EPFL - Printemps 2022	Prof. Z. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 7	

Exercice 1. 1. Soit A un anneau euclidien, avec une fonction euclidienne $\nu\colon A\setminus\{0\}\to\mathbb{N}$. Etant donnés $a_0\in A$ et $0\neq a_1\in A$, on construit une suite d'éléments $a_i\in A$ de la manière récursive suivante :

(a) a_0, a_1 sont donnés ;

(b) pour $i\geq 1$, si $a_i\neq 0$, il existe une expression $a_{i-1}=a_iq_i+a_{i+1}$ où $\nu(a_{i+1})<\nu(a_i)$.

La condition $\nu(a_{i+1})<\nu(a_i)$ implique que l'algorithme s'arrête, c'est-à-dire qu'il existe un n tel que $a_{n+1}=0$. On prétend que

$$a_n \text{ est un pgdc de } a_0 \text{ et } a_1.$$

Prouvons cette assertion. On prétend d'abord que a_n divise tous les a_i ($i\leq n$). On procède par induction descendante sur i. Puisque $a_{n+1}=0$, on a $a_n|a_{n-1}$. Si a_n divise $a_i,\dots,a_n$, alors comme

$$a_{i-1}=a_iq_i+a_{i+1}$$

on voit que a_n divise a_{i-1}.

On prétend ensuite que si b divise a_0 et a_1, alors b divise a_n. En effet, comme $a_2=a_0-a_1q_1$, on voit que b divise a_2 ; et par induction croissante sur i, on voit que b divise tous les a_i, en particulier a_n.

La combinaison de ces deux observations montre que a_n est un pgdc de a_0 et de a_1.

Faisons la remarque suivante, qui sera utile dans la suite : si une étape de l'algorithme fournit une unité, c'est-à-dire si $a_i\in A^\times$ pour un certain i, alors a_0 et a_1 sont premiers entre eux. En effet, puisque a_i est une unité, l'étape suivante sera

$$a_{i-1}=(a_{i-1}a_i^{-1})a_i+0$$

donc $a_{i+1}=0$ et ainsi a_i est un pgdc de a_0 et a_1. Par définition cela implique que a_0 et a_1 sont premiers entre eux.

2. La division de $27-23i$ par $8+i$ donne $\frac{193}{65}-\frac{211}{65}i$. On arrondit au nombre entier le plus proche pour trouver $q=3-3i$. Attention : on ne peut pas arrondir indifféremment vers le haut ou vers le bas, sans quoi le reste de la division aura une norme trop grande ! On calcule alors

$$27-23i=(3-3i)(8+i)+(-2i)$$

Le reste vaut donc $-2i$. On poursuit la recherche du pgdc avec l'algorithme d'Euclide dans cet anneau euclidien. Comme

$$8+i=-4i^2+i=4i\cdot(-2i)+i$$

Le reste de cette division est i, un élément inversible de $\mathbb{Z}[i]$. On conclut que ces deux nombres sont premiers entre eux.

3. On calcule $11+3i=(1-i)(1+8i)+2-4i$. La division suivante $\frac{1+8i}{2-4i}=\frac{(1+8i)(2+4i)}{20}=\frac{-3+2i}{2}$ et nous retrouvons la possibilité de choisir deux quotients distincts : $q=-1+i$ ou $q'=-2+i$. Les restes correspondants sont $r=-1+2i$ et $r'=1-2i$ respectivement. Dans les deux cas on constate que $2-4i$ est un multiple de ce reste.

Ainsi le dernier reste non nul dans l'algorithme d'Euclide est $-1+2i$ ou $1-2i$. Chacun est un pgdc (de norme 5).

Exercice 2. 1. Pour $x \in [0,1]$, considérons l'application d'évaluation

$$\mathrm{ev}_x \colon \mathcal{C} \to \mathbb{R}, \quad f \mapsto f(x).$$

Alors ev_x est surjective et $\ker \mathrm{ev}_x = I_x$. Donc $\mathcal{C}/I_x \cong \mathbb{R}$ par le premier théorème d'isomorphisme, et ainsi I_x est maximal puisque $\mathbb{R}$ est un corps.

