DM n$^{\mathrm{o}}$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'$A_p$plication. $\varphi\,;\ \mathbf{Z}[i] \to \mathbf{N}\,;\ a \mapsto \bar{a}a$.

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 problème, 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 $A_p$pelle 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.

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

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.

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 $p+1$.

indication pour le DM n°9

Pour le 1e février.

EXERCICE I —Entiers de Gauss —

1. Sans problème.
2. Si Z est inversible dans $\mathbf{Z}[i]$, alors φ est inversible dans l'anneau $\mathbf{Z}$ donc vaut 1. On trouve sans mal les élément de $\mathbf{Z}[i]$ de module 1 et l'on montre instantanément qu'ils sont inversibles...
3. Le complexe $\frac{a}{b}$ est élément d'un carré de côté 1 dont les sommest sont des entier de Gauss, prendre pour q le ou l'un des sommest plus proche de $\frac{b}{a}$...
4. cf. sous-groupes de $\mathbf{Z}$ ou idéaux de $\mathbf{K}[X]$.
5. Résulte directement de $\varphi(bc) = \varphi(b)\varphi(c)$ ...

Complément éventuel

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.

6 Soit p un nombre premier impair et y un élément de $(\mathbf{Z}/p\mathbf{Z})^*$, on dit que y est un carré s'il existe un élément z de $(\mathbf{Z}/p\mathbf{Z})^*$ tel que $z^2 = y$.

1. Montrer que $\displaystyle\prod_{x\in(\mathbf{Z}/p\mathbf{Z})^*} x = \begin{cases} -y^{\frac{p-1}{2}}, & \text{si } y \text{ est un carré,} \\ y^{\frac{p-1}{2}}, & \text{sinon .} \end{cases}$

   Indication : on pourra regrouper deux à deux dans le produit les termes x et yx^{-1}.
2. En déduire
$$\begin{cases} y^{\frac{p-1}{2}} = \bar{1}, & \text{si } y \text{ est un carré,} \\ y^{\frac{p-1}{2}} = -\bar{1}, & \text{sinon .} \end{cases}$$

7 Soit p un nombre premier, impaire OU NON. Montrer l'équivalence entre les propriétés suivantes :

i. p est irréductible dans $\mathbf{Z}[i]$;
ii. $p \equiv 3$ [4] ;
iii. Il n'existe pas d'élément a de $\mathbf{Z}[i]$ tel que $p = \phi(a)$.

8 En déduire les irréductibles de $\mathbf{Z}[i]$.

PROBLÈME I —Extentions de corps —

Extensions de corps

Première partie

1. Donc on déduit (cf. exercice du cours) que les seules racines rationnelles possibles sont 1 et -1. Or $P(1) = -1$, $P(-1) = -1$. Donc P n'admet pas de racines rationnelles.

   Le polynôme P est de degré *impair* à coefficients *réels*, il admet donc une racine réelle ω.

2. Soit c un élément de $\mathbf{K}$. Par définition de $\mathbf{K}$, il existe un entier naturel n et des rationnels $a_0, a_1, \ldots, a_n$ tels que : $c = \sum_{i=0}^{n} a_i \omega^i$. Soit l'élément de $\mathbf{Q}[X]$, $C = \sum_{i=0}^{n} a_i X^i$. Faire la division euclidienne de C par P dans $\mathbf{Q}[X]$ on obtient que $\mathbf{K}$ est le Q-espace vectoriel engendré par la sous famille de $(\omega^i)_{i\in\mathbf{N}}$, $(\omega^0, \omega^1, \omega^2)$.

   La famille $(\omega^0, \omega^1, \omega^2)$ est libre. Soit λ, μ et ν des rationnels tels que : $\lambda\omega^2 + \mu\omega + \nu = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda X^2 + \mu X + \nu$. Supposons C non nul. Alors par division euclidienne : $P = \tilde{Q}C + uX + v$ avec $\tilde{Q} \in \mathbf{Q}[X]$, u et v des rationnels. En substituant dans cette égalité ω à l'indéterminée....

   Finalement $\underline{(\omega^0, \omega^1, \omega^2) \text{ est une base de } K}$.

3. après K est *stable par combinaison linéaire.*
   après K *est stable par produit.*
   après Enfin $1 = \omega^0 \in K$.
   De ces trois points on déduit : $\underline{K \text{ est une } \mathbf{Q}\text{-sous-algèbre de } \mathbf{R}}$.

4. D'après (c), K est un sous-anneau de $\mathbf{R}$, il est donc *commutatif* et *non trivial.*
   Soit, par ailleurs, x un élément non nul de K. Il existe, d'après (b), des rationnels a, b et c non tous nuls, tels que $x = a\omega^2 + b\omega + c$. Soit $D = aX^2 + bX + C$. P et D sont, dans $Q[X]$, premiers entre eux, car.... On termine par Bezout de montrer que K est stable par passage à l'inverse Conclusion : $\underline{K \text{ est un sous-corps de } \mathbf{R}}$.

