

TD n°3 - Solutions.

Exercice 1. Soit A un anneau.

Montrer que $A[\mathbb{Z}]$ est isomorphe à $A[X, Y]/(XY - 1)$.

Soit $n \geq 1$ un entier. Montrer que $A[\mathbb{Z}/n\mathbb{Z}]$ est isomorphe à $A[X]/(X^n - 1)$.

Solution. a) Se donner un morphisme $A[\mathbb{Z}] \rightarrow A[X, Y]/(XY - 1)$ de A -algèbres équivaut à se donner un morphisme de monoïdes de \mathbb{Z} vers le monoïde multiplicatif $A[X, Y]/(XY - 1)$, ou encore, puisque \mathbb{Z} est un groupe, à se donner un morphisme de groupes (abéliens) de \mathbb{Z} vers $A[X, Y]/(XY - 1)^\times$. Un morphisme de groupes abéliens est la même chose qu'un morphisme de \mathbb{Z} -module, et comme \mathbb{Z} est un \mathbb{Z} -module libre de base $\{1\}$, cela équivaut encore à ce donner un élément de $A[X, Y]/(XY - 1)^\times$. Autrement dit, étant donné $z \in A[X, Y]/(XY - 1)^\times$, il existe un unique morphisme de A -algèbres $f : A[\mathbb{Z}] \rightarrow A[X, Y]/(XY - 1)$ tel que $f(e_1) = z$. En prenant pour z la classe de X , on obtient $f : A[\mathbb{Z}] \rightarrow A[X, Y]/(XY - 1)$.

Se donner un morphisme de A -algèbres $\bar{g} : A[X, Y]/(XY - 1) \rightarrow A[\mathbb{Z}]$ équivaut à se donner un morphisme $g : A[X, Y] \rightarrow A[\mathbb{Z}]$ tel que $g(X)g(Y) - 1 = g(XY - 1) = 0$, ce qui équivaut à se donner un couple $(x, y) \in A[\mathbb{Z}]^2$ (l'image de X et l'image de Y) tel que $xy - 1 = 0$ (alors x est inversible et y est entièrement fixé par le choix de x). En prenant e_1, e_{-1} , on obtient donc un unique morphisme de A -algèbres $\bar{g} : A[X, Y]/(XY - 1) \rightarrow A[\mathbb{Z}]$ tel que $\bar{g}(\bar{X}) = e_1$.

$f\bar{g}$ envoie \bar{X} sur \bar{X} et donc $\bar{Y} = \bar{X}^{-1}$ sur lui-même. Comme $A[X, Y]/(XY - 1)$ est engendré par X, Y en tant que A -algèbre et que $f\bar{g}$ et Id envoient X et Y sur les mêmes éléments, $f\bar{g} = \text{Id}$.

De même $g\bar{f}(e_1) = e_1$, donc $g\bar{f}(e_n) = g\bar{f}(e_1^n) = g\bar{f}(e_1)^n = e_n$. Par linéarité, $g\bar{f} = \text{Id}$.

b) Se donner un morphisme $A[\mathbb{Z}/n\mathbb{Z}] \rightarrow A[X]/(X^n - 1)$ équivaut à se donner un morphisme de groupes abéliens $\mathbb{Z}/n\mathbb{Z} \rightarrow (A[X]/(X^n - 1))^\times$, ce qui équivaut à se donner un morphisme de groupes $f' : \mathbb{Z} \rightarrow (A[X]/(X^n - 1))^\times$ tel que $f'(n) = 1$, ce qui équivaut (puisque \mathbb{Z} est un \mathbb{Z} -module libre de rang 1) à se donner $z \in (A[X]/(X^n - 1))^\times$ tel que $z^n = 1$. Autrement dit, si $z^n = 1$, il existe un unique morphisme de A -algèbres $A[\mathbb{Z}/n\mathbb{Z}] \rightarrow A[X]/(X^n - 1)$ envoyant $e_{\bar{1}}$ sur z . On note f le morphisme obtenu en posant $z = \bar{X}$.

