TD n°3b.

Exercice 1. Étant donné I un idéal d'un anneau A, on note $\sqrt{I}$ son radical (ou sa racine). Soient I, J et L des idéaux de A, montrer les assertions suivantes :

a) si $I \subset J$, alors $\sqrt{I} \subset \sqrt{J}$,
b) $\sqrt{I \cdot J} = \sqrt{I \cap J}$,
c) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$,
d) $\sqrt{\sqrt{I}} = \sqrt{I}$,
e) si $\mathfrak{p}$ est un idéal premier, alors $\sqrt{\mathfrak{p}} = \mathfrak{p}$,
f) $\sqrt{I} + \sqrt{J} \subset \sqrt{I+J}$,
g) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$,
h) $\sqrt{(I \cap J) + (I \cap L)} = \sqrt{I \cap (J+L)}$,
i) soient $(\mathfrak{p}_i)_{1 \leq i \leq n}$ des idéaux premiers de A, supposons que

$$I \subset \bigcap_{i=1}^{n} \mathfrak{p}_i \subset \sqrt{I},$$

montrer que

$$\sqrt{I} = \bigcap_{i=1}^{n} \mathfrak{p}_i.$$

Exercice 2. 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 finie d'idéaux premiers, et soit I_0 maximal parmi les idéaux réduits qui ne sont pas intersection finie d'idéaux premiers (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. Comme A est noethérien toute famille non vide d'idéaux admet un élément maximal, en particulier la famille des idéaux réduits qui ne sont pas intersection finie d'idéaux premiers.

a) Comme I_0 n'est pas un idéal premier, il existe $a, b \notin I_0$ tels que $ab \in I_0$.
b) $I_0 \subset J$ et $I_0 \subset K$ donc $I_0 \subset J \cap K$. De plus si $x_1 = i_1 + ay_1 \in J$ et $x_2 = i_2 + by_2 \in K$ avec $i_1, i_2 \in I_0$ et $y_1, y_2 \in A$, $x_1x_2 = i_1i_2 + ay_1i_2 + by_2i_1 + aby_1y_2 \in I_0$ en tant que combinaison linéaire d'éléments de I_0. Or JK est engendré par les éléments de la forme x_1x_2, donc $JK \subset I$.
c) De la question précédente, on déduit que $\sqrt{JK} \subset \sqrt{I_0} \subset \sqrt{J \cap K}$. Comme I_0 est réduit $\sqrt{I_0} = I_0$. De plus $\sqrt{JK} = \sqrt{J \cap K} = \sqrt{J} \cap \sqrt{K}$ d'après l'exo 1, donc les deux inclusions dans $\sqrt{JK} \subset \sqrt{I_0} \subset \sqrt{J \cap K}$ sont des égalités.
d) Comme $I_0 \subsetneq J \subset \sqrt{J}$ et $I_0 \subsetneq K \subset \sqrt{K}$ et comme $\sqrt{J}$ et $\sqrt{K}$ sont réduits, on en déduit par maximalité de I_0 que $\sqrt{J}$ et $\sqrt{K}$ sont des intersections finies d'idéaux premiers. Comme $I_0 = \sqrt{J} \cap \sqrt{K}$, I_0 est lui aussi intersection finie d'idéaux premiers. D'où la contradiction.

Exercice 3. Un A-module M est dit artinien si toute suite décroissante de sous-A-modules de M est stationnaire. Un anneau A est dit artinien si il est artinien en tant que A-module.

a) Montrer qu'un A-module M est artinien si et seulement si toute famille de sous-module de M admet un élément minimal.
b) Soit k-un corps. Montrer qu'une algèbre de dimension finie sur k est artinienne.
c) Soit N un sous-module de M. Montrer que M est artinien si et seulement si N et M/N sont artiniens.

d) Montrer qu'un anneau intègre est artinien si et seulement si c'est un corps.

e) Soit k un corps. Montrer qu'un k-espace vectoriel M est un k-module artinien si et seulement si il est de dimension fini.

