M1-Algèbre. Lyon1.

EXEMPLES D'ANNEAUX NON FACTORIELS.

On étudie ici l'anneau $A := \mathbb{C}[X,Y]/(X^2 - Y^3)$ en mettant l'accent sur les obstructions à la factorialité. De façon sous-jacente, nous allons voir que l'anneau A "voit" les propriétés de la courbe d'équation $X^2 - Y^3 = 0$.

1 Etude directe.

Pour étudier le quotient, on va tout d'abord voir comment représenter les éléments de A de manière agréable :

Propriété. Tout élément de A s'écrit sous la forme $\overline{P_1 X + P_0}$ avec P_0, P_1 uniques dans $\mathbb{C}[Y]$.

Preuve : Il suffit de choisir un élément $\bar{S}$ de A qui se relève en un élément S de $\mathbb{C}[X,Y]$ et d'effectuer la division euclidienne de S par $X^2 - Y^3$, vu comme polynôme unitaire de $\mathbb{C}[Y][X]$. On obtient bien $S = (X^2 - Y^3)Q + P_1 X + P_0$, d'où l'écriture modulo $(X^2 - Y^3)$. L'unicité provient de l'unicité de la division euclidienne dans $\mathbb{C}(Y)[X]$.

Attention. $\mathbb{K}[X]$ et $\mathbb{Z}$ sont des anneaux euclidiens particuliers puisqu'il y a unicité du quotient et du reste !

Maintenant qu'on a mis en place l'outil principal, il reste à faire l'étude générale de l'anneau :

Propriété. On a

(i) A est un anneau intègre.
(ii) Y n'est pas premier.
(iii) Y est un irréductible de l'anneau.
(iv) L'anneau A n'est pas factoriel.

Preuve : (i) Il suffit de montrer que $(X^2 - Y^3)$ est irréductible puisque $\mathbb{C}[X,Y]$ est factoriel. On le regarde comme polynome de $\mathbb{C}[Y][X]$. Son contenu est 1, et donc il suffit de montrer qu'il est irréductible dans $\mathbb{C}(Y)[X]$. Comme il est de degré 2, il suffit de voir qu'il ne possède pas de racine dans $\mathbb{C}(Y)$. Supposons par l'absurde S/R, $S, R \in \mathbb{C}[Y]$ tels que $(S/R)^2 = Y^3$ ce qui implique $S^2 = R^2 Y^3$. La parité du degré montre que cela est impossible.

(ii) On a

$$A/(Y) \simeq \mathbb{C}[X,Y]/(X^2 - Y^3, Y) = \mathbb{C}[X,Y]/(X^2, Y) \simeq (\mathbb{C}[X,Y]/Y)/(X^2) \simeq \mathbb{C}[X]/(X^2).$$

Il est donc clair que $A/(Y)$n'est pas intègre.

(iii) On suppose que $Y = (P_1 X + P_0)(Q_1 X + Q_0)$, il vient alors

$$(P_1 Q_0 + P_0 Q_1)X + P_1 Q_1 Y^3 + P_0 Q_0 = Y,$$

dans A, et donc $P_1Q_0 + P_0Q_1 = 0$ et $P_1Q_1Y^3 + P_0Q_0 = Y$ dans $\mathbb{C}[Y]$ par unicité ! En évaluant en 0 la seconde équation, il vient $P_0(0)Q_0(0) = 0$. On peut supposer $P_0(0) = 0$ par symétrie. Il vient que Y divise P_0. En reportant cela dans la première équation, il vient que Y divise P_1Q_0 (dans $\mathbb{C}[Y]$).
Si Y divise Q_0, alors Y^2 divise $P_1Q_1Y^3+P_0Q_0 = Y$, absurde. Il vient que Y divise P_1, donc il divise $P_1X + P_0$ et par conséquent $Q_1X + Q_0$ est inversible puisque $Y = (P_1X + P_0)(Q_1X + Q_0)$.

Attention ! Ce n'est pas fini. Il faut aussi montrer que Y n'est pas inversible, mais s'il n'était, on aurait $A/(Y) = 0$ ce qui contredirait le résultat plus haut.
(iv) Cela résulte de (ii) et (iii) et de la caractérisation des anneaux factoriels. ⋄

Pour le fun : faire une preuve plus pietonne du fait que Y n'est pas premier (Y divise X^2 mais ne divise pas X) et que Y n'est pas inversible (en calquant la preuve sur celle de (iii)) :

Supposons Y inversible dans A. On a donc $Y(Q_1X + Q_0) = 1$ dans A et donc $Q_1X + YQ_0 = 1$ dans $\mathbb{C}[Y]$ par l'unicité de la decomposition. En évaluant en $(0, 0)$, on voit que c'est absurde.

