TD n°5.

Géométrie algébrique

Exercice 1. Soient $F, G \in \mathbb{C}[X,Y]$ tels que $\text{pgcd}(F,G) = 1$.

a) Montrer qu'il existe $A, B \in \mathbb{C}[X,Y]$ tel que $AF + BG$ soit un polynôme non nul de $\mathbb{C}[X]$.

b) Montrer que $\mathcal{V}(F,G) := \{(x,y) \in \mathbb{C}^2, F(x,y) = G(x,y) = 0\}$ est un ensemble fini.

c) Montrer que $\mathbb{C}[X,Y]/(F,G)$ est un $\mathbb{C}$-espace vectoriel de dimension fini.

d) Décrire tous les idéaux premiers de $\mathbb{C}[X,Y]$.

Solution. Voir cours (proposition 9.49 et théorème 9.53)

Exercice 2. On dit qu'une sous-variété V de $\mathbb{C}^n$ est irréductible si pour toutes sous-variétés V_1, V_2 de $\mathbb{C}^n$ telles que $V_1 \cup V_2 = V$, alors $V = V_1$ ou $V = V_2$.
Montrer que V est irréductible si et seulement si $\mathcal{I}(V) := \{P \in \mathbb{C}[X_1, \dots, X_n], \forall x \in V, P(x) = 0\}$ est un idéal premier (si $fg \in \mathcal{I}(V)$, on pourra montrer que $V = \mathcal{V}((\mathcal{I}(V), f)) \cup \mathcal{V}((\mathcal{I}(V), g)))$.

Solution. Supposons V irréductible. Soient $f, g \in A$ tels que $fg \in \mathcal{I}(V)$ et soient $I_1 = \mathcal{I}(V) + (f)$ et $I_2 = \mathcal{I}(V) + (g)$ et $V_i = \mathcal{V}(I_i)$. On a alors $V_1, V_2 \subset V$ et si $x \in V$, alors $fg(x) = 0$ donc $f(x) = 0$ (et alors $x \in V_1$) ou $g(x) = 0$ (et alors $x \in V_2$). Donc $V = V_1 \cup V_2$. Par irréductibilité, on peut supposer $V = V_1$ (le cas $V = V_2$ est identique). Or $f \in \mathcal{I}(V_1)$, donc $f \in \mathcal{I}(V)$ donc $\mathcal{I}(V)$ est premier.
Réciproquement, supposons $\mathcal{I}(V)$ premier et soient V_1, V_2 tels que $V_1 \cap V_2 = V$. Supposons qu'il existe $f \in \mathcal{I}(V_1)$ et $g \in \mathcal{I}(V_2)$ tels que $f, g \notin \mathcal{I}(V)$. Alors $fg \notin \mathcal{I}(V)$ mais $f(x) = 0$ pour tout $x \in V_1$ et $g(x) = 0$ pour tout $x \in V_2$ donc fg est nulle sur $V_1 \cup V_2 = V$, ce qui contredit $fg \notin \mathcal{I}(V)$. Donc soit $\mathcal{I}(V_1) \subset \mathcal{I}(V)$ et alors $V \subset V_1$, soit $\mathcal{I}(V_2) \subset \mathcal{I}(V)$ et alors $V \subset V_2$. D'où l'irréductibilité de V

Exercice 3. Composantes irréductibles
Soit V une sous-variété de $\mathbb{C}^n$. Montrer qu'il existe des sous-variétés irréductibles $V_1, \cdots, V_n$ telles que $V = V_1 \cup \cdots \cup V_n$ (on pourra par l'absurde considérer un idéal maximal de $\mathbb{C}[X_1, \cdots, X_n]$ tel que $\mathcal{V}(I)$ n'admette pas de telle décomposition).
Montrer que si on suppose que $V_i \not\subseteq V_j$ pour $i \neq j$, alors cette décomposition est unique à réordonnement près des V_i (on pourra commencer par montrer que si W est une sous variété irréductible telle que $W \subset V_1 \cup \cdots \cup V_n$ alors il existe i tel que $W \subset V_i$).

