Université de Bordeaux
Mathématiques

L2, Algèbre linéaire 2
Année 2024–2025

FEUILLES D'EXERICES N°2

Anneaux

1. Exercices

Exercice 1. (Solution)
On pose $\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\} \subset \mathbb{C}$.

(1) Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
(2) Déterminer le groupe $\mathbb{Z}[i]^\times$ des inversibles de $\mathbb{Z}[i]$ (indication : on pourra utiliser la fonction $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(z) = |z|^2$).

Exercice 2. (Solution)
Soit A un anneau commutatif. Montrer que les trois assertions suivantes sont équivalentes :

(1) A est un corps ;
(2) $A \neq \{0\}$ et les seuls idéaux de A sont $\{0\}$ et A ;
(3) $A \neq \{0\}$ et tout morphisme de A dans un anneau non nul est injectif.

Exercice 3. (Solution)
Soient m, n deux entiers strictement positifs. Montrer qu'il existe un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si m divise n et que dans ce cas, ce morphisme est unique.

Exercice 4. (Solution)
On munit $\mathbb{Z}$ et $\mathbb{R}$ de leurs structures usuelles d'anneaux.

(1) Déterminer les morphismes d'anneaux de $(\mathbb{Z}, +, \times)$ dans lui même.
(2) Soit f un morphisme d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même.
   (a) Montrer que pour tout $x \in \mathbb{Q}$, $f(x) = x$.
   (b) Montrer que pour tout $x \in \mathbb{R}^+$, $f(x) \geq 0$ et en déduire que f est croissante.
   (c) Déterminer f.

Exercice 5. (Solution)
On pose pour $n \in \mathbb{Z}$, $n \geq 2$, $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid (a, b) \in \mathbb{Z}^2\}$.

(1) Montrer que $\mathbb{Z}[\sqrt{n}]$ est un sous-anneau de $\mathbb{R}$ (muni des lois usuelles).
(2) Quels sont les morphismes d'anneaux de $\mathbb{Z}[\sqrt{2}]$ dans lui-même ?
(3) Existe-t-il un morphisme d'anneaux de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{3}]$?

Polynôme

Lorsqu'aucune précision n'est donnée, les polynômes considérés appartiennent à $K[X]$ où K est un corps et les calculs se font dans $K[X]$.

Exercice 6. (Solution)
Montrer que pour tout $n \in \mathbb{N}$, on a :

$$(X^3+X^2+X+1)\sum_{k=0}^{2n}(-1)^k X^k = X^{2n+3}+X^{2n+1}+X^2+1$$

Exercice 7. (Solution)
Effectuer dans $\mathbb{C}[X]$ les divisions euclidiennes suivantes :

(1) $3X^5+2X^4-X^2+1$ par X^3+X+2 ;
(2) $X^5-7X^4-X^2-9X+9$ par X^2-5X+4 ;
(3) $4X^3+X^2$ par $X+1+i$.

Exercice 8. (Solution)
Factoriser :

(1) X^4+1 dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.
(2) X^3-3 dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.
(3) $X^2+(3i-1)X-2-i$ dans $\mathbb{C}[X]$.

Exercice 9. (Solution)
Soient $P(X) \in \mathbb{C}[X]$ et a, b deux nombres complexes distincts. Exprimer (en fonction de $a, b, P(a), P(b), P'(a)$) les restes des divisions euclidiennes dans $\mathbb{C}[X]$ de $P(X)$ par les polynômes suivants :

(1) $X-a$;
(2) $(X-a)^2$;
(3) $(X-a)(X-b)$.

Exercice 10. (Solution)
Montrer que pour tout $n \in \mathbb{N}$, le polynôme

$$P = nX^{n+2}-(n+2)X^{n+1}+(n+2)X-n$$

est divisible par $(X-1)^3$ dans $\mathbb{Q}[X]$.

Exercice 11. (Solution)
On considère le polynôme $X^5-11X^3+11X^2+8X-4$ de $\mathbb{R}[X]$. Trouver l'ordre de multiplicité de sa racine 2.

Exercice 12. (Solution)
Factoriser dans $\mathbb{R}[X]$ le polynôme $P = 16X^5-20X^3+5X-1$ sachant qu'il admet au moins deux racines multiples dans $\mathbb{C}$.

