{Q}(a)$ est isomorphe en tant que corps au corps $\mathbf{Q}(X)$.

5. Montrer que pourtout entier naturel k, l'ordre de M est 2^k si et seulement si p divise Y_{k-2}.

II

1. Montrer que A_p est un corps si et seulement si $\bar{3}$ n'est pas le carré d'un élément de $\mathbf{Z}_p$.
2. Dans cette question, on suppose que $\bar{3}$ est un carré dans $\mathbf{Z}_p$: $\bar{3} = a^2$, où $a \in \mathbf{Z}_p$). Montrer que M est semblable à une matrice diagonale. En déduire que A_p est isomorphe à l'anneau produit $\mathbf{Z}_p \times \mathbf{Z}_p$, puis donner le nombre des éléments de A_p de déterminant 1, ainsi que celui de ses éléments inversibles.
3. Dans cette question, on suppose que $\bar{3}$ n'est pas un carré dans $\mathbf{Z}_p$.
   (a) Montrer que Δ donne un homomorphisme du groupe multiplicatif des éléments non nuls de A_p dans celui des éléments non nuls de $\mathbf{Z}_p$. En déduire que le nombre des éléments de l'image de Δ est un diviseur de $p-1$ et que celui des éléments du noyau de Δ est un multiple de $p+1$.
   (b) Vérifier que, pour tout $\lambda \in \mathbf{Z}_p$, il y a au plus deux éléments μ de $\mathbf{Z}_p$ tels que $\Delta(\lambda M + \mu I) = 1$

   Donner alors de nombre des éléments de A_p de déterminant 1.
4. Montrer que l'ordre de M divise le nombre des éléments de A_p de déterminant 1.
   En déduire que, si p divise Y_{k-2} alors 2^k divise $p-1$ ou $p+1$.