Se donner un morphisme de A -algèbres $\bar{g} : A[X]/(X^n - 1) \rightarrow A[\mathbb{Z}/n\mathbb{Z}]$ équivaut à se donner un morphisme $g : A[X] \rightarrow A[\mathbb{Z}/n\mathbb{Z}]$ tel que $g(X)^n - 1 = 0$, ce qui équivaut à se donner $x \in A[\mathbb{Z}/n\mathbb{Z}]$ tel que $x^n - 1 = 0$. En prenant $x = e_1$, on obtient un unique morphisme $\bar{g} : A[X]/(X^n - 1) \rightarrow A[\mathbb{Z}/n\mathbb{Z}]$ tel que $\bar{g}(\bar{X}) = e_1$.

$f\bar{g}(\bar{X}) = \bar{X}$, et comme $A[X]/(X^n - 1)$ est engendré par \bar{X} , $f\bar{g} = \text{Id}$. De même $\bar{g}f(e_1) = e_1$, donc $\bar{g}f(e_n) = \bar{g}f(e_1)^n = e_n$, et comme $A[\mathbb{Z}/n\mathbb{Z}]$ est engendré par les e_n , $\bar{g}f = \text{Id}$.

Exercice 2. Soit A un anneau non nul. Soit $B = A[\mathbb{N}^n]$, on note $S = \{e_\nu, \nu \in \mathbb{N}^n\} \subset B$ (S est une partie multiplicative de B). Montrer que $S^{-1}B$ est isomorphe à $A[\mathbb{Z}^n]$.

Solution. Il existe un unique morphisme $f : B \rightarrow C := A[\mathbb{Z}^n]$ envoyant e_ν sur e_ν pour tout $\nu \in \mathbb{N}^n$. Comme $f(S) \subset C^\times$, f se prolonge de façon unique en un morphisme $f' : S^{-1}B \rightarrow C$, qui est surjectif : effectivement, si $\nu \in \mathbb{Z}^n$, $\nu = a - b$ avec $a, b \in \mathbb{Z}^n$ et $e_\nu = f'(e_a/e_b)$. Si $a/s \in \ker(f')$, $0 = f'(a/s) = f(a)f'(s)^{-1}$, donc $f(a) \in \ker f$. Or f est injectif puisqu'il transforme la base $(e_\nu)_{\nu \in \mathbb{N}^n}$ du A -module B en la famille $(e_\nu)_{\nu \in \mathbb{N}^n}$, qui est une famille libre du A -module C . Donc f est un isomorphisme.

Exercice 3. Soit $A = \mathbb{C}[\mathbb{Z}]$. On notera $X = e_1$.

- Montrer que tout élément a non nul de A peut s'écrire de façon unique sous la forme $a = X^m P(X)$ où $m \in \mathbb{Z}$ et P est un polynôme de terme constant non nul. On note $e(a) = \deg(P)$.
- Soient $a, b \in A$ montrer qu'il existe $q, r \in A$ tels que $a = bq + r$ et : $r = 0$ ou $e(r) < e(b)$.
- En déduire que A est principal.

Solution. a) Ecrivons $a = \sum_{i \in \mathbb{Z}} a_i X^i$. Si $a = X^m P(X)$ avec $P(0) \neq 0$, alors $a_i \neq 0$ implique $i \geq m$ et $a_m \neq 0$: cela caractérise m comme devant être $\min\{i, a_i \neq 0\}$. D'où l'unicité. Réciproquement, posons $m = \min\{i, a_i \neq 0\}$, alors $P = X^{-m}a$ est bien un polynôme en X et son coefficient constant est bien non nul.