Solution. Supposons par l'absurde qu'il existe I telle que $\mathcal{V}(I)$ ne soit pas union finie de sous-variétés irréductibles (toute sous-variété étant de la forme $\mathcal{V}(I)$, une contradiction impliquera l'énoncé), et choisissons un tel I maximal (il en existe par noethérianité de $\mathbb{C}[X_1, \cdots, X_n]$).
Comme $\mathcal{V}(I)$ n'est pas irréductible $\mathcal{V}(I) = V_1 \cup V_2$ avec $V_1 = \mathcal{V}(J_1), V_2(J_2)$ strictement inclus dans $\mathcal{V}(I)$. Quitte à remplacer J_1 par $I + J_1$ (ce qui ne change pas V_1) et J_2 par $I + J_2$, on peut supposer que J_1 et J_2 contiennent strictement I. Donc par maximalité de I, V_1 et V_2 sont unions finies d'irréductibles, donc leur union V aussi, d'où la contradiction
Si $W \subset V = V_1 \cup \cdots \cup V_n$ est irréductible, alors $W = \bigcup_i (W \cap V_i)$, donc par irréductibilité de W, il existe i tel que $W = W \cap V_i$ et donc $W \subset V_i$.
Donc si $V = \bigcup_{j=1}^m W_j$ est une autre décomposition en irréductibles ne se contenant pas les uns les autres, alors pour tout $j \leq m$, il existe $\sigma(j) \leq n$ tel que $W_j \subset V_{\sigma(j)}$. De même, pour tout $i \leq n$, il existe $\tau(i) \leq n$ tel que $V_i \subset W_{\tau(i)}$. Donc $V_i \subset W_{\tau(i)} \subset V_{\sigma(\tau(i))}$ et l'hypothèse implique donc $i = \sigma\tau(i)$ pour tout i et la double inclusion donne $V_i = W_{\tau(i)}$. De même, pour tout j, $j = \tau\sigma(j)$, donc σ et τ sont des bijections réciproques l'une de l'autre comme voulu.

Exercice 4. Soit A un anneau noethérien et I un idéal réduit (c'est-à-dire $I = \sqrt{I}$). On veut montrer qu'il existe des idéaux premiers $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ de A tels que $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$
Suppsons par l'absurde qu'il existe un idéal réduit qui n'est pas intersection fini d'idéaux premiers, I_0 maximal (justifier l'extistence d'un tel I_0).

a) Montrer qu'il existe $a, b \notin I_0$ tels que $ab \in I_0$. On note $J = I_0 + aA$ et $K = I_0 + bA$.

b) Montrer que $JK \subset I_0 \subset J \cap K$.

c) Montrer que $I_0 = \sqrt{J} \cap \sqrt{K}$.

d) En déduire une contradiction.

Solution. Voir cours (théorème 11.13)

Exercice 5. Topologie de Zariski Montrer que l'ensemble $\{\mathbb{C}^n - V, V$ sous-variété algébrique fermé de $\mathbb{C}\}$ est une topologie sur $\mathbb{C}^n$, moins fine que la topologie usuelle.

Solution. Soit $T = \{\mathbb{C}^n - V, V$ sous-variété algébrique fermé de $\mathbb{C}\}$.
On a $\mathbb{C}^n = \mathcal{V}(\mathbb{C}[X_1, \cdots, X_n])^c \in T$ et $\emptyset = \mathcal{V}(\{0\})^c \in T$.
Si $(U_i = \mathcal{V}(I_i)^c)_i$ est une famille d'éléments de T, alors $\bigcup_i U_i = (\bigcap_i \mathcal{V}(I_i))^c = \mathcal{V}(\langle I_i \rangle_i)^c \in T$.
Si $U_1 = \mathcal{V}(I_1)^c$ et $U_2 = \mathcal{V}(I_2)^c$ sont dans T, alors $U_1 \cap U_2 = \mathcal{V}(I_1 I_2)^c \in T$.
Donc T est une topologie.
Si $V = \mathcal{V}(I)$ est une sous-variété algébrique, $V = \bigcap_{f \in I} f^{-1}(\{0\})$ est fermé pour la topologie usuelle en tant qu'intersection d'images réciproques de fermés par des applications continues. Donc tout élément de T est ouvert pour la topologie usuelle.

Exercice 6. Soit $\mathfrak{m}$ un idéal maximal de $A := \mathbb{R}[X_1, \cdots, X_n]$. Montrer que $A/\mathfrak{m}$ est isomorphe à $\mathbb{R}$ où $\mathbb{C}$.