f) On suppose dorénavant que A est un anneau artinien.

i) Montrer que tout idéal premier de A est un idéal maximal.

ii) Montrer que A n'a qu'un nombre fini d'idéaux maximaux (on pourra utiliser le lemme chinois ou un argument de comaximalité).

iii) Si $\mathfrak{m} \in \mathrm{Spec}(A)$, on note $\mathfrak{m}^\infty = \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n$ et $k_\mathfrak{m} = A/\mathfrak{m}$. Munir $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ d'une structure de $k_\mathfrak{m}$-espace vectoriel et montrer qu'il est de dimension finie. En déduire que $A/\mathfrak{m}^\infty$ est un anneau noethérien.

iv) Montrer que $A \to \prod_{\mathfrak{m}\in\mathrm{Spec}(A)} A/\mathfrak{m}^\infty$ est surjective. Soit $\mathfrak{R}^\infty$ le noyau de ce morphisme. Montrer que $\mathfrak{R}^\infty \cdot \mathfrak{m} = \mathfrak{R}^\infty$ pour tout idéal maximal $\mathfrak{m}$ de A. Soit $J = \mathrm{Ann}(\mathfrak{R}^\infty) = \{x \in A, \forall y \in \mathfrak{R}^\infty, xy = 0\}$.

v) On suppose $J \neq A$. Montrer qu'il existe un idéal J' contenant J tel que J'/J soit un A-module simple et, en utilisant la question 2 de l'exercice 2, en déduire qu'il existe un idéal maximal $\mathfrak{m}$ de A tel que $J'\mathfrak{m} \subset J$. En déduire que $J' \subset \mathrm{Ann}(\mathfrak{R}^\infty)$ et obtenir une contradiction.

vi) En déduire que $A \to \prod_{\mathfrak{m}\in\mathrm{Spec}(A)} A/\mathfrak{m}^\infty$ est un isomorphisme. Montrer que A est un anneau noetherien.

g) Réciproquement soit A un anneau noethérien dont tout idéal premier est maximal.

i) Montrer qu'il existe un sous-module de A maximal M pour la propriété d'être artinien.

ii) Soit $a \in A - M$, montrer que $M + (a)$ et $M + (a)/M$ sont artiniens et en déduire une contradiction. En déduire que A est artinien.

Exercice 4. Un A-module est dit simple si il a exactement deux sous-modules (0 et lui-même). Un A-module M est dit de longueur finie si il existe une suite de sous-modules

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_m = M$$

telle que, pour tout $1 \leq i \leq n$, M_i/M_{i-1} soit simple (une tel suite est appelé suite de décomposition de M et les M_i/M_{i-1} sont).

a) Soit I un idéal de A. Montrer que A/I est un A-module simple si et seulement si I est un idéal maximal.

b) Soit M un module simple. Montrer qu'il existe un idéal maximal $\mathfrak{m}$ tel que M soit isomorphe à $A/\mathfrak{m}$.

c) Montrer que si M est un module de type fini non nul, alors M a un sous-module N tel que M/N soit simple.

d) Montrer qu'un A-module est de longueur fini si et seulement si il est noethérien et artinien.

e) Montrer que si M est de longueur fini, la longueur m de la suite de décomposition ne dépend pas du choix de la suite de décomposition et que les facteurs non plus à permutation près. Plus précisément, si

$$0 = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_n = M$$

est une autre suite de décomposition, montrer que $m = n$ et qu'il existe $\sigma \in \mathfrak{S}_n$ tel que M_i/M_{i-1} soit isomorphe à $N_{\sigma(i)}/N_{\sigma(i)-1}$.

