M1G
Anneaux, corps et représentations
contrôle du vendredi 24 octobre 2025
durée : 1H30

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

Correction

3 **Question de cours.** Soit K un corps fini. Montrer que $|K| = p^n$ pour un certain nombre premier p et un entier $n \geqslant 1$.

Comme K est fini, le morphisme d'anneaux $\mathbb{Z} \to K$, $n \mapsto \underbrace{1 + \ldots + 1}_{n\,\text{fois}}$ n'est pas injectif. Notons $p\mathbb{Z}$ le noyau. Comme $1 \notin p\mathbb{Z}$, $p \neq \pm 1$, comme $\mathbb{Z}/p\mathbb{Z}$ s'identifie à un sous-anneau de K, $\mathbb{Z}/p\mathbb{Z}$ est intègre donc p est un nombre premier. Donc K est un $\mathbb{Z}/p\mathbb{Z}-$espace vectoriel. Sa dimension n est finie car K est finie. Alors on a un isomorphisme de groupes $(K, +) \simeq ((\mathbb{Z}/p\mathbb{Z})^n, +)$ donc $|K| = p^n$.

Exercice 1
Soient $P = X^3 - X - 1$ et $Q = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$.

2 a) Montrer que P, Q sont irréductibles sur $\mathbb{Q}$. Le polynôme P n'a pas de racine dans $\mathbb{Z}$ car sinon ce serait un diviseur de 1 *c-à-d* ± 1 or $P(1) = -1 \neq 0$, $P(-1) = -1 \neq 0$. Comme P est unitaire à coefficients entiers, P n'a pas non plus de racine dans $\mathbb{Q}$ car sinon ce serait un entier. Donc P est irréductible sur $\mathbb{Q}$. De même Q est irréductible sur $\mathbb{Q}$ car $Q(1) = -1 \neq 0$ et $Q(1) = 1 \neq 0$.

4 b) Soit y_1 une racine de Q (dans $\mathbb{C}$). Montrer que $y_2 = y_1^2 - 2$ est aussi racine de Q. En déduire que $\mathbb{Q}(y_1)$ est le corps de décomposition de Q sur $\mathbb{Q}$ dans $\mathbb{C}$.

$Q(y_2) = y_1^6 - 5y_1^4 + 6y_1^2 - 1$. Or $y_1^3 = -y_1^2 + 2y_1 + 1 \Rightarrow y_1^4 = -y_1^3 + 2y_1^2 + y_1 = 3y_1^2 - y_1 - 1$. Donc $y_1^6 = y_1^2 y_1^4 = 3y_1^4 - y_1^3 - y_1^2 = 9y_1^2 - 5y_1 - 4$.

Ainsi, $Q(y_2) = 9y_1^2 - 15y_1^2 + 6y_1^2 - 5y_1 + 5y_1 - 4 + 5 - 1 = 0$.

Comme Q est irréductible, y_1 est de degré 3 sur $\mathbb{Q}$. En particulier, $y_1 \neq y_1^2 - 2$ car y_1 n'est pas annumé par un polynôme de degré 2.

Si on note y_3 la troisième racine de Q. On a $y_1 + y_2 + y_3 = -1$ (relations coefficients-racines). Donc $y_3 = -1 - y_1 - y_2 = 1 - y_1 - y_1^2$. Le corps de décomposition de Q dans $\mathbb{C}$ est le corps $\mathbb{Q}(y_1, y_2, y_3) = \mathbb{Q}(y_1, y_1^2 - 2, 1 - y_1 - y_1^2) = \mathbb{Q}(y_1)$.