- Ecrivons $a = X^m P_1(X)$ et $b = X^n P_2(X)$ comme dans la question précédente, et soit $P_1 = QP_2 + R$ la division euclidienne de P_1 par P_2 . Alors $a = X^{m-n}Qb + X^m R$, avec $e(X^m R) \leq \deg(R) < \deg(P_2) = e(b)$. D'où le résultat en posant $q = X^{m-n}Q$ et $r = X^m R$.

c) D'après la question précédente, A est un anneau euclidien, donc principal.

Exercice 4. Montrer que dans un anneau principal A , les idéaux premiers sont maximaux.

Solution. Soit \mathfrak{p} un idéal premier et soit \mathfrak{m} un idéal le contenant. Comme l'anneau est principal, on peut écrire $\mathfrak{p} = (p)$ et $\mathfrak{m} = (m)$. Le fait que $\mathfrak{p} \subset \mathfrak{m}$ se traduit par : $p = am$ avec $a \in A$. Mais alors comme \mathfrak{p} est premier, on a $a \in \mathfrak{p}$ ou $m \in \mathfrak{p}$. Si $m \in \mathfrak{p}$, alors $\mathfrak{p} = \mathfrak{m}$ et on a fini. Sinon, alors $a \in \mathfrak{p}$ donc il existe $u \in A$ tel que $a = up$ donc $p = upm$ et comme A est intègre (car principal) on a $1 = um$ donc m est inversible et $\mathfrak{m} = A$. L'idéal \mathfrak{p} est donc maximal.

Exercice 5. 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 6. 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 $k = \text{Frac}(A)[X]$.

- 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) Montrer 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 $A \rightarrow A/(p)$ 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 $p \nmid p_i$ et $p \nmid q_j$. Calculons $(PQ)_{i_0+j_0} = \sum_{i+j=i_0+j_0} p_i q_j$. Donc $p \mid p_{i_0} q_{j_0}$. 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 $B \in \text{Frac}(A)[X]$. On peut multiplier par d , tel que $dB \in A[X]$ et $c(dB) = 1$. On alors $(dB) \cdot P = dQ$. Mais $d \mid c(dQ) = c(dB)c(P) = 1$ donc d est inversible et $B \in A[X]$.

Exercice 7. 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 polynôme 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 $X^4 + X^2 Y^3 + Y$ 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 polynôme 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. (i) 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 $P_0 Q_0$ 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 8. 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 .

- 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.
- Montrer que si A est factoriel, alors A est intégralement clos.

Exercice 9. Montrer que $A = k[X, Y]/(X^2 - Y^3)$ est intègre et s'identifie à un sous-anneau de $k[T]$. Montrer que A n'est pas intégralement clos (et donc en particulier n'est pas factoriel).

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 $f : k[X, Y] \rightarrow k[T]$ 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 $\phi : A \rightarrow k[T]$. 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 $\phi(P(Y) + XQ(Y)) = \sum a_i T^{2i} + \sum b_j T^{2j+3} = 0$. 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 10. Déterminer les décompositions en facteurs irréductibles de

- 120 dans le localisé $S^{-1}\mathbb{Z}$ avec $S = \{1, 2, 2^2, \dots, 2^n, \dots\}$.
- 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) .
- $X^2Y^2 - X^3 - Y^3 + XY$ dans $\mathbb{C}[X, Y]$.
- $-X^2Y + X^2Z + XY^2 - XZ^2 - Y^2Z + YZ^2$ dans $\mathbb{Q}[X, Y, Z]$.
- $X^n - Y$ dans $k[X, Y]$ où k est un corps.
- $X^n + Y^n - 1$ dans $k[X, Y]$ où k est un corps.
- $a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ dans $k[a_0, \dots, a_n, X]$ 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 $\text{car}(k) \nmid n$, alors $X^n + Y^n - 1$ est irréductible.