Deuxième partie CAS GÉNÉRAL :

Soit a un réel.

1. Soit K_0 un sous-corps de $\mathbf{R}$. Il contient 1, est stable par somme et différence et par passage à l'inverse et multiplication il contient donc $\mathbf{Q}$.

2. Soit $\mathcal{K}$ l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a. considérer

$$\mathbf{Q}(a) = \bigcap_{K\in\mathcal{K}} K.$$

3. Facile !D'après la question précédente, ϕ induit notamment un morphisme de l'anneau $\mathbf{Q}[X]$ sur l'anneau $\mathbf{R}$. I en est le *noyau*, ...

4. après HYPOTHÈSE : I non réduit à 0.
   Il existe donc un polynôme P élément de $\mathbf{Q}[X]$, non nul tel que $P(a) = 0$. Multiplier P par le produit des dénominateurs de ses coefficients...
   après HYPOTHÈSE : a est algébrique.
   Presque immédiatement : I est non réduit à $\{0\}$.

5. I est un idéal de $\mathbf{Q}[X]$, donc, d'après le programme on en déduit le résultat.

   $\mu_a(a) = 0$, donc μ_a ne saurait être un inversible de $\mathbf{Q}[X]$. Soient A et B des éléments de $\mathbf{Q}[X]$, tels que $\mu_a = AB$. $A(a)B(a) = \mu_a(a) = 0$ Montre que l'un des polynômes A ou B est inversible car sinon I contiendrait un polynôme de degré strictement plus petit que celui de μ_a $\underline{\text{Donc } \mu_a \text{ est irréductible.}}$

   Le degré de μ_a est supérieur ou égal à 2 , sinon il serait égal à 1 et a serait rationnel.

$$\underline{\mu_{\sqrt{2}} = X^2 - 2.}$$

Maintenant $a = \sqrt{\frac{1+\sqrt{5}}{2}}$. L'élément de $\mathbf{Q}[X]$, $X^4 - X^2 - 1$ admet a comme racine. Donc $\mu_a | X^4 - X^2 - 1$. On peut montrer que $X^4 - X^2 - 1$ est irréductible dans $\mathbf{Q}[X]$ (regarder ses racines). Donc

$$\underline{\mu_a = X^4 - X^2 - 1}.$$

6. $\mathbf{Q}[a]$ est l'image par le morphisme d'anneaux ϕ de l'anneau $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-anneau* de $\mathbf{R}$. Comme $\mathbf{R}$ est un corps, l'anneau $\mathbf{Q}[a]$ est *commutatif et non trivial.* Soit x un élément non nul de $\mathbf{Q}[a]$. Il existe $P \in \mathbf{Q}[X]$ tel que $x = P(a)$. La division euclidienne de P par μ_a conduit à l'existence de Q et R éléments de $\mathbf{Q}[X]$ tels que : $P = Q\mu_a + R$ et $\mathrm{d}^{\mathrm{o}}R < \mathrm{d}^{\mathrm{o}}\mu_a$. D'où $x = P(a) = Q(a)\mu_a(a) + R(a) = R(a)$. x étant non nul, R est non nul, Donc μ_a ne saurait divisé R. Or μ_a est irréductible dans $\mathbf{Q}[X]$ (cf. 6.), donc R et μ_a sont premiers entres eux dans $\mathbf{Q}[X]$. Le lemme de Bezout permet de montrer l'inversibilité de x.
   CONCLUSION : $\underline{\mathbf{Q}[a] \text{ est un corps.}}$

   $\mathbf{Q}[a]$ est un corps qui contient a. Donc $\mathbf{Q}(a) \subset \mathbf{Q}[a]$
   Soit Soit x un élément de $\mathbf{Q}[a]$. Il sécrit

$$x = \sum_{i=0}^{n} c_i a^i,$$

   avec n un naturel et $c_0, c_1, \ldots, c_n$ des rationnels. Reste à montrer quele corps $\mathbf{Q}(a)$ contient $\sum_{i=0}^{n} c_i a^i = x$.
   Donc $\mathbf{Q}[a] \subset \mathbf{Q}(a)$.

   CONCLUSION : $\underline{\mathbf{Q}(a) = \mathbf{Q}[a]}$. $\mathbf{Q}[a]$ est l'image par ϕ, morphisme de $\mathbf{Q}$-espaces vectoriels, de l'espace vectoriel $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-espace vectoriel* du Q-espace vectoriel $\mathbf{R}$. En raisonnant comme dans le début de la question on montre que

$$Q[a] = \underset{\mathbf{Q}}{\mathrm{vect}}(a^0, a^1, \ldots, a^{n-1}).$$

   la famille *la famille* $(a^0, a^1, \ldots, a^{n-1})$ *engendre donc* $\mathbf{Q}[a]$.