Exercice 5. Soit A un anneau local, d'idéal maximal $\mathfrak{m}$. Soit $k = A/\mathfrak{m}$

a) Soit P un A-module projectif (cf. TD 3 exo 9) de type fini.

b) Montrer qu'il existe $n \in \mathbb{N}$ et un A-module de type fini P' tel que $P \oplus P' \simeq A^n$. On identifie dorénavant $P \oplus P'$ et A^n.

c) Munir $P/\mathfrak{m}P$ et $P'/\mathfrak{m}P'$ d'une structure de k-espace vectoriel. Soit $(\bar{e}_i)_{i\in I}$ et $(\bar{e}'_j)_{j\in J}$ une base de $P/\mathfrak{m}P$ et $P'/\mathfrak{m}P'$ respectivement. Montrer que $\mathrm{Card}(I) + \mathrm{Card}(J) = n$

d) Soit e_i un antécédent de $\bar{e}_i$ par le morphisme $P \to P/\mathfrak{m}P$ et e'_j un antécédent de $\bar{e}'_j$ par le morphisme $P' \to P'/\mathfrak{m}P'$. Montrer que $(e_i)_{i\in I}$ et $(e'_j)_{j\in J}$ sont des familles génératrices de P et P' (on pourra appliquer le lemme de Nakayama (TD 3 exo 13) à $P/\langle e_i\rangle_{i\in I}$).

e) En déduire deux applications surjectives $A^{\mathrm{Card}(I)} \to P$ et $A^{\mathrm{Card}(J)} \to P'$. En déduire une application surjective $f : A^n \to A^n$.

f) Montrer que $\det f$ est inversible (on pourra réduire modulo $\mathfrak{m}$). Montrer que f est un isomorphisme.

g) En déduire que P est un module libre.

Exercice 6. Soit A l'anneau des fonctions continues de $\mathbb{R}$ vers $\mathbb{R}$ qui sont π-périodiques. Soit $P = \{g \in \mathcal{C}^0(\mathbb{R},\mathbb{R}), g(x+\pi) = -g(x)\}$.

a) Munir P d'une structure de A-module via $(f.g)(x) = f(x)g(x)$.

b) Montrer que $\Big((\cos,\sin),(\sin,-\cos)\Big)$ forme une base du A-module $P \oplus P$.

c) Montrer que P n'est pas un A-module libre (on pourra commencer par montrer que toute famille d'au moins deux éléments de P est liée).

1 Anneaux factoriels

Exercice 7. Soit A un anneau factoriel et $a \in A$. Montrer que $\sqrt{aA}$ est un idéal principal.

Solution. Si $a = 0$, alors $\sqrt{(a)} = 0$ puisque A est intègre. Sinon, soit $a = \prod_i p_i^{n_i}$ la décomposition en facteurs irréductibles de a, avec $n_i \geq 1$. Soit $b = \prod_i p_i$. Alors $b^{\max_i n_i} \in (a)$ et donc $b \in \sqrt{(a)}$. Réciproquement si $c \in \sqrt{(a)}$, alors il existe n tel que a divise c^n. En particulier p_i divise c^n et donc p_i divise c d'après le lemme de Gauss. Donc $b = \prod_i p_i$divise c. Donc $\sqrt{(a)} = (b)$.

Exercice 8. Contenus
A désigne un anneau factoriel. On note $c(P)$ pour $P \in A[X]$, le contenu de P : c'est le pgcd de ses coefficients. P est primitif si $c(P)$ est inversible. On note $k = \mathrm{Frac}(A)[X]$.

a) Soit p premier un élément de A qui divise $P \cdot Q \in A[X]$. Montrer que p divise P ou Q. (Lemme de Gauss)

b) i) Montrer que, si P et Q sont primitifs, alors PQ est primitif

ii) Montrer que $c(P)c(Q) = c(PQ)$

c) Monrter que, si P primitif divise Q dans $k[X]$, alors P divise Q.

d) Montrer que $P \in A[X]$ est irréductible si et seulement si il est primitif et irréductible dans $k[X]$.