2. Il est facile de trouver $f, g \in \mathcal{C}$ tels que $f(x) = 0 = g(y)$ et $f(y) \neq 0 \neq g(x)$ (on peut construire de telles fonctions linéaires par parties). Donc ni f ni g n'appartient à $I_x \cap I_y = \{h \in \mathcal{C} \mid h(x) = 0 = h(y)\}$, tandis que $fg \in I_x \cap I_y$.
3. Pour chaque $x \in [0,1]$, par hypothèse il existe $0 \neq f_x \in I$ tel que $f_x(x) \neq 0$. Puisque f_x est continue, l'ensemble $\mathcal{U}_x := \{y \in [0,1] \mid f_x(y) \neq 0\}$ est ouvert (dans la topologie euclidienne de $[0,1]$) et contient x. Ainsi

$$[0,1] = \bigcup_{x \in [0,1]} \mathcal{U}_x.$$

Puisque la topologie euclidienne fait de $[0,1]$ un espace compact, la propriété de Heine–Borel implique qu'il existe $x_1, \ldots, x_n \in [0,1]$ tels que

$$[0,1] = \bigcup_{i=1}^{n} \mathcal{U}_{x_i}.$$

Considérons maintenant la fonction continue

$$F := \sum_{i=1}^{n} f_{x_i}^2.$$

Alors $F \in I$ et par construction F est strictement positive sur $[0,1]$. Ainsi $1/F \in \mathcal{C}$, et $1 = F \cdot 1/F \in I$. Donc $I = \mathcal{C}$.

4. Soit $I \subset \mathcal{C}$ un idéal maximal. En vertu du point précédent, puisque $I \neq \mathcal{C}$ il existe un I_x tel que $I \subseteq I_x$. Puisque I est maximal, on en déduit que $I = I_x$.

Il est également possible de définir une topologie sur l'ensemble $\{I_x \mid x \in [0,1]\}$ (la topologie la moins fine pour laquelle les sous-ensembles $\{I_x \mid f \in I_x\}$ sont ouverts pour des $f \in \mathcal{C}$ quelconques), pour laquelle la bijection

$$[0;1] \to \{\text{idéaux maximaux de } \mathcal{C}\}, \quad x \mapsto I_x$$

devient un homéomorphisme. En d'autres termes, il est possible de reconstruire l'espace topologique $[0,1]$ à partir de son anneau de fonctions réelles continues. C'est une forme de *dualité* entre $[0,1]$ et $\mathcal{C}$. Le même résultat est vrai plus généralement pour les espaces topologiques Hausdorff et compacts.

Exercice 3. 1. On vérifie que

$$f(x) = (x-2)(x^2+1) \quad \text{et} \quad g(x) = (x-2)(x^3+7),$$

et on prétend que x^2+1 et x^3+7 sont premiers entre eux. En fait, ceux deux polynômes sont primitifs et ne se décomposent pas dans $\mathbb{Q}[x]$ (car -1 n'as pas de racine carrée dans $\mathbb{Q}$, et -7 n'a pas de racine cubique dans $\mathbb{Q}$), donc en vertu de la Proposition 3.8.13 ils sont irréductibles dans $\mathbb{Z}[x]$. Ainsi $x-2$ est un pgdc de f et de g.

2. Voir le point précédent.
3. Les décompositions $f = (x-2)(x^2+1)$ et $g = (x-2)(x^3+7)$ sont encore valables après la réduction modulo p. Après cette réduction, le pgdc n'est plus égal à $x - [2]_p$ si et seulement si $x^2 + [1]_p$ et $x^3 + [7]_p$ ne sont plus premiers entre eux dans $\mathbb{F}_p[x]$.

Notons qu'on peut écrire (en suivant la méthode de l'algorithme d'Euclide, même si $\mathbb{Z}[x]$ n'est pas euclidien) :

$$x^3+7 = x(x^2+1)+(-x+7), \quad x^2+1 = (-x-7)(-x+7)+50$$

et ces égalités sont encore valables modulo p. En fait, comme $\mathbb{F}_p[x]$ est un anneau euclidien dont la fonction euclidienne est donnée par le degré, la réduction modulo p de ces deux égalités donne les deux premiers pas de l'algorithme d'Euclide pour $x^3+[7]_p$ et $x^2+[1]_p$ (voir l'Exercice 1.1). Notons que le second reste est $[50]_p$. Si $[50]_p = 0$, alors l'algorithme est complet et

$$\text{pgdc}(x^2+[1]_p, x^3+[7]_p) = -x+[7]_p \quad \text{et ainsi} \quad \text{pgdc}(\bar{f},\bar{g}) = (x-[2]_p)(-x+[7]_p).$$