2 c) Soit y_3 la troisième racine de Q. Calculer

$$\frac{1}{y_1^2} + \frac{1}{y_2^2} + \frac{1}{y_3^2}.$$

On a :

$$\frac{1}{y_1^2} + \frac{1}{y_2^2} + \frac{1}{y_3^2} = \frac{y_2^2 y_3^2 + y_1^2 y_3^2 + y_1^2 y_2^2}{y_1^2 y_2^2 y_3^2}$$

$$= \frac{(y_1 y_2 + y_1 y_3 + y_2 y_3)^2 - 2y_1 y_2^2 y_3 - 2y_1^2 y_2 y_3 - 2y_1 y_2 y_3^2}{(y_1 y_2 y_3)^2}$$

or,
$$y_1 + y_2 + y_3 = -1,\ y_1y_2y_3 = 1,\ y_1y_2 + y_1y_3 + y_2y_3 = -2$$
Donc
$$\frac{1}{y_1^2} + \frac{1}{y_2^2} + \frac{1}{y_3^2} = \frac{2^2 - 2.(-1)}{1^2} = 6.$$

3

d) Soient x_1, x_2, x_3 les racines de P dans $\mathbb{C}$. Calculer
$$\Delta = (x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$$
et en déduire que P n'a qu'une seule racine réelle.
On a $\Delta = -P'(x_1)P'(x_2)P'(x_3) = -(3x_1^2 - 1)(3x_2^2 - 1)(3x_3^2 - 1)$. Or $\forall\, i = 1, 2, 3,\ P(x_i) = 0 \Rightarrow x_i^2 = 1 + \frac{1}{x_i}$. Donc
$$\Delta = -\prod_{i=1,2,3}(2 + \frac{3}{x_i}) = -\prod_{i=1,2,3}(2x_i + 3)$$
car $x_1x_2x_3 = 1$. Donc
$$\Delta = -8\prod_{i=1,2,3}(\frac{3}{2} + x_i) = 8\prod_{i=1,2,3}(-\frac{3}{2} - x_i)$$
$$= 8P(-\frac{3}{2})$$
car $P(X) = (X - x_1)(X - x_2)(X - x_3)$. Donc $\Delta = -23$.

2

e) Soit K le corps de décomposition de P sur $\mathbb{Q}$ dans $\mathbb{C}$. Déterminer $[K : \mathbb{Q}]$.
$K = \mathbb{Q}(x_1, x_2, x_3) = \mathbb{Q}(x_1, x_2)$ car $x_1 + x_2 + x_3 = 0 \Rightarrow x_3 = -x_1 - x_2 \in \mathbb{Q}(x_1, x_2)$.
Comme P est irréductible sur $\mathbb{Q}$, x_1 est de degré 3 sur $\mathbb{Q}$. Comme x_2 est annulé par le polynôme $\frac{P}{X - x_1} \in \mathbb{Q}(x_1)[X]$, x_2 est de degré au plus 2 sur $\mathbb{Q}(x_1)$.
Donc $3 | [K : \mathbb{Q}] = [\mathbb{Q}(x_1)(x_2) : \mathbb{Q}(x_1)][\mathbb{Q}(x_1) : \mathbb{Q}] \leqslant 6$. Donc $[K : \mathbb{Q}] = 3$ ou 6. Or $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in K$ et $\delta^2 = \Delta = -23$ donc $\delta = \pm i\sqrt{23}$ est de degré 2 sur $\mathbb{Q}$. Donc $2 = [\mathbb{Q}(\delta) : \mathbb{Q}] | [K : \mathbb{Q}] \Rightarrow [K : \mathbb{Q}] = 6$.

4

f) Montrer que $\mathbb{Z}[x_1]/(2)$ et $\mathbb{Z}[y_1]/(2)$ sont des corps finis. Déterminer leur cardinal et donner un isomorphisme de corps $\mathbb{Z}[x_1]/(2) \simeq \mathbb{Z}[y_1]/(2)$.
On a :
$$\mathbb{Z}[x_1]/(2) \simeq \mathbb{Z}[X]/(X^3 - X - 1, 2) \simeq \mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X + 1)$$
$$\mathbb{Z}[y_1]/(2) \simeq \mathbb{Z}[X]/(X^3 + X^2 - 2X - 1, 2) \simeq \mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X^2 + 1)$$
Or, n'y ayant pas de racines, les polynômes $X^3 + X + 1$ et $X^3 + X^2 + 1$ sont irréductibles sur le corps $\mathbb{Z}/2\mathbb{Z}$. Donc les anneaux quotients
$$\mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X + 1),\ \mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X^2 + 1)$$
sont des corps de cardinal $2^3 = 8$.
Posons $\overline{x_1} = x_1 \bmod 2 \in \mathbb{Z}[x_1]/(2)$ et $\overline{y_1} = y_1 \bmod 2 \in \mathbb{Z}[y_1]/(2)$.
On a $\mathbb{Z}[x_1]/(2) = \mathbb{Z}/2\mathbb{Z}[\overline{x_1}] \simeq \mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X + 1)$.