Solution. a) On a un morphisme $A \to A/(p)$ qui se prolonge en $A[X] \mapsto A/(p)[X]$, qui est intègre. Sinon, autre méthode. Supposons que p ne divise ni P, ni Q. Soit i_0 et j_0 les indices maximum tels que $p \not| p_i$ et $p \not| q_j$. Calculons $(PQ)_{i_0+j_0} = \sum_{i+j=i_0+j_0} p_i q_j$. Donc $p | p_{i_0} q_{j_0}$. Contradiction.

b) Tout diviseur premier de $c(PQ)$ divise $c(P)$ ou $c(Q)$ donc leur produit et réciproquement. ON fait une récurrence sur le nombre de facteurs dans la décomposition de $c(P)c(Q)$.

c) Soit $BP = Q$ où $B \in \mathrm{Frac(A)}[X]$. On peut multiplier pat d, tel que $dB \in A[X]$ et $c(dB) = 1$. On alors $(dB) \cdot P = dQ$. Mais $d | c(dQ) = c(dB)c(P) = 1$ donc d est inversible et $B \in A[X]$.

Exercice 9. Critère d'irréductibilité d'Eisenstein

a) soit A un anneau factoriel et K son corps des fractions. Soit $f = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynômes de degré $d \geq 1$. Soit p un élément irréductible de A. Supposons que p ne divise pas a_d, que p divise a_i pour $0 \leq i < d$ et que p^2 ne divise pas a_0. Montrer que f est irréductible dans $K[X]$.

b) Montrer que $X^4 + X^2Y^3 + Y$ est irréductible dans $\mathbb{Q}[X,Y]$.

c) Soient A est un anneau intègre et $\mathfrak{p}$ un idéal premier Soit $f = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynômes de degré $d \geq 1$ tel qu'aucun élément non inversible ne divise tous les coefficients. Supposons $a_d \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ pour $0 \leq i < d$ et que $a_0 \notin \mathfrak{p}^2$. Montrer que f est irréductible dans $A[X]$.

Solution. (1) Supposons que $f = PQ$ avec P et Q dans $K[X]$. On peut alors écrire $P(X) = \frac{1}{a}P_0(X)$ avec $P_0 \in A[X]$ et $a \in A$ tel qu'aucun facteur irréductible de a ne divise P_0. On écrit de même $Q(X) = \frac{1}{b}Q_0(X)$. On a alors $abf(X) = P_0(X)Q_0(X)$. Si p est un irréductible divisant ab, il divise P_0Q_0 donc d'après le lemme de Gauss, il divise P_0 ou Q_0. En le divisant on obtient une relation semblable avec un facteur irréductible de moins. On peut donc supposer par récurrence que ab est inversible puis en divisant encore que $a = b = 1$.
Remarquons tout d'abord que comme p est irréductible et que A est factoriel, alors l'idéal (p) est premier (cf. exercice précédent). On va donc se placer dans $A/(p)[X]$ qui est un anneau intègre. Avec les hypothèses, on peut alors calculer

$$Cl(a_d)X^d = Cl(f) = Cl(P)Cl(Q).$$

Il existe donc un entier k tel que $Cl(P) = Cl(\lambda)X^k$ et $Cl(Q) = Cl(\mu)X^{d-k}$ avec λ et $\mu \in A$ tels que $Cl(\lambda)Cl(\mu) = Cl(a_d)$. On sait alors que $\deg(P) \geq \deg(Cl(P)) = k$, $\deg(Q) \geq \deg(Cl(Q)) = d-k$ et $\deg(P)\deg(Q) = \deg(f) =$

d. On en déduit que $\deg(P) = k$ et $\deg(Q) = d - k$. Si $k, d - k \geq 1$, alors $P(0)$ et $Q(0)$ sont divisibles par p, et donc $f(0)$ est divisible par p^2 contrairement à l'hypothèse. Donc P ou Q est de degré 0.
(ii) On se place dans $\mathbb{Q}[Y][X] = A[X]$ et on considère $p = Y$ qui est irréductible dans $A = \mathbb{Q}[Y]$. Le polynôme $X^4 + X^2Y^3 + Y$ vérifie les hypothèses du (i) donc il est irréductible dans $\mathbb{Q}(Y)[X]$ et donc à fortiori dans $\mathbb{Q}[X, Y]$.