Si $[50]_p \neq 0$, alors il s'agit d'une unité dans $\mathbb{F}_p[x]$, et donc la prochaine étape de l'algorithme donne un reste nul. Ainsi le pgdc de $x^2+[1]_p$ et de $x^3+[7]_p$ est une unité, autrement dit ces deux polynômes sont encore premiers entre eux.
Puisque $50 = 2\cdot 5^2$, on a $[50]_p = 0$ si et seulement si $p \in \{2,5\}$. Ainsi :

(a) Si $p \notin \{2,5\}$, alors $\text{pgdc}(\bar{f},\bar{g}) = x-[2]_p$.
(b) Si $p=2$, alors $\text{pgdc}(\bar{f},\bar{g}) = x(x+[1]_2)$.
(c) Si $p=5$, alors $\text{pgdc}(\bar{f},\bar{g}) = (x-[2]_5)(-x+[2]_5)$.

Exercice 4. 1. Montrons d'abord que $\mathbb{Q}[i\sqrt{d}]$ est un corps. Puisque $(i\sqrt{d})^2 \in \mathbb{Q}$, on voit que

$$\mathbb{Q}[i\sqrt{d}] = \{a+bi\sqrt{d} \mid a,b \in \mathbb{Q}\}.$$

Les inverses de ces éléments existent dans $\mathbb{C}$, où ils sont donnés par

$$(a+bi\sqrt{d})^{-1} = \frac{a-bi\sqrt{d}}{|a+bi\sqrt{d}|^2}, \quad \text{où } |a+bi\sqrt{d}|^2 = a^2+b^2d \in \mathbb{Q}.$$

Le côté droit appartient aussi à $\mathbb{Q}[i\sqrt{d}]$, on en déduit donc qu'il s'agit d'un corps.
On a l' inclusion évidente $\mathbb{Z}[i\sqrt{d}] \subset \mathbb{Q}[i\sqrt{d}]$. Pour chaque $a+bi\sqrt{d} \in \mathbb{Q}[i\sqrt{d}]$, on peut écrire

$$a+bi\sqrt{d} = \frac{a'}{n} + \frac{b'}{n} i\sqrt{d}$$

où n est le plus petit dénominateur commun de a et b, et $a', b' \in \mathbb{Z}$. Ainsi $\mathbb{Q}[i\sqrt{d}]$ est un corps de fractions pour $\mathbb{Z}[i\sqrt{d}]$.

2. Montrons que x^3-2i est irréductible dans $\mathbb{Z}[i][x]$. Puisque le coefficient dominant est une unité, ce polynôme est primitif. En vertu du lemme de Gauss (Proposition 3.8.13) et du premier point, il est irréductible dans $\mathbb{Z}[i][x]$ si et seulement si il est irréductible dans $\mathbb{Q}[i][x]$. Si x^3-2i se décompose dans $\mathbb{Q}[i][x]$, l'un des facteurs doit être un polynôme linéaire. Donc x^3-2i est irréductible dans $\mathbb{Q}[i][x]$ si et seulement si il n'a pas de racines dans $\mathbb{Q}[i]$.
Supposons que $2i$ possède une racine cubique dans $\mathbb{Q}[i]$. On peut écrire cette racine $\frac{a+bi}{n}$, avec $n \in \mathbb{N}$ et $a,b \in \mathbb{Z}$. On a alors

$$n^3 2i = (a+bi)^3$$

et en prenant les modules au carré, on obtient

$$4n^6 = (a^2+b^2)^3.$$

C'est une égalité entre deux entiers, on peut donc compter les puissances de 2 dans chaque membre et s'apercevoir qu'elles n'ont pas le même reste modulo 3. C'est une contradiction. Ainsi $2i$ n'a pas de racine cubique dans $\mathbb{Q}[i]$.
On a donc montré que x^3-2i est irréductible dans $\mathbb{Z}[i\sqrt{d}][x]$.
Remarque : Le critère d'Eisenstein ne peut être invoqué pour résoudre l'exercice. En effet la décomposition en facteurs irréductibles de $2i$ est

$$2i = (1+i)^2,$$

où $1+i$ est irréductible en vertu de la Proposition 3.4.8

Exercice 5. 1. Notons $A = k[t^2, t^3]$. Puisque $A \subset k[t]$, on a

$$A^\times \subseteq (k[t])^\times = k^\times$$

et l'inclusion inverse étant claire, on obtient $A^\times = k^\times$. On prétend ensuite que t^2 et t^3 sont irréductibles dans A :