Le morphisme surjectif d'anneaux

$$\mathbb{Z}/2\mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}[\overline{y_1}],\ P(X) \mapsto P(\overline{y_1}+1)$$

est bien défini et contient X^3+X+1 dans son noyau car dans $\mathbb{Z}/2\mathbb{Z}[\overline{y_1}]$, $(\overline{y_1}+1)^3+(\overline{y_1}+1)+1 = \overline{y_1}^3+3\overline{y_1}^2+3\overline{y_1}+1+\overline{y_1}+1+1 = \overline{y_1}^3+\overline{y_1}^2+1 = 0$. D'où un morphisme surjectif de corps :

$$\mathbb{Z}/2\mathbb{Z}[\overline{x_1}] \to \mathbb{Z}/2\mathbb{Z}[\overline{y_1}],\ P(\overline{x_1}) \mapsto P(\overline{y_1}+1).$$

Ce morphisme surjectif est un isomorphisme car les deux corps sont finis de même cardinal ($=8$).

Exercice 2

2

a) Montrer que le polynôme X^2+Y^2-1 est irréductible dans $\mathbb{C}[X,Y]$.
Le polynôme $p = Y-1$ est irréductible dans $\mathbb{C}[Y]$. Comme $p|Y^2-1$ et $p^2 \ \|Y^2-1$, d'après le critère d'Eisenstein, le polynôme X^2+Y^2-1 est irréductible sur $\mathbb{C}(Y)$. Comme son contenu est 1 (vu comme polynôme à coefficients dans $\mathbb{C}[Y]$), il est irréductible sur $\mathbb{C}[Y]$ *c-à-d* dans $\mathbb{C}[X,Y]$.

4

b) Montrer que l'élément $X+iY$ est inversible dans l'anneau quotient $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ et déterminer son inverse. En déduire un isomorphisme d'anneaux

$$\mathbb{C}[X,Y]/(X^2+Y^2-1) \simeq \mathbb{C}[T,T^{-1}]$$

(le sous-anneau du corps $\mathbb{C}(T)$ des fractions rationnelles en une variable engendré par $\mathbb{C}$, T, T^{-1}).
$(X+iY)(X-iY) = X^2+Y^2 = 1 \bmod X^2+Y^2-1$. Donc dans l'anneau quotient $\mathbb{C}[X,Y]/(X^2+Y^2-1)$, $X+iY$ est inversible d'inverse $X-iY \bmod X^2+Y^2-1$. Posons $x = X \bmod X^2+Y^2-1$, $y = Y \bmod X^2+Y^2-1$. Comme $(x+iy)^{-1} = x-iy$ dans $\mathbb{C}[X,Y]/X^2+Y^2-1$, le morphisme d'anneaux

$$\phi : \mathbb{C}[T^{\pm 1}] \to \mathbb{C}[X,Y]/X^2+Y^2-1,\ \sum_{k\in\mathbb{Z}\ \text{fini}} c_k T^k \mapsto \sum_{k\in\mathbb{Z}\ \text{fini}} c_k(x+iy)^k$$

est bien défini. Pour trouver la réciproque (éventuelle), on résout :

$$T = x'+iy',\ T^{-1} = x'-iy' \Leftrightarrow x' = \frac{T+T^{-1}}{2},\ y' = \frac{T-T^{-1}}{2i}.$$

Le morphisme d'anneaux $\mathbb{C}[X,Y] \to \mathbb{C}[T^{\pm 1}]$, $X \mapsto \frac{T+T^{-1}}{2}$, $Y \mapsto \frac{T-T^{-1}}{2i}$ est bien défini et contient le polynôme X^2+Y^2-1 dans son noyau car

$$(\frac{T+T^{-1}}{2})^2 + (\frac{T-T^{-1}}{2i})^2 = \frac{T^2+T^{-2}+2}{4} - \frac{T^2+T^{-2}-2}{4} = 1.$$

D'où un morphisme d'anneaux $\psi : \mathbb{C}[X,Y]/(X^2+Y^2-1) \to \mathbb{C}[T^{\pm 1}]$, $x \mapsto \frac{T+T^{-1}}{2}$, $y \mapsto \frac{T-T^{-1}}{2i}$. On vérifie facilement que $\phi \circ \psi = Id_{\mathbb{C}[x,y]}$, $\psi \circ \phi = Id_{\mathbb{C}[T^{\pm 1}]}$ donc ϕ, ψ sont des isomorphismes d'anneaux réciproques l'un de l'autre.