Solution. $k = A/\mathfrak{m}$ est un extension de corps de $\mathbb{R}$ de dimension au plus dénombrable en tant que $\mathbb{R}$-espace vectoriel. Si k contient un élément transcendant t sur $\mathbb{R}$, alors $(\frac{1}{t-a})_{a \in \mathbb{R}}$ formerait une famille libre indénombrable, ce qui contredit la dimension de k. Donc k est une extension algébrique de $\mathbb{R}$, c'est donc $\mathbb{R}$ ou $\mathbb{C}$.

Exercice 7. Soit I un idéal maximal de $\mathbb{R}[X_1, \cdots, X_n]$. Montrer que $\mathcal{V}(I)$ est réduit à un point ou est vide. Donner un exemple où $\mathcal{V}(I)$ est vide.

Solution. Si $z \in \mathbb{R}^n$, soit $\mathfrak{m}_z = \ker(f_z : P \mapsto P(z))$, c'est un idéal maximal puisque f_z est surjective à valeur dans un corps. Si $x, y \in \mathcal{V}(I)$. Alors $I \subset \mathfrak{m}_x, \mathfrak{m}_y$, et la maximalité implique $\mathfrak{m}_x = I = \mathfrak{m}_y$. Comme $X_i - x_i \in \mathfrak{m}_x$, on en déduit $X_i - x_i \in \mathfrak{m}_y$ et donc $y_i = x_i$ pour tout i, donc $x = y$. D'où le résultat.
On peut prendre $I = (X_1^2 + 1, X_2, \cdots, X_n)$.

Exercice 8. Soit $A = \mathbb{C}[X_1, \cdots, X_n]$. Soient I, J deux idéaux de A. Si $x \in \mathbb{C}^n$, on note $\mathfrak{m}_x = \{P \in A, P(x) = 0\}$.

a) Montrer que $x \in V(I)$ si et seulement si $I \subset \mathfrak{m}_x$.

b) Montrer que $\mathcal{V}(I) = \emptyset$ si et seulement si $I = A$.

c) Montrer que $I + J = A$ si et seulement si $\mathcal{V}(I) \cap \mathcal{V}(J) = \emptyset$.

Exercice 9. Soit I un idéal de $A := \mathbb{C}[X_1, \cdots, X_n]$. Soit $J = \mathcal{I}(\mathcal{V}(I))$.

a) Montrer que $\sqrt{I} \subset J$ et $\sqrt{J} = J$.

b) Soit $f \in J$. On considère l'idéal J_0 de $A[T]$ engendré par l'image de I et $1 - fT$. Montrer que $\mathcal{V}(J_0) = \emptyset$.

c) En déduire que $1 - fT$ est inversible dans $A/I[T]$.

d) En déduire que $f \in \sqrt{I}$ (voir dm2).

Solution. Voir cours (théorème 11.7).

Exercice 10. Soient $V \subset \mathbb{C}^n$ et $W \subset \mathbb{C}^m$ deux sous-variétés affines. Une fonction $f : V \to W$ est appelée application régulière de V vers W s'il existe $P_1, \cdots, P_m \in \mathbb{C}[X_1, \cdots, X_n]$ tels que $f(x_1, \cdots, x_n) = (P_1(x_1, \cdots, x_n), \cdots, P_m(x_1, \cdots, x_n)$ pour tout $(x_1, \cdots, x_n) \in V$. On note $\mathrm{Hom}_{\mathrm{Aff}}(V, W)$ l'ensemble des applications régulières de V vers W.
On note $\mathcal{A}(V) = \mathbb{C}[X_1, \cdots, X_n]/\mathcal{I}(V)$.

a) Montrer que si $f : V_1 \to V_2$ et $g : V_2 \to V_3$ sont des applications régulières, alors gf est une application régulière.

b) Montrer que $\mathrm{Hom}_{\mathrm{Aff}}(V, \mathbb{C})$, muni de la multiplication $(f \cdot g)(x) = f(x) \times g(x)$, est une $\mathbb{C}$-algèbre, isomorphe à $\mathcal{A}(V)$.

c) Construire une bijection $\mathrm{Hom}_{\mathrm{Aff}}(V, W) \to \mathrm{Hom}_{\mathbb{C}\text{-Alg}}(\mathcal{A}(W), \mathcal{A}(V))$.

Exercice 11. Soit $V = \{(t^3, t^4, t^5) \in \mathbb{C}^3, t \in \mathbb{C}\}$. Montrer que V est une sous-variété irréductible de $\mathbb{C}^3$ (on pourra décrire $\mathcal{I}(V)$ comme le noyau d'un morphisme $\mathbb{C}[X, Y, Z] \to \mathbb{C}[T]$).