Exercice 10. Soit A un anneau intègre et K son corps de fractions. On dit que $x \in K$ est entier sur A si $A[x]$ est un A-module de type fini. On dit que A est intégralement clos si tout élément de K entier sur A est dans A.

a) Montrer que $x \in K$ est entier sur A si et seulement si il existe un polynôme unitaire de $A[X]$ dont x est racine.

b) Montrer que si A est factoriel, alors A est intégralement clos.

Exercice 11. Montrer que $A = k[X, Y]/(X^2 - Y^3)$ est intègre et s'identifie à un sous-anneau de $k[T]$.

Solution. Il suffit de montrer que $X^2 - Y^3$ est irréductible dans $k[Y][X]$ et donc dans $k(Y)[X]$. Si $X^2 - Y^3$ est réductible, alors le polynôme à une racine dans $k(Y)$ (et même dans $k[Y]$ puisque $X^2 - Y^3$ est unitaire). D'où $P \in K[Y]$ tel que $P^2 = Y^3$. Alors $2\deg(P) = 3$, ce qui aboutit à une contradiction.
Soit $f : k[X, Y] \to k[T]$ l'unique morphisme d'anneau envoyant X sur T^3 et Y sur T^2. Alors $X^2 - Y^3 \in \ker(f)$, d'où par passage au quotient un morphisme d'anneau $\phi : A \to k[T]$. Comme $X^2 - Y^3$ est unitaire, la division euclidienne nous dit que A est un $k[Y]$-module libre de base $1, X$. Soit $P(Y) + XQ(Y) \in \ker \phi$, avec $P = \sum \alpha_i Y^i$ et $Q = \sum b_j Y^j$. Alors $\phi(P(Y) + XQ(Y) = \sum a_i T^{2i} + \sum b_i T^{2j+3} = 0$. Comme $2i \neq 2j+3$, la famille $(T^{2i})_i \cup T^{2j+3}$ est k-libre et donc $a_i = b_j = 0$. Donc ϕ est injective.

Exercice 12. Déterminer les décompositions en facteurs irréductibles de
(i) 120 dans le localisé $S^{-1}\mathbb{Z}$ avec $S = \{1, 2, 2^2, \cdots, 2^n, \cdots\}$.
(ii) 120 dans le localisé $S^{-1}\mathbb{Z}$ avec $S = \mathbb{Z} - (2)$, i.e. le localisé de $\mathbb{Z}$ en l'idéal premier (2).
(iii) $X^2Y^2 - X^3 - Y^3 + XY$ dans $\mathbb{C}[X, Y]$.
(iv) $-X^2Y + X^2Z + XY^2 - XZ^2 - Y^2Z + YZ^2$ dans $\mathbb{Q}[X, Y, Z]$.
(v) $X^n - Y$ dans $k[X, Y]$ où k est un corps.
(vi) $X^n + Y^n - 1$ dans $k[X, Y]$ où k est un corps.
(vii) $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ dans $k[a_0, \cdots, a_n, X]$ où k est un corps.

Solution. (i) On commence par écrire la décomposition en facteurs premiers de 120 dans $\mathbb{Z}$:

$$120 = 2^3 \times 3 \times 5.$$

Mais alors dans $S^{-1}\mathbb{Z}$, l'élément 2 devient inversible alors que les éléments 3 et 5 restent irréductibles (on a $S^{-1}\mathbb{Z}/3S^{-1}\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$ et $S^{-1}\mathbb{Z}/5S^{-1}\mathbb{Z} = \mathbb{Z}/5\mathbb{Z}$ qui sont des corps). Ainsi on a

$$120 \diamond 15 = 3 \times 5.$$

(ii) Dans ce cas ce sont 3 et 5 qui deviennent inversibles alors que 2 reste irréductible (on a $S^{-1}\mathbb{Z}/2S^{-1}\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$ qui est un corps). Ainsi on a