Exercice 13. (Solution)
Soient λ et μ deux nombres complexes. Déterminer une condition nécessaire et suffisante sur λ et μ pour que le polynôme $P = X^4+X^3+\lambda X^2+\mu X+2$ soit divisible par X^2+2 dans $\mathbb{C}[X]$.

Exercice 14. (Solution)
Déterminer une relation de Bézout entre les polynômes de $\mathbb{Q}[X]$:

(1) X^3-1 et X^3+1 ;
(2) $(X-1)^3$ et $(X+1)^3$;
(3) X^3+X^2+1 et X^3+X+1.

Exercice 15. (Solution)
Déterminer le pgcd des deux polynômes $X^5+5X^4+9X^3+7X^2+5X+3$ et $X^4+2X^3+2X^2+X+1$ en tant qu'éléments de $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Exercice 16. (Solution)
Déterminer tous les polynômes P de $\mathbb{C}[X]$ tels que P' divise P dans $\mathbb{C}[X]$.

Exercice 17. (Solution)
Soient $n \geq m$ deux entiers naturels non nuls.

(1) En considérant la division de n par m, déterminer le reste de la division euclidienne de X^n-1 par X^m-1.
(2) En déduire que le pgcd X^n-1 et X^m-1 est $X^{\mathrm{pgcd}(n,m)-1}$.

Exercice 18. (Solution)
Soit un entier $n>1$ et soit $P(X) \in \mathbb{C}[X]$ un polynôme de degré $< n$. On suppose qu'il existe $r \in \mathbb{R}$ tel que pour tout entier $k \in [\![1;n]\!]$ on ait $P(k)=r^k$. Pour tout entier $k \in [\![1;n]\!]$, on pose :

$$L_k(X) = \prod_{i=1, i\neq k}^{n} \frac{X-i}{k-i}$$

(1) Déterminer pour deux entiers $(k,l) \in [\![1;n]\!]^2$, $L_k(l)$.
(2) Montrer que $P(X) = \sum_{k=1}^{n} r^k L_k(X)$.
(3) Calculer $P(n+1)$.

Exercice 19. (Solution)
Donner une condition nécessaire et suffisante sur l'entier $n>0$ pour que X^2+X+1 divise $(X+1)^n-X^n-1$ dans $\mathbb{Q}[X]$.

Exercice 20. (Solution)
Soit $P \in \mathbb{Z}[X]$ de degré ≥ 1 et $n \in \mathbb{Z}$, on pose $m=P(n)$.

(1) Montrer que pour tout $k \in \mathbb{Z}$, m divise $P(n+km)$ dans $\mathbb{Z}$.
(2) En déduire que $P(l)$ ne peut pas être un nombre premier pour tout $l \in \mathbb{N}$.

2. Solutions

Solution 1. (Enoncé)
1. Il faut montrer que : $1 \in \mathbb{Z}[i]$, et que pour tout $(x, y) \in \mathbb{Z}[i]^2$, $x - y \in \mathbb{Z}[i]$ et $xy \in \mathbb{Z}[i]$.
$1 \in \mathbb{Z}[i]$ car $1 = 1 + 0 \times i$. Soit maintenant $x = a + ib \in \mathbb{Z}[i]$ et $y = a' + ib' \in \mathbb{Z}[i]$, alors :

$$x - y = \underbrace{(a - a')}_{\in \mathbb{Z}} + i \underbrace{(b - b')}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$$

et,

$$xy = \underbrace{(aa' - bb')}_{\in \mathbb{Z}} + i \underbrace{(ab' + a'b)}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$$

et cela conclut.
2. On rappelle que par définition :

$$\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i] \mid \exists z' \in \mathbb{Z}[i],\ zz' = 1\}$$