Supposons maintenant que $p = \text{car}(k) \mid n$. On écrit alors $n = p^a m$ avec $p \nmid m$. 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 $p \nmid m$, on sait que $X^m + Y^m - 1$ est irréductible. Ainsi si $p = \text{car}(k) \mid n$, avec $n = p^a m$, $p \nmid m$, alors on a la décomposition en irréductibles

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

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

Exercice 11. Montrer que le polynôme $X_1^2 + \dots + X_n^2$ est irréductible pour $n \geq 2$ dans $\mathbb{R}[X_1, \dots, X_n]$ et pour $n \geq 3$ dans $\mathbb{C}[X_1, \dots, X_n]$.

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

$$X_1^2 + X_2^2 = (X_1 + iX_2)(X_1 - iX_2)$$

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 $X_1^2 + \dots + X_n^2 = PQ$. Alors on voit que P et Q sont de degrés 1. On écrit alors $P = \sum_i p_i X_i$ et $Q = \sum_i q_i X_i$. On a alors

$$PQ = \sum_{i=1}^n p_i q_i X_i^2 + 2 \sum_{i < j} (p_i q_j + p_j q_i) X_i X_j.$$

On a donc $p_i q_i = 1$ (donc tous les p_i et les q_i sont inversibles) et $p_i q_j + p_j q_i = 0$. 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 $p_1 q_1 = 1$, $p_2 q_2 = 1$ et $p_1 q_2 + p_2 q_1 = 0$. En multipliant la dernière équation par $p_1 p_2$, 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 $X_1^2 + \dots + X_n^2 = PQ$. Alors on voit que P et Q sont de degrés 1. On considère pour un polynôme P , l'ensemble

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

Dans le cas des nombres réels, l'ensemble $V(X_1^2 + \dots + X_n^2)$ est réduit au singleton $\{(0, \dots, 0)\}$. 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 $\{(0, \dots, 0)\}$.

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 $(0, \dots, 0)$. Soit $(x_1, \dots, x_n) \in V(P) \cap V(Q)$ non nul. Il existe donc i tel que $x_i \neq 0$. On calcule

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

Mais on a

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

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

Exercice 12. Soit $P = a_n X^n + \dots + a_0$ un élément de $\mathbb{Z}[X]$. Et soit $r = \frac{p}{q} \in \mathbb{Q}$ une racine de P

- a) $qX - p$ divise P .
- b)
 - i) En déduire que $p|a_0$
 - ii) En déduire que $q|a_n$
 - iii) En déduire que $p - q|P(1)$
 - iv) En déduire que $p + q|P(-1)$.
- c) Trouver les racines rationnelles de $A(x) = x^3 - 6x^2 + 15x - 14$ et $B(x) = x^4 - 2x^3 - 8x^2 + 13x - 24$.

Solution. a) Dans $\mathbb{Q}[X]$, on $X - p/q|P$, donc $qX - p$ divise P dans $\mathbb{Q}[X]$. $c(qX - p) = 1$ donc $qX - p$ divise P dans $\mathbb{Z}[X]$. On a donc $P = (qX - p)Q$.

- b)
 - i) On déduit de $P(0) = -pQ(0)$.
 - ii) On a $a_n = qq_{n-1}$.
 - iii) On a $P(1) = (q - p)Q(1)$
 - iv) On a $P(-1) = -(p + q)Q(-1)$.
- c) Racines de $x^3 - 6x^2 + 15x - 14$. On trouve que $p|14, q|1, p+q|36, p-q|4$. Les conditions restent inchangées par la transformation $(p, q) \mapsto (-p, -q)$. On a donc $q = 1, p \in \{-1, 0, 1, 2, 3, 5\} \cap \{-7, -2, -1, 1, 2, 7\} = \{1, 2\}$.
On trouve $p = 2, q = 1$.
Racines de $x^4 - 2x^3 - 8x^2 + 13x - 24$. On trouve $q = 1, p|24, p+1|42, p-1|20$. On obtient $p = -3$.