$$120 \diamond 8 = 2^3.$$

(iii) On peut écrire

$$X^2Y^2 - X^3 - Y^3 + XY = (X^2 - Y)(Y^2 - X).$$

Par ailleurs on voit que $\mathbb{C}[X, Y]/(X^2 - Y)$ et $\mathbb{C}[X, Y]/(Y^2 - X)$ sont isomorphes (échanger X et Y) et on a vu à l'exercice 26 qu'ils sont principaux et donc intègres (en fait ils sont isomorphes respectivement à $\mathbb{C}[X]$ et $\mathbb{C}[Y]$). Ainsi les idéaux $(X^2 - Y)$ et $(Y^2 - X)$ sont premiers et les éléments $X^2 - Y$ et $Y^2 - X$ sont irréductibles. L'écriture précédente était donc la décomposition en facteurs irréductibles.
(iv) On peut écrire

$$-X^2Y + X^2Z + XY^2 - XZ^2 - Y^2Z + YZ^2 = (X - Y)(Y - Z)(Z - X).$$

Par ailleurs on voit que $\mathbb{C}[X, Y, Z]/(X - Y)$, $\mathbb{C}[X, Y, Z]/(Y - Z)$ et $\mathbb{C}[X, Y, Z]/(Z - X)$ sont isomorphes (échanger X, Y et Z) et ils sont isomorphes respectivement à $\mathbb{C}[X, Z]$, $\mathbb{C}[X, Y]$ et $\mathbb{C}[Y, Z]$. Ils sont donc intègres. Ainsi les idéaux $(X - Y)$, $(Y - Z)$ et $(Z - X)$ sont premiers et les éléments $X - Y$, $Y - Z$ et $Z - X$ sont irréductibles. L'écriture précédente était donc la décomposition en facteurs irréductibles.
(v) Soit $A = k[X]$, $Y - X^n$ est un polynôme unitaire de degré 1, donc irréductible.
(vi) Soit $A = k[Y]$, l'élément $p = Y - 1$ est irréductible car $k[Y]/(Y - 1) \simeq k$. Par ailleurs $Y - 1$ divise $Y^n - 1$. Ainsi si $(Y - 1)^2$ ne divise pas $Y^n - 1$, alors on est dans les hypothèses du critère d'Eisenstein.

Cependant, $(Y-1)^2$ divise Y^n-1 si et seulement si $Y-1$ divise le polynôme

$$\frac{\partial}{\partial Y}(Y^n-1)=nY^{n-1}.$$

Ceci est équivalent à dire que $n=0$ ce qui n'arrive que si la caractéristique du corps k divise n. Ainsi, si $\mathrm{car}(k)\not| \, n$, alors X^n+Y^n-1 est irréductible.
Supposons maintenant que $p=\mathrm{car}(k)\,|\,n$. On écrit alors $n=p^am$ avec $p\not| \, m$. On a alors

$$X^n+Y^n-1=(X^m)^{p^a}+(Y^m)^{p^a}-1^{p^a}$$

mais d'après l'exercice 39, pour tout u et v en caractéristique p, on a $u^p+v^p=(u+v)^p$ et $u^p-v^p=(u-v)^p$. Ainsi, on voit que

$$(X^m)^{p^a}+(Y^m)^{p^a}-(1^m)^{p^a}=(X^m)^{p^a}+(Y^m-1)^{p^a}=(X^m+Y^m-1)^{p^a}.$$

Cependant comme $p\not| \, m$, on sait que X^m+Y^m-1 est irréductible. Ainsi si $p=\mathrm{car}(k)\,|\,n$, avec $n=p^am$, $p\not| \, m$, alors on a la décomposition en irréductibles

$$X^n+Y^n-1=(X^m+Y^m-1)^{p^a}.$$

(vii) Dans $k[a_1,\cdots,a_n,X][a_0]$, $a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$ est un polynôme unitaire de degré 1

Exercice 13. Montrer que le polynôme $X_1^2+\cdots+X_n^2$ est irréductible pour $n\geq 2$ dans $\mathbb{R}[X_1,\cdots,X_n]$ et pour $n\geq 3$ dans $\mathbb{C}[X_1,\cdots,X_n]$.