Montrons que $\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$:
Inclusion directe : Si $z = a + ib \in \mathbb{Z}[i]^\times$ alors il existe $z' \in \mathbb{Z}[i]^\times$ tel que $zz' = 1$ donc $N(zz') = N(1) = 1$. Or par propriété du module il vient

$$1 = N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z').$$

Et de plus, $N(z) = a^2 + b^2 \in \mathbb{N}$ et de même pour $N(z')$. on a donc écrit 1 comme un produit de deux entiers naturels, ces entiers sont donc forcément 1 et $N(z) = 1$.
Inclusion réciproque : Soit $z = a + ib \in \mathbb{Z}[i]$ tel que $N(z) = 1$, alors il suffit de remarquer que :

$$z\overline{z} = |z|^2 = N(z) = 1$$

et $\overline{z} = a - ib \in \mathbb{Z}[i]$ et donc $z \in \mathbb{Z}[i]^\times$ et cela conclut.
Déterminer les inversibles de $\mathbb{Z}[i]$ revient donc à déterminer les éléments $z = a + ib \in \mathbb{Z}[i]$ vérifiant $N(z) = 1$ *i.e.* $a^2 + b^2 = 1$. De l'inégalité

$$0 \leq a^2 \leq a^2 + b^2 \leq 1$$

on voir que a^2 est un entier compris entre 0 et 1, c'est donc 0 ou 1 donc $a \in \{-1, 0, 1\}$ et de même pour b. Enfin, si $a \neq 0$, alors $a^2 = 1$ et donc $b^2 = 0$ *i.e.* $b = 0$. Les couples solutions sont donc :

$$(1, 0),\ (-1, 0),\ (0, 1),\ (0, -1)$$

qui correspondent aux éléments $1, -1, i, -i$ d'où :

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\} = \mathbb{U}_4$$

Solution 2. (Enoncé)
1) $\implies$ 2) : Si A est un corps alors A n'est pas l'anneau nul. Soit $I \subset A$ un idéal. On suppose $I \neq \{0\}$ et on va montrer $I = A$. Soit $x \in I$ non nul, comme A est un corps, il existe $a \in A$ tel que $yx = 1$, mais alors :

$$1 = \underbrace{a}_{\in A}\ \underbrace{x}_{\in I} \in I,$$

car I idéal. Soit maintenant $b \in A$, alors :

$$b = \underbrace{b}_{\in A}\ \underbrace{1}_{\in I} \in I$$

donc $b \in I$ *i.e.* $A \subset I$ et finalement $I = A$ ce qui conclut.
2) $\implies$ 3) Soit $f : A \to B$ un morphisme d'anneaux où $B \neq \{0\}$. Alors par le

cours, l'ensemble $\ker(f) = \{x \in A \mid f(x) = 0_B\}$ est un idéal de A donc pas hypothèse, $\ker(f) = \{0\}$ ou $\ker(f) = A$. Comme f est un morphisme d'anneaux,

$$f(1_A) = 1_B \neq 0$$

car B n'est pas l'anneau nul. Donc $1 \notin \ker(f)$ et donc $\ker(f) \neq A$ et finalement $\ker(f) = \{0\}$. On peut en déduire que f injective car si $f(x) = f(y)$ avec $(x, y) \in A^2$, alors

$$f(x - y) = f(x) - f(y) = 0_B$$

car f morphisme d'anneaux, d'où $x - y \in \ker(f) = \{0\}$ et donc $x = y$: l'application f est bien injective.
3) $\implies$ 1) (Hors-programme) Soit $x \in A$ non nul, on considère le morphisme de $f : A \to A/(x)$ de réduction modulo l'idéal engendré par x. Si $(x) \neq A$, alors $A/(x) \neq 0$ et donc par hypothèse f est injective mais $f(x) = 0 = f(0)$ donc $x = 0$ ce qui est exclu. Donc $(x) = A$ et x est inversible : A est bien un corps.