2 Etude via une paramétrisation.

En fait la courbe d'équation implicite $X^2 - Y^3 = 0$ se paramétrise en $X = T^3$, $Y = T^2$. Cela se retrouve au niveau des anneaux :

Propriété. $A \simeq \mathbb{C}[T^2, T^3]$.

Preuve : La propriété universelle permet de fournir un morphisme ϕ de $\mathbb{C}[X, Y] \to \mathbb{C}[T^2, T^3]$, tel que $\phi(X) = T^3$ et $\phi(Y) = T^2$. ϕ est clairement surjectif. Il suffit de montrer que $\ker\phi = (X^2 - Y^3)$.
L'inclusion inverse est évidente car $(T^3)^2 - (T^2)^3 = 0$.
Reste à montrer l'inclusion. Soit S dans $\ker\phi$ et $S = (X^2 - Y^3)Q + P_1X + P_0$, la division euclidienne avec P_0, P_1 dans $\mathbb{C}[Y]$. Il vient que $P_0(T^2) + T^3P_1(T^2) = 0$. En regardant la parité des degrés de $P_0(T^2)$ et de $T^3P_1(T^2) = 0$, on voit que $P_0 = P_1 = 0$. ⋄

Cet isomorphisme permet de montrer facilement que A est intègre, non factoriel, que les unités de A sont les constantes non nulles, que X et Y sont irréductibles...
On peut voir aussi les phénomènes suivants :
1. XY et Y^3 n'ont pas de PGCD dans A. Il suffit de voir pour cela que T^5 et T^6 n'ont pas de PGCD dans $\mathbb{C}[T^2, T^3]$. Effectivement, T^2 et T^3 sont tous deux des diviseurs minimaux de T^5 et T^6 !
2. $A[Y^{-1}]$ est factoriel (et même principal). Cela provient du fait que $\mathbb{C}[T^2, T^3][T^{-2}]$ contient T et T^{-1}, donc par double inclusion, on a que $\mathbb{C}[T^2, T^3][T^{-2}] = \mathbb{C}[T, T^{-1}] = \mathbb{C}[T][T^{-1}]$, qui est principal car il s'agit du localisé d'un anneau principal.
En géométrie algébrique, cela signifie que, une fois débarrassé du point $(0, 0)$ la courbe d'équation $X^2 = Y^3$ n'a pas de point singulier...

3 Contre-exemples

Dans cette partie, on note K le corps des fractions de l'anneau A.
Exemples d'irréductibles non premiers : Dans l'exemple précédent, $\bar{X}$ et $\bar{Y}$ sont des irréductibles non premiers.
De la même manière, si on travaille sur $A := \mathbb{Z}[i\sqrt{5}]$, on a que l'anneau A n'est pas factoriel. Effectivement, $(1+i\sqrt{5})(1-i\sqrt{5}) = 2\times 3$ alors que tous les facteurs en jeu sont irréductibles. Par exemple 2 a pour norme $N(2) = 4$, donc si z est un irréductible qui divise 2, on a forcément que $N(z) = 2$ ou 4. Or, $a^2 + 5b^2 = 2$ n'a pas de solution dans $\mathbb{Z}$ donc $N(z) = 4$ et donc $z = 2$ modulo les inversibles de A. Il vient que modulo 2, $(1+i\sqrt{5})$ et $(1-i\sqrt{5})$ sont non nuls (puisque 2 ne les divise pas) alors que leur produit est nul. Ainsi, 2 n'est pas premier. (*Ce qu'on pourrait voir aussi en disant que* $A/(2) \simeq \mathbb{F}_2/(X^2+5) = \mathbb{F}_2/(X^2+1) = \mathbb{F}_2/(X+1)^2$).
Exemples de polynômes primitifs irréductibles sur $A[X]$ mais non irréductibles sur $K[X]$: Si $A = \mathbb{C}[X,Y]/(X^2-Y^3)$, on prend le polynôme $Z^2 - Y \in A[Z]$. Il est bien primitif puisqu'il est unitaire. Il se réduit sur $K[Z]$ puisque le corps des fractions de A contient $T = T^3/T^2 = X/Y$, via l'isomorphisme ϕ, et que $Z^2 - Y = Z^2 - T^2 = (Z-T)(Z+T)$. Mais il est irréductible sur A sinon il aurait une racine dans A alors que $T \notin A$.
De même, si $A := \mathbb{Z}[i\sqrt{5}]$, alors le polynôme $X^2 + X + 1$ est primitif, réductible sur le corps des fractions K de A car $X^2 + X + 1 = (X - j)(X - j^2)$ et $j \in K$. Mais il est irréductible sur A car $j \notin A$.
L'idée derrière ces contre-exemples est la suivante : si A est factoriel, et si $P \in A[X]$ unitaire, alors $P(z) = 0$, avec $z \in K$ implique $z \in A$. Ceci se montre facilement en prenant $z = p/q$, avec p premier avec q et en utilisant le lemme de Gauss...