Solution. On vérifie que $V = \mathcal{V}(I := (X^4 - Y^3, X^5 - Z^3, Y^4 - Z^5))$ est bien une sous-variété algébrique.
Considérons $f : \mathbb{C}[X, Y, Z] \to \mathbb{C}[T]$ qui envoie X sur T^3, Y sur T^4 et Z sur T^5. Soit $J = \ker(f)$. Si $P \in J$ et $x = (t^3, t^4, t^5) \in V$, $P(x) = 0$, donc $V \subset \mathcal{V}(J)$. De plus $I \subset J$, donc $\mathcal{V}(J) \subset \mathcal{V}(I) = V$. Or $\mathbb{C}[X, Y, Z]/J$ est intègre en tant que sous-anneau de $\mathbb{C}[T]$. Donc V est irréductible.

Polynômes et extensions de corps

Exercice 12. Soit p un nombre premier.

a) Donner la décomposition en facteurs irréductibles de $P = X^p - 1 \in \mathbb{Q}[X]$ (on pourra considérer $P(X+1)$).

b) Calculer $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ où ζ_p est une racine primitive p^{e} de 1.

c) Calculer $[\mathbb{Q}(\cos(2\pi/p) : \mathbb{Q}]$.

Solution. a) $P(X+1) = X(X^{p-1} + \sum_{i=1}^{p-2} \binom{p}{i+1} X^i + p)$. Comme $\binom{p}{i+1}$ est divisible par p pour tout i dans $[1, p-2]$, on peut appliquer le critère d'Eisenstein à $Q = X^{p-1} + \sum_{i=1}^{p-2} \binom{p}{i+1} X^i + p$, qui est donc irréductible. Donc $P = (X-1)Q(X-1) = (X-1)(X^{p-1} + \cdots + 1)$ est la décomposition de P en facteur irréductible ($Q(X-1)$ est encore irréductible parce que $f \mapsto f(X-1)$ est un automorphisme d'anneau de $\mathbb{Q}[X]$).

b) Comme ζ_p n'est pas racine de $X-1$, son polynôme minimal est $X^{p-1} + \cdots + 1$, et donc $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$.

c) SI $p = 2$ alors $[\mathbb{Q}(\cos(2\pi/p)) : \mathbb{Q}] = 1$. On pose $\zeta_p = \exp(2i\pi/p)$. Si p est impair, on a $\mathbb{Q}(\cos(2\pi/p)) \subset \mathbb{Q}(\zeta_p)$ car $\cos(2\pi/p) = (\zeta_p + \zeta_p^{-1})/2$. De plus ζ_p est racine de $X^2 - 2\cos(2\pi/p)X + 1 \in \mathbb{Q}(\cos(2\pi/p))[X]$. Donc$[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\cos(2\pi/p))] \leq 2$. Or $\mathbb{Q}(\cos(2\pi/p)) \subset \mathbb{R}$ et $\mathbb{Q}(\zeta_p) \not\subset \mathbb{R}$. Donc $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\cos(2\pi/p))] = 2$ et $[\mathbb{Q}(\cos(2\pi/p) : \mathbb{Q}] = \frac{p-1}{2}$ par multiplicativité.

Exercice 13. Soit P le polynôme $X^3 + X^2 + X - 1 \in \mathbb{F}_3[X]$. On note K l'anneau quotient $\mathbb{F}_3[X]/(P)$ et α la classe de X modulo (P).

a) Montrer que K est un corps.

b) Quels sont les ordres multiplicatifs possibles des éléments de K^* ?

c) On dit qu'un élément de K est dit primitif s'il est générateur du groupe multiplicatif K^*.

i) Montrer que K admet un élément primitif.

ii) Combien existe-t-il d'éléments primitifs de K ?

iii) Soit x un élément de K^* distinct de -1. Montrer que x est primitif si et seulement si $x^{13} = -1$.

iv) Soit x est un élément de K^* distinct de -1 et 1. Montrer que x ou $-x$ est primitif.

d) On pose $\beta = \alpha(1-\alpha)$.

i) Vérifier que $\beta^2 = \alpha$.

ii) Quel est l'ordre de α ? En déduire que $-\alpha$ est primitif.