   On montre que la famille $(a^0, a^1, \ldots, a^{n-1})$ est libre. Soient $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ des rationnels tels que : $\lambda_0 a^0 + \lambda_1 a^1 + \cdots + \lambda_{n-1} a^{n-1} = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda_0 X^0 + \lambda_1 X^1 + \cdots + \lambda_{n-1} X^{n-1}$.
   Supposons C non nul. Alors par division euclidienne : $\mu_a = \tilde{Q}C + R$ avec $\tilde{Q} \in \mathbf{Q}[X]$, $R \in \mathbf{Q}[X]$ et $\mathrm{d}^{\mathrm{o}}R \leq n-1$. Reste à montrer la nulité de R...

   Finalement $\underline{(a^0, a^1, \ldots, a^{n-1}) \text{ est une base de } \mathbf{Q}[a], \text{ qui est donc de dimension } n}$.
7. facile !
8. Si a est non algébrique, $(a^n)_{n \in \mathbf{N}^*}$ est libre...

Problème, partie II

1. A_p est un corps ssi tout élément R non nul est inversible dans A_p . Or si $R = \lambda M + \mu I \neq 0$ alors il admet $\lambda' M + \mu' I$ pour inverse si et seulement si (λ', μ') est solution d'un système dont le déterminant est $\Delta(R)$

• Cas 3 n'est pas un carré dans Z_p.

Ce déterminant est non nul : deux cas à envisager, μ nul ou non Dans le premier on arrive, en suposant le déterminant nul, à 3 est un carré

Dans le second il est non nul car R est non nul.

Cas 2 : 3 est un carré $3 = a^2$, on peut choisir $(\lambda,\ \mu)$ non nul tel que $\Delta(R) = 0$: il suffit de prendre $\mu = \bar{1}$ et $\lambda = a - \bar{2}$....

2. • Le polynôme caractéristique de M est $X^2 - 4X + 1 = (X-2)^2 2 - a^2$. Il admet pour racines distinctes ...... M est donc diagonalisable.

Tout les éléments de R sont codiagonalisables et la conjugaison ϕ par la matrice de passage P qui intervient dans la diagonalisation est un morphisme d'anneaux (à voir) de A_p sur l'ensemble des matrice 2-2 diagonales à coefficient dans Z_p, lui même isomorphe à $Z_p \times Z_p$

•ϕ conserve le déterminant et donc l'inversibilité ; on peut donc raisonner dans

Il y en a $(p-1)^2$ éléments inversibles . Les éléments de déterminant il y en a $p-1$ de déterminant 1.

3.

Cas 3 n'est pas un carré dans Z_p.

(a) • Dans ce cas, A_p est, comme on l'a vu en II.1. , un corps. Tout élément R non nul de A_p est donc inversible dans A_p et *a fortiori* dans $\mathcal{M}_2(\mathbf{Z})_p$, donc $\Delta(R) \neq 0$. Δ est donc bien une Application de A_p dans Z_p^*, et c'est un morphisme de groupes par propriétés du déterminant.

• L'image de Δ est un sous-groupe de Z_p donc son cardinal divise lecardinal de $\mathbf{Z}_p$

. • Le cardinal du noyau de Δ est le quotient du cardinal de A_p par celui de l'image de Δ (à prouver). On obtient bien un multiple de $p + 1$.

(b) • $\Delta(\lambda M + \mu I) = 1$ signifie $\lambda 2 + 4\lambda\mu + \mu^2 = 1$. Cette équation polynomiale en μ , de degré 2 , admet au plus deux racines dans le corps $\mathbf{Z}_p$.

• λ peut prendre p valeurs ; il y a donc au plus $2p$ éléments de déterminant 1 dans A_p , $|\mathrm{Ker}(\Delta)| \leq 2p$. Comme c'est aussi, on l'a vu en a., un multiple (non nul) de p + 1 , on peut conclure....

4. Cas où p divise $Y_{k?2}$.

• Le raisonnement du II.1. a montré que tout élément de déterminant 1 de A_p est inversible dans A_p . Il est alors immédiat que l'ensemble S des éléments de déterminant 1 de A_p est un sous-groupe de A_p et est donc un groupe multiplicatif. Comme $M \in S$, son ordre divise celui de S , i.e. $p - 1$ ou $p + 1$ selon que 3 soit un carré dans $\mathbf{Z}_p$(question II2.) ou ne le soit pas (question II3.) . Et c'est fini par I.5 !

.