(a) Si on peut écrire $t^2 = fg$ dans A, alors cette décomposition est aussi valable dans $k[t]$. Donc soit f ou g est une unité dans $k[t]$ et donc dans A, soit $\deg f = 1 = \deg g$. Or A ne contient aucun polynôme linéaire en t (observez que $A = k + t^2 \cdot k[t] + t^3 \cdot k[t]$, et que les éléments de $t^2 \cdot k[t]$ et de $t^3 \cdot k[t]$ n'ont pas de termes d'ordre 1). On voit donc que t^2 est irréductible dans A.

(b) Pour t^3, on procède de la même manière : les seules décompositions non-triviales dans $k[t]$ sont données par $t^3 = t \cdot t \cdot t = t \cdot t^2$, mais $t \notin A$.

On peut ainsi affirmer que

$$(t^2)^3 = (t^3)^2 \quad \text{dans } A,$$

et que t^2 et t^3 sont des éléments irréductibles non associés de A, puisqu'il n'existe pas de constante $\lambda \in k^\times$ telle que $\lambda t^2 = t^3$. Cela montre que A n'est pas factoriel.

2. On montre de la même manière que $k[t^2, t^5]$ et $k[t^3, t^7]$ ne sont pas factoriels.

3. On prétend que $k[x, y]/(x^2 - y^3)$ est isomorphe à $k[t^2, t^3]$. En effet, considérons l'homomorphisme d'évaluation k-linéaire

$$\varphi \colon k[x, y] \to k[t^2, t^3], \quad x \mapsto t^3,\ y \mapsto t^2.$$

Alors φ est surjective et $k[x, y]/\ker\varphi \cong k[t^2, t^3]$. On prétend que $\ker\varphi = (x^2 - y^3)$. L'inclusion $\supseteq$ est claire. Pour montrer l'inclusion inverse, prenons $f \in \ker\varphi$ et faisons l'observation suivante : il existe un polynôme $g \in k[x, y]$ tel que $\deg_x[f - (x^2 - y^3) \cdot g] < 2$. En effet, puisque $f - (x^2 - y^3) \cdot g \in \ker\varphi$, cela se montre aisément par induction sur $\deg_x$ pour les éléments de $\ker\varphi$. Si nous montrons que $f - (x^2 - y^3) \cdot g \in (x^2 - y^3)$, nous aurons établi l'inclusion désirée. Nous pouvons donc supposer que $\deg_x f < 2$, et nous allons en fait montrer que $f = 0$.
Si $\deg_x f = 0$, alors $f = \sum_i a_i y^i$ et $\varphi(f) = \sum_i a_i t^{2i}$. Il est alors clair que $\varphi(f) = 0$ si et seulement si $f = 0$.
Si $\deg_x f = 1$, alors on peut écrire

$$f = \sum_i a_i y^i + \sum_j b_j x y^j$$

et ainsi

$$\varphi(f) = \sum_i a_i t^{2i} + \sum_j b_j t^{3+2j}.$$

Les puissances de t dans la première somme sont paires, celles dans la seconde sont impaires : il n'y a donc pas de simplifications possibles entre ces deux sommes, et on en déduit que $\varphi(f) = 0$ si et seulement si $f = 0$.
On a donc montré que $k[x, y]/(x^2 - y^3) \cong k[t^2, t^3]$. Il reste à remarquer que la propriété d'être factoriel est préservée par isomorphisme. Puisque $k[t^2, t^3]$ n'est pas factoriel, on en déduit que $k[x, y]/(x^2 - y^3)$ n'est pas non plus factoriel.

Exercice 6. 1. Rappelons que

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix}$$

de quoi il s'ensuit immédiatement que la fonction

$$A \to \mathbb{Z} \times \mathbb{Q}, \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

est un homomorphisme surjectif dont le noyau est I.