Solution. Remarquons tout d'abord que si $n=1$, alors X_1^2 n'est jamais irréductible. Ensuite, si $n=2$ et qu'on se place sur le corps des nombres complexes, alors

$$X_1^2+X_2^2=(X_1+\mathrm{i}X_2)(X_1-\mathrm{i}X_2)$$

qui n'est donc pas irréductible. Il reste à montrer que dans les autres cas c'est irréductible. Voici deux méthodes.
Première méthode : supposons qu'il existe P et Q de degrés non nuls tels que $X_1^2+\cdots+X_n^2=PQ$. Alors on voit que P et Q sont de degrés 1. On écrit alors $P=\sum_i p_iX_i$ et $Q=\sum_i q_iX_i$. On a alors

$$PQ=\sum_{i=1}^n p_iq_iX_i^2+2\sum_{i<j}(p_iq_j+p_jq_i)X_iX_j.$$

On a donc $p_iq_i=1$ (donc tous les p_i et les q_i sont inversibles) et $p_iq_j+p_jq_i=0$. La dernière égalité nous donne

$$\frac{p_i}{q_i}=-\frac{p_j}{q_j}.$$

Supposons $n\geq 3$, alors on a

$$\frac{p_1}{q_1}=-\frac{p_2}{q_2},\ \frac{p_1}{q_1}=-\frac{p_3}{q_3}\text{ et }\frac{p_2}{q_2}=-\frac{p_3}{q_3}$$

ce qui donne

$$\frac{p_3}{q_3}=-\frac{p_3}{q_3}$$

c'est absurde.
Si les p_i et les q_i sont réels et que $n=2$, alors on a $p_1q_1=1$, $p_2q_2=1$ et $p_1q_2+p_2q_1=0$. En multipliant la dernière équation par p_1p_2, on obtient $p_1^2+p_2^2=0$ ce qui impose $p_1=p_2=0$ ce qui est impossible.
Deuxième méthode : on commence de la même manière : supposons qu'il existe P et Q de degrés non nuls tels que $X_1^2+\cdots+X_n^2=PQ$. Alors on voit que P et Q sont de degrés 1. On considère pour un polynôme P, l'ensemble

$$V(P)=\{(x_1,\cdots,x_n)\in k^n\ /\ P(x_1,\cdots,x_n)=0\}.$$

Dans le cas des nombres réels, l'ensemble $V(X_1^2+\cdots+X_n^2)$ est réduit au singleton $\{(0,\cdots,0)\}$. Or l'ensemble $V(PQ)=V(P)\cup V(Q)$ est la réunion de deux hyperplans (puisque P et Q sont de degré 1). Mais alors si $n\geq 2$, cette réunion contient une infinité de points et ne peut donc être réduite au singleton $\{(0,\cdots,0)\}$.
Dans le cas des nombres complexes, l'ensemble $V(Q)$ n'est plus un singleton et on ne peut raisonner de la même façon. Supposons $n\geq 3$. Alors $V(P)\cap V(Q)$ est l'intersection de deux hyperplans, elle est donc non réduite au singleton $(0,\cdots,0)$. Soit $(x_1,\cdots,x_n)\in V(P)\cap V(Q)$ non nul. Il existe donc i tel que $x_i\neq 0$. On calcule

$$\frac{\partial(X_1^2+\cdots+X_n^2)}{\partial X_i}(x_1,\cdots,x_n)=2x_i.$$

Mais on a

$$\frac{\partial PQ}{\partial X_i}(x_1, \cdots, x_n) = \frac{\partial P}{\partial X_i}(x_1, \cdots, x_n)Q(x_1, \cdots, x_n) + P(x_1, \cdots, x_n)\frac{\partial Q}{\partial X_i}(x_1, \cdots, x_n) = 0.$$

On obtient $2x_i = 0$ alors que $x_i \neq 0$, c'est absurde.