Solution 3. (Enoncé)
Supposons qu'il existe un morphisme d'anneaux $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. On note pour $x \in \mathbb{Z}$, $\overline{x}^{(m)}$ sa classe dans $\mathbb{Z}/m\mathbb{Z}$ et $\overline{x}^{(n)}$ sa classe dans $\mathbb{Z}/n\mathbb{Z}$. Comme f est un morphisme d'anneaux :

$$\overline{0}^{(m)} = f(\overline{0}^{(n)}) = f(\overline{n}^{(n)}) = f(n \cdot \overline{1}^{(n)}) = n \cdot f(\overline{1}^{(n)}) = n \cdot \overline{1}^{(m)} = \overline{n}^{(m)},$$

où la première égalité vient des propriétés des morphismes d'anneaux et la quatrième égalité vient de :

$$f(n \cdot \overline{1}^{(n)}) = f(\underbrace{\overline{1}^{(n)} + \cdots + \overline{1}^{(n)}}_{n \text{ fois}}) = \underbrace{f(\overline{1}^{(n)}) + \cdots + f(\overline{1}^{(n)})}_{n \text{ fois}} = n \cdot \overline{1}^{(m)}.$$

Donc $\overline{n}^{(m)} = \overline{0}^{(m)}$ et donc nécessairement, m divise n. Dans ce cas, on a nécessairement :

$$f(\overline{k}^{(n)}) = \overline{k}^{(m)}.$$

En effet, car pour $k \in \mathbb{Z}$,

$$f(\overline{k}^{(n)}) = f(k \cdot \overline{1}^{(n)}) = k f(\overline{1}^{(n)}) = k\overline{1}^{(m)} = \overline{k}^{(m)}$$

et l'application $\overline{k}^{(n)} \mapsto \overline{k}^{(m)}$ est bien un morphisme d'anneaux

Solution 4. (Enoncé)
Soit $f : \mathbb{Z} \to \mathbb{Z}$ un morphisme d'anneaux, alors $f(1) = 1$. De plus, on peut écrire $2 = 1+1$ donc :

$$f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$$

On montre alors par récurrence que $f(n) = n$ pour tout $n \geq 0$. L'initialisation est vraie car un morphisme d'anneaux envoie 0 sur 0. Supposons l'assertation vrai au rang $n \geq 0$ *i.e.* $f(n) = n$, alors :

$$f(n + 1) = f(n) + f(1) = n + 1,$$

d'où l'hérédité et donc pour tout $n \geq 0$, $f(n) = n$. Soit maintenant n un entier négatif, $-n$ est un entier positif donc par ce qui précède, $f(-n) = -n$ d'où :

$$0 = f(n - n) = f(n) + f(-n) = f(n) + (-n) = f(n) - n$$

et donc $f(n) = n$. Finalement $f(n) = n$ pour tout $n \in \mathbb{Z}$ et donc $f = \mathrm{Id}_{\mathbb{Z}}$. Inversement l'application $\mathrm{Id}_{\mathbb{Z}}$ est bien un morphisme d'anneaux.

2. *a*) Par le même raisonnement que précédemment, $f(n) = n$ pour tout $n \in \mathbb{Z}$. Soit maintenant $r = \frac{p}{q} \in \mathbb{Q}$, alors en utilisant les propriétés des morphismes d'anneaux :

$$qf(r) = qf\left(\frac{p}{q}\right) = f(q)f\left(\frac{p}{q}\right) = f\left(q \times \frac{p}{q}\right) = f(p) = p$$

donc, $f(r) = r$ et cela conclut.
b) Soit $x \in \mathbb{R}^+$, alors on peut considérer l'élément $\sqrt{x} \in \mathbb{R}^+$ d'où :

$$f(x) = f(\sqrt{x}^2) = f(\sqrt{x})^2 \geq 0$$

Si l'on prend maintenant $y \geq x$ deux réels, alors $y - x \geq 0$ donc $f(y - x) \geq 0$ mais $f(y - x) = f(y) - f(x)$ et donc $f(y) \geq f(x)$ et f est bien croissante.
c) Montrons que $f = \mathrm{Id}_{\mathbb{R}}$. Soit $x \in \mathbb{R}$, alors il existe des suites (q_n) et (r_n) de rationnels qui convergent vers x tels que :

$$\forall n \geq 0, \quad q_n \leq x \leq r_n.$$

On peut par exemple tronquer le développement décimal de x à la n-ème décimale par défaut pour q_n et par excès pour r_n. La croissance de f assure que :

$$\forall n \geq 0, \quad f(q_n) \leq f(x) \leq f(r_n).$$

Or $f(q_n) = q_n$ et $f(r_n) = r_n$ car q_n et r_n sont rationnels. Donc en faisant tendre n vers $+\infty$ il vient par encadrement $f(x) = x$ et donc $f = \mathrm{Id}_{\mathbb{R}}$. Inversement, l'application $\mathrm{Id}_{\mathbb{R}}$ est bien un morphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{R}$.