Montrons maintenant que l'anneau commutatif $\mathbb{Z}\times\mathbb{Q}$ est Noethérien. Soit $I \subset \mathbb{Z}\times\mathbb{Q}$ un idéal. Il est facile de vérifier que l'intersection $I' := I\cap(\{0\}\times\mathbb{Q})$ est un idéal de $\mathbb{Q}$ via l'identification évidente $\mathbb{Q} = \{0\} \times \mathbb{Q}$. Puisque $\mathbb{Q}$ est un corps, on a $I' = \{(0,0)\}$ ou $I' = \{0\} \times \mathbb{Q}$.

(a) Supposons que $I' = \{(0,0)\}$. Alors tous les éléments de I sont de la forme $(x, 0)$. En effet, si $(x, y) \in I$, alors $(0, 1) \cdot (x, y) \in I$ et donc $(0, y) \in I'$, d'où $y = 0$.
Dans ce cas, I s'identifie à un idéal de $\mathbb{Z}$ via l'identification évidente $\mathbb{Z} = \mathbb{Z} \times \{0\}$. L'anneau $\mathbb{Z}$ est principal puisqu'il est Euclidien (Proposition 3.3.3), donc on en déduit que I est généré par un élément de la forme $(n, 0)$.

(b) Supposons que $I' = \{0\} \times \mathbb{Q}$. Alors on prétend que $I = I'' \times \mathbb{Q}$ pour un idéal I'' de $\mathbb{Z}$. En effet, soit $(x, y) \in I$. Puisque $(0, z) \in I'$ pour tout $z \in \mathbb{Q}$, on voit que $(x, y) + (0, z) = (x, y + z) \in I$ pour tout $z \in \mathbb{Q}$. Puisque la translation par y dans $\mathbb{Q}$ est bijective, on en déduit que $(x, z) \in I$ pour tout $z \in \mathbb{Q}$. Cela prouve qu'on peut écrire $I = I'' \times \mathbb{Q}$ pour un certain sous-ensemble $I'' \subset \mathbb{Z}$. Puisque I est un idéal, on vérifie aisément que I'' doit être un idéal de $\mathbb{Z}$. Si $I'' = (n)$, alors I est généré par $(n, 1)$.

On a montré que tous les idéaux de $\mathbb{Z} \times \mathbb{Q}$ étaient finiment générés (en fait, ils sont tous principaux), ce qui montre que cet anneau produit est Noethérien (et même principal).

2. Soit J un idéal à droite qui contient un élément de la forme

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \quad 0 \neq b \in \mathbb{Q}.$$

Le calcul au début du point précédent montre alors que J contient tous les éléments de la forme

$$\begin{pmatrix} 0 & bz \\ 0 & 0 \end{pmatrix}, \quad z \in \mathbb{Q}$$

et il s'ensuit que $J \supseteq I$. Cela montre que I est minimal comme idéal à droite.
Notons que I n'est pas minimal comme idéal à gauche, puisqu'il contient strictement le sous-idéal à gauche

$$\left\{ \begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix} \mid n \in \mathbb{Z} \right\}.$$

3. Montrons finalement que A est Noethérien à droite. Soit

$$J_1 \subseteq J_2 \subseteq \dots$$

une suite croissante d'idéaux à droite. Alors chaque $J_k \cap I$ est un sous-idéal à droite de I. Par le point précédent, pour chaque k on a soit $J_k \cap I = I$, soit $J_k \cap I = 0$. Puisque la suite est croissante, ces intersections sont toujours les mêmes pour k assez grand. Quitte à oublier les premiers idéaux, on peut donc supposer que $J_k \cap I = 0$ pour *tous* les k, ou que $J_k \cap I = I$ pour *tous* les k.
Considérons l'application quotient $\pi\colon A \to A/I$. Puisque π est surjective, les ensembles images $\pi(J_k)$ sont tous des idéaux (à droite) de A/I (la vérification est aisée), et on obtient une suite croissante d'idéaux

$$\pi(J_1) \subseteq \pi(J_2) \subseteq \dots$$

dans A/I. Nous avons montré dans le premier point que A/I est Noethérien : donc $\pi(J_k) = \pi(J_{k+1})$ pour tous les k assez grands.
On prétend que $\pi(J_k) = \pi(J_{k+1})$ entraîne $J_k = J_{k+1}$. Si ce n'est pas le cas, on peut trouver $x \in J_{k+1} \setminus J_k$. Puisque $\pi(x) \in \pi(J_{k+1}) = \pi(J_k)$, il existe $x' \in J_k$ tel que $x - x' \in \ker \pi = I$.