2 c) Montrer que l'anneau $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ est principal.
D'après l'isomorphisme précédent il suffit de montrer que l'anneau $\mathbb{C}[T^{\pm 1}]$ est principal. Soit $I \leqslant \mathbb{C}[T^{\pm 1}]$ un idéal. L'idéal de $\mathbb{C}[T]$: $I \cap \mathbb{C}[T]$ est principal car $\mathbb{C}[T]$ est un anneau principal. Soit $p \in \mathbb{C}[T]$ tel que $I \cap \mathbb{C}[T] = p\mathbb{C}[T]$. Alors $I = (p)$. En effet, si $f \in I$, il existe $N \in \mathbb{N}$ tel que $T^N f \in \mathbb{C}[T]$. Comme I est un idéal dans $\mathbb{C}[T^{\pm 1}]$, $T^k f \in I \cap \mathbb{C}[T] \Rightarrow T^N f = pq$ pour un certain $q \in \mathbb{C}[T]$. Donc $f = p\frac{q}{T^N} \in (p)$. L'inclusion réciproqe est évidente. Comme de plus $\mathbb{C}[T^{\pm 1}] \subseteq \mathbb{C}(T)$, l'anneau $\mathbb{C}[T^{\pm 1}]$ est aussi intègre donc principal.

1 d) Montrer que l'anneau $A = \mathbb{R}[X,Y]/(X^2+Y^2-1)$ est intègre.
D'après le critère d'Eisenstein, le polynôme X^2+Y^2-1 est irréductible dans $\mathbb{R}[X,Y]$. Comme l'anneau $\mathbb{R}[X,Y]$ est factoriel, le quotient $\mathbb{R}[X,Y]/(X^2+Y^2-1)$ est alors intègre.

2 e) Justifier que pour tout $P(X,Y) \in \mathbb{R}[X,Y]$, il existe un unique couple $(a(X), b(X)) \in \mathbb{R}[X]^2$ tels que

$$P(X,Y) = a(X) + b(X)Y \bmod X^2+Y^2-1.$$

Unicité. Si $a(X)+b(X)Y = c(X) = d(X)Y \bmod X^2+Y^2-1$ pour certains $a,b,c,d \in \mathbb{R}[X]$, alors

$$X^2+Y^2-1 | (a(X)-b(X)) + (c(X)-d(X))Y$$

mais pour des raisons de degrés en Y on a alors $(a(X)-b(X)) + (c(X)-d(X))Y = 0$ dans $\mathbb{R}[X,Y$ donc $a(X) = b(X)$ et $c(X) = d(X)$.
Existence. Soit $P(X,Y) \in \mathbb{R}[X,Y]$. Comme X^2+Y^2-1 est unitaire de degré 2 dans $\mathbb{R}[X][Y]$, on peut faire la division euclidienne de P par X^2+Y^2-1 en restant dans $\mathbb{R}[X][Y]$. Le reste est de degré $\leqslant 1$ en Y donc de la forme voulue.

4 f) Montrer que l'application

$$N : A \to \mathbb{R}[X],\ a(X)+b(X)Y \bmod X^2+Y^2-1 \mapsto a(X)^2 - b(X)^2 + X^2 b(X)^2$$

est multiplicative. En déduire les inversibles de l'anneau A.
Soient $a,b,c,d \in \mathbb{R}[X]$. On a :

$$N(\overline{a(X)+b(X)Y}\,.\,\overline{c(X)+d(X)Y}) = N(\overline{a(X)c(X)+b(X)d(X)Y^2+(a(X)d(X)+b(X)c(X))Y})$$