Exercice 13. a) Trouver un pgcd de $X^6 - 1$ et de $X^4 - 1$ dans $\mathbb{C}[X]$, par factorisation et par l'algorithme d'Euclide.

- b) Résoudre dans $\mathbb{C}[X]^2$, l'équation $P(X)(X^6 - 1) + Q(X)(X^4 - 1) = X^3 + 2X^2 - X - 2$.
- c) Résoudre la même équation dans $\mathbb{R}[X]$.

Solution.

Exercice 14. Soit p un nombre premier.

Montrer que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_p[X]/(X^2 + 1)$.

EN déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans \mathbb{F}_p .

Exercice 15. Factorisations et congruences

- a) Soit $P(X) = X^4 + 1$. Décomposer P dans $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$ en produits de facteurs irréductibles.
- b) Montrer que $-1, 2$ ou -2 est un carré dans \mathbb{F}_p pour tout p .
- c) Montrer que $X^4 + 1$ est factorisable dans \mathbb{F}_p (on utilisera les égalités $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - 1)^2 + 2X^2 = (X^2)^2 - (-1)$).
- d) Factoriser $Q(X) = X^5 - X - 1$ dans $\mathbb{F}_5[X]$ (on vérifiera que si x est un élément d'une extension de degré 2 de \mathbb{F}_5 , alors $x^{25} = x$) et en déduire que $X^5 - X - 1$ est irréductible dans $\mathbb{Q}[X]$.
- e) Montrer que $X^5 - X^2 - 1$ est irréductibles dans $\mathbb{Q}[X]$.

Solution. On a $X^4 + 1 = (X^2 + i)(X^2 - i) = (X + \frac{1+i}{\sqrt{2}})(X - \frac{1+i}{\sqrt{2}})(X + \frac{1-i}{\sqrt{2}})(X - \frac{1-i}{\sqrt{2}})$.

On a $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$.

Si $X^4 + 1$ n'était pas irréductible dans $\mathbb{Q}[X]$, alors ce serait aussi une factorisation dans $\mathbb{R}[X]$. Or l'unique factorisation non triviale dans $\mathbb{R}[X]$ n'est pas rationnelle. Donc $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$.

Puisque $X^4 + 1$ est unitaire, il est aussi irréductible dans $\mathbb{Z}[X]$.

- a) Si $p = 2$, -1 est un carré. Si p est impair et si (-1) et 2 ne sont pas des carrés, alors $(-1)^{(p-1)/2} = 2^{(p-1)/2} = -1$ donc $(-2)^{(p-1)/2} = 1$ et -2 est un carré.

- b) $X^5 - X - 1$ est irréductible dans $\mathbb{F}_5[X]$. En effet il n'a pas de racine car $x^5 = x$ et s'il y avait un facteur de degré 2, alors il y aurait une racine dans une extension K de degré 2 de \mathbb{F}_5 . Comme $\text{Card } K = 25$ et donc $\text{Card } K^* = 24$, $x^4 = 1$ pour $x \neq 0$ et donc $x^5 = x$. Mais si $x^5 = x + 1$, alors $x^{25} = (x + 1)^5 = 1 + x^5 = 1 + 2x \neq x$ car $x \neq -1$. Donc $X^5 - X - 1$ est irréductible dans $\mathbb{F}_5[X]$ et donc dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.
De même avec $X^5 - X^2 - 1$. Si x est une racine dans \mathbb{F}_5 alors $x^5 = x^2 + 1 = x$ et on vérifie qu'il n'y a pas de tel solution. Si x est une racine dans une extension K de \mathbb{F}_5 de degré 2, on a $x = x^{25} = (x^2 + 1)^5 = x^{10} + 1 = (x^2 + 1)^2 + 1 = x^4 + 2x^2 + 2$. En calculant le pgcd de $X^5 - X^2 - 1$ et $X^4 + 2X^2 - X + 2$, on tombe sur $X^2 + X + 2$.
On obtient $X^5 - X^2 - 1 = (X^3 - X^2 - X + 2)(X^2 + X + 2) = \bar{P}\bar{Q}$ dans $\mathbb{F}_5[X]$ et on vérifie que les deux facteurs sont irréductibles (car ils n'ont pas de racine dans \mathbb{F}_5). Donc si $X^5 - X^2 - 1 = PQ$ dans $\mathbb{Z}[X]$ alors par unicité de la factorisation dans $\mathbb{F}_5[X]$, on obtient $P(0) \equiv 2 \pmod{5}$, or $P(0)Q(0) = -1$ est inversible dans \mathbb{Z} , donc $P(0) = 1$ ou -1 . Contradiction. $X^5 - X^2 - 1$ est bien irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$.