Solution. a) $X^3 + X^2 + X - 2$ est irréductible car il n'a pas de racine dans $\mathbb{F}_3$. K est donc un corps de cardinal $3^3 = 27$.

b) Le groupe K^* est un groupe de cardinal 26, donc l'ordre de tout élément est 1, 2, 13 ou 26.

c) i) Comme un élément d'ordre n est racine de $X^n - 1$, il y a au plus n éléments d'ordre n. Donc le nombre d'élément d'ordre 1, 2 ou 13 est inférieur à $1 + 2 + 13 = 16 < 26$ ce qui prouve qu'il y a un élément d'ordre 26

ii) Il y a $\phi(26) = 12$ éléments d'ordre 26.

iii) Si x est primitif alors $x^{13} = -1$ car $(x^{13})^2 = 1$.

iv) Si $x^{13} = -1$ alors x n'est pas d'ordre 13 ni d'ordre 1. Il n'est pas d'ordre 2 car $x \neq -1$.

d) i) On a $\beta^2 = \alpha^2 - 2\alpha^3 + \alpha^4 = \alpha$ par division euclidienne.

ii) α est un carré donc α est d'ordre 13. $-\alpha$ est d'ordre 26.

Exercice 14. On pose $P = X^4 + X + 1 \in \mathbb{F}_2[X]$ et $K = \mathbb{F}_2[X]/(P)$. On note α la classe de X modulo (P).

a) Montrer que K est un corps et déterminer son cardinal.

b) Montrer que K admet un élément primitif.

c) Quel est l'ordre de α dans le groupe K^* ?

d) On pose $\beta = 1 + \alpha^3$. Déterminer un polynôme irréductible à coefficients dans $\mathbb{F}_2$ dont β soit racine.

e) Montrer que le polynôme $F = X^3 + X + 1$ est irréductible dans $K[X]$. Déterminer le cardinal de $K[X]/(F)$.

Solution. a) $X^4 + X + 1$ est irréductible car il n'a pas de racine dans $\mathbb{F}_2$ et n'est pas égal à $(X^2 + X + 1)^2$. K est un corps de cardinal $2^4 = 16$.

b)

c) L'ordre de tout élément de K^* divise 15, c'est donc $1, 3, 5$ ou 15. Le nombre d'éléments d'ordre $1, 3$ ou 5 est inférieur à $1 + 3 + 5 = 9 < 15$, donc K admet un élément d'ordre 15.

d) L'ordre de α divise 15. On a $\alpha^3 \neq 1$ car 1 et α sont libres. $\alpha^5 = \alpha \cdot \alpha^4 = \alpha \cdot (1 + \alpha) \neq 1$. Donc α est d'ordre 15.

e) On a $\alpha \cdot (1 + \alpha^3) = 1$, donc $\beta = \alpha^{-1}$ et $X^4 P(1/X) = X^4 + X^3 + 1$ annule β.

f) Les racines de $X^3 + X + 1$ "vivent" dans $\mathbb{F}_8$ et sont donc d'ordre 7. On peut vérifier d'ailleurs que si γ est racine de F, alors $\gamma^3 = \gamma + 1$, donc $\gamma^6 = 1 + \gamma^2$ et $\gamma^7 = \gamma + \gamma^3 = 1$. Mias K n'a pas d'éléments d'ordre 7. Donc F n'a pas de racine et est donc irréductible car de degré 3.

g) $K[X]/(F)$ est un corps fini de cardinal $(\sharp K)^3 = 2^{12}$.

Exercice 15. Soit Ω une extension d'un corps k. Soient K et L deux sous-corps de Ω contenant k. On suppose que $m := [K : k]$ et $n := [L : k]$ sont finis. Soit Ω un corps contenant K et L. On note KL le composé de K et L dans Ω i.e. l'ensemble des sommes finies $\sum a_i b_i$ où $a_i \in K$ et $b_i \in L$.

a) Montrer que KL est un corps et que c'est le sous-corps de Ω engendré par K et L.

b) Montrer que KL est une extension finie de k de degré $\leq mn$.

c) Montrer que si m et n sont premiers entre eux, on a $[KL : k] = mn$.

d) Montrer qu'en général la conclusion de l'assertion 3 est fausse si m et n ne sont pas premiers entre eux.