or $Y^2 = 1 - X^2 \bmod X^2+Y^2-1$ donc

$$N(\overline{a(X)+b(X)Y}\,.\,\overline{c(X)+d(X)Y}) =$$

$$\begin{aligned} &N(\overline{a(X)c(X)+b(X)d(X)(1-X^2)+(a(X)d(X)+b(X)c(X))Y}) \\ &= ((ac+bd(1-X^2))^2 - (ad+bc)^2 + X^2(ad+bc)^2 \\ &= (a^2c^2+b^2d^2-(ad+bc)^2+2abcd+X^2(-2b^2d^2+(ad+bc)^2-2abcd)+X^4b^2d^2 \\ &= (a^2c^2+b^2d^2-a^2d^2-b^2c^2)+X^2(a^2d^2+b^2c^2-2b^2d^2)+X^4b^2d^2) \\ &= (a^2-b^2+b^2X^2)(c^2-d^2+d^2X^2) \\ &= N(\overline{a+bY})N(\overline{c+dY}). \end{aligned}$$

Et $N(1) = 1$. En particulier si $a + bY \bmod X^2 + Y^2 - 1$ est inversible, alors $a^2 - b^2 + X^2b^2 \in \mathbb{R}[X]^* = \mathbb{R}^*$. Il existe donc une constante $c \in \mathbb{R}^*$ telle que $a^2 = c + (-X^2 + 1)b^2$. Si on compare les coefficients dominants, on voit que $b^2 = 0$ (sinon le coefficient dominant du terme de droite est strictement négatif alors que celui du terme de gauche est positif) et a est constant. Donc $A^* \subseteq \mathbb{R}^*$. L'inclusion réciproque est évidente donc $A^* = \mathbb{R}^*$.

2

g) Montrer que $X \bmod X^2 + Y^2 - 1$, $1 - Y \bmod X^2 + Y^2 - 1$, $1 + Y \bmod X^2 + Y^2 - 1$ sont irréductibles dans A. L'anneau A est-il factoriel ?

Soit $x = X \bmod X^2 + Y^2 - 1$. Alors $N(x) = X^2$. Si $x = \alpha\beta$ avec $\alpha, \beta \in A$, alors $N(x) = X^2 = N(\alpha)N(\beta)$ dans $\mathbb{R}[X]$. Or l'équation $N(\alpha) = tX$, $t \in \mathbb{R}^*$ n'a pas de solution dans A. En effet, si $\alpha = a + bY \bmod X^2 + Y^2 - 1$, $a, b \in \mathbb{R}[X]$, alors :

$$N(\alpha) = tX \Leftrightarrow a^2 - b^2 + X^2b^2 = tX \Leftrightarrow a^2 = tX + (-X^2 + 1)b^2.$$

Si $b \neq 0$, le terme de droite a un coefficient dominant < 0 ce qui est impossible pour le terme de gauche. Donc $b = 0$. Donc $a^2 = tX \Rightarrow \deg a = \frac{1}{2}$ impssible !

Donc $N(\alpha)$ ou $N(\beta) \in \mathbb{R}^*$ donc α ou $\beta \in A^*$ donc X est irréductible dans A. Posons $y = Y \bmod X^2 + Y^2 - 1$. Alors $N(1 - y) = N(1 + y) = X^2$ donc de même que x, $1 \pm y$ sont irréductibles dans A. Or, $x^2 = (1 - y)(1 + y)$ et $x, 1 - y$ ne sont pas associés dans A car il n'esxiste pas de $c \in \mathbb{R}^*$ tel que $x = c(1 - y)$. Donc A n'est pas factoriel.

3

h) Trouver un idéal maximal de A contenant $X \bmod X^2 + Y^2 - 1$.

L'idéal $m = (x, 1 - y) \leqslant A$ contient x et est maximal car

$$A/m \simeq \mathbb{R}[X, Y]/(Xr + Y^2 - 1, X, 1 - Y) = \mathbb{R}[X, Y]/(X, 1 - Y)$$

car $X^2 + Y^2 - 1 = X^2 + (1 - Y)(1 + Y) \in (X, 1 - Y)$

$$\simeq \mathbb{R}$$

par l'évaluation en $X = 0, Y = 1$.