Solution 5. (Enoncé)
1. Il faut montrer que : $1 \in \mathbb{Z}[\sqrt{n}]$, et que pour tout $(x, y) \in \mathbb{Z}[\sqrt{n}]^2$, $x - y \in \mathbb{Z}[\sqrt{n}]$ et $xy \in \mathbb{Z}[\sqrt{n}]$.
$1 \in \mathbb{Z}[\sqrt{n}]$ car $1 = 1 + 0 \times i$. Soit maintenant $x = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ et $y = a' + b'\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, alors :

$$x - y = \underbrace{(a - a')}_{\in\mathbb{Z}} + \underbrace{(b - b')}_{\in\mathbb{Z}}\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$$

et,

$$xy = \underbrace{(aa' + nbb')}_{\in\mathbb{Z}} + \underbrace{(ab' + a'b)}_{\in\mathbb{Z}}\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$$

et cela conclut.
2. Soit $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ un morphisme d'anneaux. En refaisant le même raisonnement que l'exercice précédent, on montre que $f(n) = n$ pour tout $n \in \mathbb{Z}$. Soit alors $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,

$$f(a + b\sqrt{2}) = f(a) + f(b\sqrt{2}) = f(a) + f(b)f(\sqrt{2}) = a + bf(\sqrt{2}).$$

Il s'agit donc de déterminer $f(\sqrt{2})$. On a :

$$f(\sqrt{2})^2 = f(\sqrt{2}^2) = f(2) = 2$$

donc $f(\sqrt{2}) = \sqrt{2}$ ou $f(\sqrt{2}) = -\sqrt{2}$. Dans le premier cas f est l'identité, dans le second f est l'application $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Inversement, ces deux applications sont bien des morphismes d'anneaux.
3. On pourrait penser que l'application $f : a + b\sqrt{2} \mapsto a + b\sqrt{3}$ est un morphisme d'anneaux de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{3}]$ mais ce n'est pas le cas car :

$$f(\sqrt{2})^2 = \sqrt{3}^2 = 3 \neq 2 = f(\sqrt{2}^2)$$

On va montrer qu'il n'y a pas de morphisme d'anneaux de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{3}]$. On suppose par l'absurde qu'il existe un tel morphisme f, alors :

$$2 = f(2) = f(\sqrt{2}^2) = f(\sqrt{2})^2$$

donc $f(\sqrt{2}) = \pm\sqrt{2}$ doit s'écrire $a + b\sqrt{3}$ avec $(a, b) \in \mathbb{Z}^2$. Si par exemple, $\sqrt{2} = a + b\sqrt{3}$ alors en élevant au carré :

$$2 = a^2 + 2ab\sqrt{3} + 3b^2$$

Donc comme $\sqrt{3}$ est irrationnel, $ab = 0$. Si $a = 0$ alors $2 = 3b^2$ avec $b \in \mathbb{Z}$ ce qui est absurde car 3 ne divise pas 2. Si $b = 0$ alors $\sqrt{2} = a \in \mathbb{Z}$ ce qui est aussi absurde. Un tel morphisme f n'existe donc pas.

Solution 6. (Enoncé)
On remarque que :

$$X^3 + X^2 + X + 1 = (X^2 + 1)(X + 1),$$

et :

$$(X + 1)\sum_{k=0}^{2n}(-1)^k X^k = X^{2n+1} + 1.$$

Donc,

$$\begin{aligned}(X^3 + X^2 + X + 1)\sum_{k=0}^{2n}(-1)^k X^k &= (X^2 + 1)(X + 1)\sum_{k=0}^{2n}(-1)^k X^k \\ &= (X^2 + 1)(X^{2n+1} + 1) \\ &= X^{2n+3} + X^{2n+1} + X^2 + 1.\end{aligned}$$

Solution 7. (Enoncé)