Solution. (i) Soient $(a_i)_{1 \leq i \leq m}$ une base de K/k et $(b_j)_{1 \leq j \leq n}$ une base de L/k. La famille $(a_i b_j)_{i,j}$ est un système générateur ayant au plus mn éléments du k-espace vectoriel KL. Ainsi, KL est une K-algèbre de dimension finie, qui est intègre. Par suite, KL est un corps, car une algèbre intègre A qui est de dimension finie sur un corps, est un corps : en effet, si x_0 est un élément non nul de A, alors x_0 est inversible dans A, comme on le constate en considérant l'endomorphisme de A qui à x associe xx_0. Par ailleurs, le sous-corps de Ω engendré par K et L contient les sommes finies $\sum a_i b_i$ où $a_i \in K$ et $b_i \in L$, donc contient KL. D'où le résultat.
(ii) Cette assertion se déduit du fait que le k-espace vectoriel KL contient un système générateur ayant au plus mn éléments.
(iii) On a

$$[KL : k] = [KL : K]m = [KL : L]n.$$

Les entiers m et n étant premiers entre eux, m divise $[KL : L]$ et n divise $[KL : K]$. Les degrés $[KL : L]$ et $[KL : K]$ divise $[KL : k]$, les entiers m et n divisent donc $[KL : k]$. Puisque m et n sont premiers entre eux, mn divise $[KL : k]$. D'après l'assertion 1, on a donc $mn = [KL : k]$.
(iv) On prend $k = \mathbb{Q}$, $K = \mathbb{Q}(\alpha)$ où $\alpha^3 = 2$ et $L = \mathbb{Q}(j\alpha)$ où $j^3 = 1$, $j \neq 1$. On a $[K : \mathbb{Q}] = [L : \mathbb{Q}] = 3$. Vérifions que $[KL : \mathbb{Q}] = 6$. On a

$$\mathbb{Q} \subseteq K \subseteq KL \subseteq \mathbb{Q}(\alpha)\mathbb{Q}(j).$$

Compte tenu de la question 2, on a $[\mathbb{Q}(\alpha)\mathbb{Q}(j) : \mathbb{Q}] = 6$. Ainsi $[KL : \mathbb{Q}] = 3$ ou 6. Si $[KL : \mathbb{Q}] = 3$, on a $KL = K$ et j est dans K, ce qui n'est pas. D'où l'assertion.
(v) D'après l'assertion 3, on a $[L(\alpha) : K] = nd$, d'où $[L(\alpha) : L] = n$ et le résultat.

Exercice 16. a) Montrer que l'équation $a^2 + 5b^2 = 2$ avec $(a, b) \in \mathbb{Z}^2$ n'a pas de solution.
Soit K le corps $\mathbb{Q}(\sqrt{-5})$.

b) i) Quel est de degré de l'extension $K/\mathbb{Q}$, donner une base de K sur $\mathbb{Q}$. Soit x un élément de K qui n'est pas dans $\mathbb{Q}$, montrer que $K = \mathbb{Q}(x)$.

ii) Déterminer les automorphismes $\mathbb{Q}$-linéaires du corps K tel que si $x \in \mathbb{Q}$, on a $\sigma(x) = x$.
On note G cet ensemble d'automorphismes et pour $x \in K$, on définit

$$N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in G} \sigma(x).$$

c) i) En écrivant $x = a + b\sqrt{-5}$ avec a et b dans $\mathbb{Q}$, calculer $N_{K/\mathbb{Q}}(x)$ et montrer que $N_{K/\mathbb{Q}}(x) \in \mathbb{Q}$.

ii) Notons $m_x : K \to K$ la multiplication par x. Montrer que $N_{K/\mathbb{Q}}(x) = \det(m_x)$.
Notons A le sous-anneau $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ de K.

d) Montrer que A est isomorphe à $\mathbb{Z}[X]/(X^2 + 5)$.

e) Soit x un élément non nul de A.

i) Montrer que l'idéal (x) est un $\mathbb{Z}$-module libre de rang 2 et qu'il existe une $\mathbb{Z}$-base (e_1, e_2) de A et des éléments $(c_1, c_2) \in \mathbb{N}^2$ tels que $(c_1 e_1, c_2 e_2)$ est une $\mathbb{Z}$-base de (x).

ii) Montrer que l'anneau $A/(x)$ est fini et déterminer son cardinal que l'on le notera $N(x)$.