(a) Si $J_{k+1} \cap I = 0$, puisque $x - x' \in J_{k+1} \cap I$ on obtient $x = x' \in J_k$, contradiction.

(b) Si $J_{k+1} \cap I = I$, alors par notre simplification initiale on a aussi $J_k \cap I = I$ et donc $I \subseteq J_k$. Alors $x - x' \in J_k$ et ainsi $x = x' + (x - x') \in J_k$, contradiction.

Ainsi $J_k = J_{k+1}$ pour tous les k assez grands, ce qui montre que la chaîne d'idéaux se stabilise. Ainsi A est Noethérien à droite.

Exercice 7. 1. On a $x^2+y^2 = (x+iy)(x-iy)$ dans $\mathbb{C}[x,y]$, donc le polynôme n'est pas irréductible dans $\mathbb{C}[x,y]$.

Montrons qu'il est irréductible dans $\mathbb{Q}[x,y]$. Posons $A := \mathbb{Q}[x]$, c'est un anneau factoriel en vertu des Corollaires 3.3.5 et 3.7.2. On a $\mathbb{Q}[x,y] = A[y]$, et $x^2+y^2 \in A[y]$ est primitif puisque son coefficient dominant est une unité. Donc par la Proposition 3.8.13, x^2+y^2 est irréductible dans $A[y]$ si et seulement si il est irréductible dans $\mathrm{Frac}(A)[y]$.

On a

$$\mathrm{Frac}(A) = \mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0 \right\}.$$

Puisque $\deg_y(y^2+x^2) = 2$ et que les polynômes constants non-nuls de $\mathrm{Frac}(A)[y]$ sont des unités, le polynôme $y^2+x^2 \in A[y]$ se scinde dans $\mathrm{Frac}(A)[y]$ si et seulement si y^2+x^2 (vu comme un polynôme en y) admet une racine dans $\mathrm{Frac}(A) = \mathbb{Q}(x)$, autrement dit si et seulement si il existe $f(x), g(x) \in \mathbb{Q}[x]$ tels que

$$\left(\frac{f(x)}{g(x)}\right)^2 = -x^2.$$

Cela impliquerait que

$$f(x)^2 = -x^2 g(x)^2 \quad \text{dans } \mathbb{Q}[x].$$

Regardons le coefficient dominant de chaque côté : celui de $f(x)^2$ est positif (il s'agit du carré du coefficient dominant de $f(x)$), celui de $-x^2g(x)^2$ est négatif (il s'agit de l'opposé du carré du coefficient dominant de $g(x)$), c'est une contradiction.

Donc $y^2+x^2 \in \mathrm{Frac}(A)[y]$ est irréductible, et ainsi $y^2+x^2 \in \mathbb{Q}[x,y]$ est irréductible.

2. Montrons que $x^3-(y^7+2y^5+y^3)$ est irréductible dans $\mathbb{Q}[x,y]$. Comme dans le point précédent (en échangeant les rôles de x et y), il suffit de montrer qu'il n'existe pas de polynômes $f(y), g(y) \in \mathbb{Q}[y]$ tels que

$$\left(\frac{f(y)}{g(y)}\right)^3 = y^7+2y^5+y^3 \quad \text{dans } \mathbb{Q}(y).$$

Cela impliquerait que

$$f(y)^3 = (y^7+2y^5+y^3)g(y)^3 \quad \text{dans } \mathbb{Q}[y].$$

Regardons le degré de chaque côté : celui de gauche est un multiple de 3, tandis que celui de droite vaut 1 modulo 3. C'est une contradiction, et on en déduit que $x^3-(y^7+2y^5+y^3)$ est irréductible dans $\mathbb{Q}[x,y]$.

Remarque : le critère d'Eisenstein ne peut être appliqué dans aucun des deux cas (remarquons que le décomposition de $y^7+2y^5+y^3$ en facteurs premiers est $(y^2+1)^2y^3$).