1. $$\begin{array}{rrrrr|l} 3X^5 + 2X^4 & & - X^2 & & + 1 & X^3 + X + 2 \\ \cline{6-6} - 3X^5 & & - 3X^3 - 6X^2 & & & 3X^2 + 2X - 3 \\ \cline{1-3} & & 2X^4 - 3X^3 - 7X^2 & & & \\ & - 2X^4 & & - 2X^2 - 4X & & \\ \cline{2-4} & & - 3X^3 - 9X^2 - 4X & & + 1 & \\ & & 3X^3 & & + 3X + 6 & \\ \cline{3-5} & & & - 9X^2 & - X + 7 & \end{array}.$$

2. $$\begin{array}{rrrrrr|l} X^5 - 7X^4 & & & - X^2 & - 9X & + 9 & X^2 - 5X + 4 \\ \cline{7-7} - X^5 + 5X^4 & - 4X^3 & & & & & X^3 - 2X^2 - 14X - 63 \\ \cline{1-2} & - 2X^4 & - 4X^3 & - X^2 & & & \\ & 2X^4 & - 10X^3 & + 8X^2 & & & \\ \cline{2-4} & & - 14X^3 & + 7X^2 & - 9X & & \\ & & 14X^3 & - 70X^2 & + 56X & & \\ \cline{3-5} & & & - 63X^2 & + 47X & + 9 & \\ & & & 63X^2 & - 315X & + 252 & \\ \cline{4-6} & & & & - 268X & + 261 & \end{array}.$$

Solution 8. (Enoncé)
1. On cherche les racines de X^4+1 dans $\mathbb{C}[X]$, ce sont les racines 4-ème de -1 *i.e.* $e^{\frac{i\pi}{4}}$, $e^{-\frac{i\pi}{4}}$, $e^{\frac{3i\pi}{4}}$ et $e^{-\frac{3i\pi}{4}}$. La factorisation de X^4+1 dans $\mathbb{C}[X]$ est alors :

$$X^4+1=(X-e^{\frac{i\pi}{4}})(X-e^{-\frac{i\pi}{4}})(X-e^{\frac{3i\pi}{4}})(X-e^{-\frac{3i\pi}{4}}).$$

En regroupant les racines qui sont complexes conjuguées, on en déduit la factorisation de X^4+1 dans $\mathbb{R}[X]$:

$$\begin{aligned}X^4+1&=\left[(X-e^{\frac{i\pi}{4}})(X-e^{-\frac{i\pi}{4}})\right]\left[(X-e^{\frac{3i\pi}{4}})(X-e^{-\frac{3i\pi}{4}})\right]\\&=\left(X^2-\left(e^{\frac{i\pi}{4}}+e^{-\frac{i\pi}{4}}\right)X+e^{\frac{i\pi}{4}}e^{-\frac{-i\pi}{4}}\right)\left(X^2-\left(e^{\frac{3i\pi}{4}}+e^{\frac{-3i\pi}{4}}\right)X+e^{\frac{3i\pi}{4}}e^{-\frac{-3i\pi}{4}}\right)\\&=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).\end{aligned}$$

2. La encore, on peut chercher les racines de X^3-3 dans $\mathbb{C}$. Ce sont $\sqrt[3]{3}$, $j\sqrt[3]{3}$ et $\overline{j}\sqrt[3]{3}$ où $j=e^{\frac{2i\pi}{3}}$. On en déduit la factorisation de P dans $\mathbb{C}$:

$$X^3-3=(X-\sqrt[3]{3})(X-j\sqrt[3]{3})(X-\overline{j}\sqrt[3]{3})$$

En regroupant les racines qui sont complexes conjuguées, on en déduit la factorisation de X^3-3 dans $\mathbb{R}[X]$:

$$\begin{aligned}X^3-3&=(X-\sqrt[3]{3})\left[(X-j\sqrt[3]{3})(X-\overline{j}\sqrt[3]{3})\right]\\&=(X-\sqrt[3]{3})(X^2-(j+\overline{j})\sqrt[3]{3}X+j\sqrt[3]{3}\overline{j}\sqrt[3]{3})\\&=(X-\sqrt[3]{3})(X^2+\sqrt[3]{3}X+2^{\frac{2}{3}})\end{aligned}$$