f) Considérons l'application $\mathbb{Z}$-linéaire $u : A \to (x)$ définie par $u(e_i) = c_i e_i$ qui est inversible d'inverse $u^{-1} : (x) \to A$ défini par $u^{-1}(c_i e_i) = e_i$. Considérons maintenant l'application $\mathbb{Z}$-linéaire $v : (x) \to (x)$ définie par $v = m_x \circ u^{-1}$ où $m_x : A \to (x)$ est la multiplication par x.

i) Montrer que dans la base (c_1e_1, c_2e_2), la matrice de v est à coefficients dans $\mathbb{Z}$.

ii) Montrer que v est surjective et en déduire que $\det(v) = \pm 1$.

iii) En calculant $\det(m_x)$ de deux manières, montrer que $N(x) = N_{K/\mathbb{Q}}(x)$.

g) Soit I un idéal non nul de A

i) Montrer que A/I est un ensemble fini. On définit $N(I) = \mathrm{Card}(A/I)$ pour tout idéal I non nul de A.

ii) Calculer $N(I)$ pour $I = (2, 1 + \sqrt{-5})$.

iii) Montrer que l'anneau A n'est pas principal.

Solution. (i) Si on a une solution alors nécessairement $b = 0$ sinon $a^2 + 5b^2 \geq 5 > 2$. Mais si b est nul on doit avoir a^2 avec $a \in \mathbb{Q}$ ce qui est impossible.
(ii).a. On a $(\sqrt{-5})^2 + 5 = 0$ donc le polynôme minimal de $\sqrt{-5}$ est $X^2 + 5$ et l'extension est de degré 2 de base $(1, \sqrt{-5})$. Si $x \in K$ n'est pas dans $\mathbb{Q}$, alors le sous-corps $\mathbb{Q}(x)$ de K est différent de $\mathbb{Q}$ donc de dimension au moins 2 sur $\mathbb{Q}$ et est donc égal à K.
b. Écrivons $x \in K$ sous la forme $x = a + b\sqrt{-5}$. On a alors $\sigma(x) = a + b\sigma(\sqrt{-5})$ et il suffit de déterminer l'image de $\sqrt{-5}$. On a

$$\sigma(\sqrt{-5})^2 = \sigma(\sqrt{-5}^2) = \sigma(-5) = -5$$

donc $\sigma(\sqrt{-5}) = \pm\sqrt{-5}$ et on a deux tels automorphismes : l'identité et l'application définie par $\sigma(x) = a - b\sqrt{-5}$.
(iii).a. On a $N_{K/\mathbb{Q}}(x) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Q}$.
b. Soit $x = a + b\sqrt{-5}$, on regarde m_x dans la base $(1, \sqrt{-5})$. Sa matrice est alors

$$\begin{pmatrix} a & -5b \\ b & a \end{pmatrix}$$

de déterminant $\det(m_x) = a^2 + 5b^2 = N_{K/\mathbb{Q}}(x)$.
(iv) On construit un morphisme π de $\mathbb{Z}[X]$ vers A de la manière suivante : à P on associe $P(\sqrt{-5})$. C'est un morphisme d'anneaux évidement surjectif et le polynôme $X^2 + 5$ est dans son noyau. Soit maintenant P dans le noyau, comme $X^2 + 5$ a un coefficient dominant inversible, on peut effectuer la division Euclidienne et on a

$$P(X) = (X^2 + 5)Q(X) + R(X)$$

avec $R \in \mathbb{Z}[X]$ de degré au plus 1. Mais alors en évaluant en $\sqrt{-5}$, on trouve $R(\sqrt{-5}) = 0$ ce qui n'est possible que si $R = 0$ car $\sqrt{-5} \notin \mathbb{Q}$. On a donc $\ker \pi = (X^2 + 5)$ et l'isomorphisme recherché.
(v).a. L'idéal (x) est évidement un sous-$\mathbb{Z}$-module de A et comme A est sans torsion, il est sans torsion. On en déduit donc qu'il est libre. Par ailleurs, les éléments x et $x\sqrt{-5}$ sont dans (x) et sont libres sur $\mathbb{Z}$. En effet, si on avait une relation $ax + bx\sqrt{-5} = 0$, les éléments 1 et $\sqrt{-5}$ seraient liés dans $\mathbb{Q}$ ce qui n'est pas le cas puisque c'est une base du $\mathbb{Q}$-espace vectoriel K. Le $\mathbb{Z}$-module (x) est donc libre de rang 2.
Le théorème des bases adaptées pour les $\mathbb{Z}$-modules nous donne la fin de la question.
b. On a $N(x) = c_1c_2$.
(vi) Considérons l'application $\mathbb{Z}$-linéaire $u : A \to (x)$ définie par $u(e_i) = c_i e_i$ qui est inversible d'inverse $u^{-1} : (x) \to A$ défini par $u^{-1}(c_i e_i) = e_i$. Considérons maintenant l'application $\mathbb{Z}$-linéaire $v : (x) \to (x)$ définie par $v = m_x \circ u^{-1}$ où $m_x : A \to (x)$ est la multiplication par x.
a. L'image par v de $c_i e_i$ est xe_i qui appartient à (x) donc s'écrit dans la base (c_1e_1, c_2e_2) sous la forme