Exercice 16. Quels sont les polynômes irréductibles de degré inférieur à 4 dans $\mathbb{F}_2[X]$?

Solution.

Exercice 17. Montrer que $P(X) = (X - a_1) \cdots (X - a_n) - 1$ est irréductible dans $\mathbb{Q}[X]$ si les a_i sont des entiers distincts.

Solution. Il suffit de montrer qu'il est irréductible dans $\mathbb{Z}[X]$. Si $P = QR$ avec Q et R non constants, alors $Q(a_i)R(a_i) = -1$ pour tout i , donc $Q(a_i) \in \{1, -1\}$. Donc $Q + R$ s'annule en tous les a_i , or $\deg Q + R < n$, donc $Q = -R$. Donc $P = -Q^2$, se qui contredit la positivité du coefficient dominant.

Exercice 18. a) Soit R un anneau euclidien. Montrer qu'il existe $x \in R$ non inversible tel que $R^* \cup \{0\} \rightarrow R/(x)$ soit surjective.

b) Soit $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Déterminer A^* et montrer que A n'est pas euclidien.

c) Soit $x \in \mathbb{C}$. On veut montrer qu'il existe $q \in A$ tel que $|x - q| < 1$ ou $|2x - q| < 1$. On pose $x = u + iv$ avec $u, v \in \mathbb{R}$.

i) Se ramener au cas où $v \in [0, \sqrt{19}/4]$.

ii) Montrer que si $v \in [0, \sqrt{3}/2[$, il existe $q \in \mathbb{Z}$ tel que $|x - q| < 1$.

iii) Montrer que si $v \in [\sqrt{3}/2, \sqrt{19}/4]$, $\sqrt{19}/2 - 2v \in [0, \sqrt{3}/2[$ et en déduire $q \in A$ tel que $|2x - q| < 1$.

d) Soient $a, b \in A \setminus 0$. Montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.

e) Montrer que (2) est un idéal maximal de A (on pourra soit écrire la table de multiplication de $A/(2)$, soit vérifier que $X^2 + X + 5$ est un polynôme irréductible de $\mathbb{Z}/(2)[X]$).

f) Soit I un idéal de A et $b \in I - \{0\}$ minimisant $|b|$. Montrer que $2I \subset (b) \subset I$.

g) Montrer que A est principal.

Solution. a) Soit $x \in R - (R^* \cup \{0\})$ tel que $v(x)$ soit minimal. Alors si $y \in R$, il existe $q, r \in R$ tel que $y = qx + r$ (et donc $\bar{y} = \bar{r}$) et $v(r) < v(x)$, donc $r \in R^* \cup \{0\}$. Donc \bar{y} est l'image de r par l'application $R^* \cup \{0\} \rightarrow R/(x)$

b) Soit $N(z) = z\bar{z} \in \mathbb{Z}$. Alors z est inversible si et seulement si $N(z) = 1$. Mais si $z = a + b\frac{1+i\sqrt{19}}{2}$, $N(z) \geq 19b^2/4 > 1$ dès que $b \neq 0$. On en déduit $R^* = \{1, -1\}$.

Si x est tel que $R^* \cup \{0\} \rightarrow R/(x)$ est surjective, alors si $y \in R$, x divise y , $y + 1$ ou $y - 1$, et donc $N(x)$ divise $N(y)$, $N(y + 1)$ ou $N(y - 1)$. En prenant $y = 2$, on obtient $N(x)$ divise 1, 4 ou 9 et en prenant $y = (1 + i\sqrt{19})/2$, on obtient $N(x)$ divise 5 ou 7. Comme $1 \times 4 \times 9$ et 5×7 sont premiers entre eux, $N(x) = 1$ ce qui contredit l'hypothèse que x n'est pas inversible. Donc R n'est pas euclidien.

c) i) Soit $n \in \mathbb{Z}$ tel que $|4v/\sqrt{19} - n| \leq 1/2$. Soit $x' = x - n\frac{1+i\sqrt{19}}{2}$. Il suffit de résoudre le problème pour x' . On pose $x' = u' + iv'$. On a $v' \in [-\sqrt{19}/4, \sqrt{19}/4]$. Si $v' \geq 0$, on s'est ramené au cas voulu ; sinon, on remplace x' par $-x'$.

ii) Soit $n \in \mathbb{Z}$ tel que $|u - n| \leq 1/2$. Alors $|x - n|^2 = |u - n|^2 + |v|^2 < 1/4 + 3/4 = 1$.

iii) Comme $v \leq \sqrt{19}/4$, on a $\sqrt{19}/2 - 2v \geq 0$. Pour l'autre inégalité, il suffit de vérifier que $3\sqrt{3}/2 \geq \sqrt{19}/2$, ce qui provient du fait que $27 \geq 19$.

Du coup, $\frac{1+i\sqrt{19}}{2} - 2x$ vérifie les conditions de ii), d'où $n \in \mathbb{Z}$ tel que $|\frac{1+i\sqrt{19}}{2} - 2x - n| < 1$ et il suffit de poser $q = \frac{1+i\sqrt{19}}{2} - n$.

- iv) On applique c) à $x = a/b$ et on pose $r = b(x - q) = a - bq$ ou $r = b(2x - q) = 2a - bq$ en fonction des cas.
- d) Le nombre $\frac{-1+i\sqrt{19}}{2}$ est racine de $X^2 + X + 5$, d'où un morphisme surjectif $f : \mathbb{Z}[X]/(X^2 + X + 5) \rightarrow \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ envoyant X sur $\frac{1+i\sqrt{19}}{2}$. Comme les deux sont des \mathbb{Z} -modules libres de rang 2, et que f envoie la base $(1, X)$ sur la base $(1, \frac{1+i\sqrt{19}}{2})$, c'est un isomorphisme. Il suffit donc de montrer que $A/(2) = \mathbb{Z}[X]/(X^2 + X + 5, 2) = \mathbb{F}_2[X]/(X^2 + X + 5)$ est un corps, et donc de montrer que $P = X^2 + X + 5$ est irréductible sur \mathbb{F}_2 . Comme le degré de P est 2 il suffit de vérifier qu'il n'y a pas de racines dans \mathbb{F}_2 , ce qui est immédiat.
- e) Remarquons que $|z|^2 \in \mathbb{N}$ donc il existe bien $b \in I - \{0\}$ minimisant $|b|^2$. Comme $b \in I$, $(b) \subset I$. Si $a \in I$. On applique c) : si $a = bq + r$, alors $r = a - bq \in I$ et par minimalité de $|b|$, $r = 0$, donc $a \in (b)$ et donc $2a \in (b)$. Si $2a = bq + r$ alors $2a \in (b)$ par le même argument.
- f) On a $(2b) \subset 2I \subset (b)$, or $(b)/(2b) \simeq A/(2)$ est un A -module simple, donc $2I = (b)$ ou $(2b)$ est principal. Comme A est intègre, I est principal aussi.