$$xe_i = a_{1,i}c_1e_1 + a_{2,i}c_2e_2$$

avec les $a_{i,j} \in \mathbb{Z}$. La matrice est la matrice des $(a_{i,j})$ et est à coefficients dans $\mathbb{Z}$.
b. Les éléments e_i sont les images par u^{-1} des éléments $c_i e_i \in (x)$. L'application u^{-1} est donc surjective. Par ailleurs, par définition de (x), l'application m_x est surjective donc v est surjective et son déterminant est ± 1.
c. On a vu que $\det(m_x) = N_{K/\mathbb{Q}}(x)$. Par ailleurs, on a $m_x = u \circ v$ donc $\det(m_x) = \det(u)\det(v) = \pm\det(u) = \pm c_1c_2 = \pm N(x)$. On conclue en disant que $N(x)$ et $N_{K/\mathbb{Q}}(x)$ sont positifs.
(vii).a. Si I est non nul il contient un élément x non nul et on a $(x) \subset I$. On a alors une surjection $A/(x) \to A/I$ ce qui prouve que A/I est fini (puisque $A/(x)$ l'est).

b. On va montrer que $A/I = \mathbb{Z}/2\mathbb{Z}$. Pour cela on utilise le fait que $A = \mathbb{Z}[X]/(X^2+1)$, le quotient A/I est alors isomorphe à $\mathbb{Z}[X]/(X^2+5, 2, 1+X)$. Remarquons que $X^2+5 = (X+1)^2 + 2(2-X)$ donc $(X^2+5, 2, X+1) = (2, X+1)$.
On définit alors un morphisme $f : \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ par $f(P) \equiv P(-1) \pmod 2$. C'est bien un morphisme d'anneaux et on va calculer son noyau. Il est clair que $(2, X+1) \subset \ker f$. Montrons la réciproque. Soit P dans le noyau, alors $P(-1)$ est pair donc $P(-1) = 2n$ avec $n \in \mathbb{Z}$. La division Euclidienne nous donne $P(X) = (X+1)Q(X) + P(-1)$ donc

$$P(X) = (X+1)Q(X) + 2n \in (2, X+1).$$

On a donc l'isomorphisme annoncé et $N(I) = 2$.
c. Si I était principal, sa norme $N(I) = 2$ serait celle d'un élément c'est-à-dire de la forme $a^2 + 5b^2$ c'est impossible d'après la première question.

Complément

Exercice 17. Soit K un espace topologique compact et soit $x \in K$. Soit $A = \mathbb{C}^0(K, \mathbb{R})$. On admet le théorème de prolongement de Tietze : Si K' est un fermé de K et $f : K' \to \mathbb{R}$ est une fonction continue, alors il existe $f' \in A$ telle que $f'_{|K'} = f$.

a) Soit $\mathfrak{m}_x = \{f \in A, f(x) = 0\}$. Montrer que M est un idéal maximal de A.

b) Soit $J = \{f \in A, \exists U$ voisinage ouvert de $x, f(U) = 0\}$. Montrer que J est un idéal de A

c) Soit $S = A - \mathfrak{m}_x$. Montrer que S est une partie multiplicative de A.

d) Montrer que si $f \in J$, il existe $t \in S$ telle que $tf = 0$. En déduire un morphisme $\phi : A/J \to S^{-1}A$ de A-algèbres.

e) Montrer que si $s \in S$, il existe $s' \in A$ telle que $ss' - 1 \in J$. En déduire un morphisme $\psi : S^{-1}A \to A/J$ de A-algèbres.

f) Montrer que ϕ et ψ sont des isomorphismes inverses l'un de l'autre.