Remarque : Pour la factorisation dans $\mathbb{R}$, on pouvait aussi utiliser la formule $a^n-b^n=(a-b)\sum_{k=0}^{n}a^kb^{n-1-k}$ et vérifier que le polynôme de degré 2 obtenu était sans racines dans $\mathbb{R}$.
3. On cherche les racines de $X^2+(3i-1)X-2-i$ dans $\mathbb{C}$, le discriminant vaut

$$\Delta=(3i-1)^2+4(2+i)=-2i=2e^{-\frac{i\pi}{2}}$$

Donc une racine de Δ est $\delta:=\sqrt{2}e^{-\frac{i\pi}{4}}=1-i$. Donc les racines recherchées sont :

$$\frac{-(3i-1)+1-i}{2}=1-2i \text{ et } \frac{-(3i-1)-(1-i)}{2}=-i$$

donc la factorisation de $X^2+(3i-1)X-2-i$ dans $\mathbb{C}[X]$ vaut :

$$X^2+(3i-1)X-2-i=(X-(1-2i))(X-(-i))=(X-1+2i)(X+i)$$

Solution 9. (Enoncé)
1. Par le théorème de division euclidienne, il existe $(Q,R)\in\mathbb{C}[X]^2$ avec $\deg(R)<\deg(X-a)=1$ tel que :

$$P(X)=Q(X)(X-a)+R(X).$$

Or $\deg(R)<1$ donc $R=\lambda$ est constant et en évaluant la relation précédente en a il vient :

$$P(a)=Q(a)(a-a)+R(a)=\lambda,$$

d'où $R=P(a)$.
2. Par le théorème de division euclidienne, il existe $(Q,R)\in\mathbb{C}[X]^2$ avec $\deg(R)<\deg((X-a)^2)=2$ tel que :

$$P(X)=Q(X)(X-a)^2+R(X).$$

Or $\deg(R) < 2$ donc on peut écrire $R = cX + d$ avec $(c, d) \in \mathbb{C}^2$ à déterminer. En évaluant la relation précédente en a il vient :

$$P(a) = Q(a)(a-a)^2 + R(a) = R(a) = ca + d.$$

De même, en dérivant la relation puis en évaluant en a il vient :

$$P'(a) = Q'(a)(a-a)^2 + 2Q(a)(a-a) + R'(a) = c$$

d'où $c = P'(a)$ et la première équation donne $d = P(a) - ac = P(a) - aP'(a)$.
3. Par le théorème de division euclidienne, il existe $(Q, R) \in \mathbb{C}[X]^2$ avec $\deg(R) < \deg((X-a)(X-b)) = 2$ tel que :

$$P(X) = Q(X)(X-a)(X-b) + R(X).$$

Or $\deg(R) < 2$ donc on peut écrire $R = cX + d$ avec $(c, d) \in \mathbb{C}^2$ à déterminer. En évaluant la relation précédente en a il vient :

$$P(a) = Q(a)(a-a)(a-b) + R(a) = R(a) = ca + d.$$

En évaluant la relation précédente en b il vient :

$$P(b) = Q(b)(b-a)(b-b) + R(b) = R(b) = cb + d.$$

Donc les inconnues c et d vérifient le système suivant :

$$\begin{cases} ca + d &= P(a) \quad (1) \\ cb + d &= P(b) \quad (2) \end{cases}$$

En faisant $(1) - (2)$ il vient,

$$c = \frac{P(a) - P(b)}{a - b},$$

car $a - b \neq 0$. Enfin, la première équation donne :

$$d = P(a) - a\frac{P(a) - P(b)}{a - b}.$$

Solution 10. (Enoncé)
On utilise la caractérisation par l'annulation des dérivées. Plus précisément, par le cours il suffit de vérifier que $P(1) = P'(1) = P''(1) = 0$. Or,

$$P(1) = n - (n+2) + (n+2) - n = 0,$$

$$P'(1) = n(n+2) - (n+2)(n+1) + (n+2) = 0$$

et

$$P''(1) = n(n+2)(n+1) - (n+2)(n+1)n = 0$$

et cela conclut.
Remarque : On peut vérifier que $P^{(3)}(1) \neq 0$ donc 1 est racine de P de multiplicité exactement 3.

Solution 11. (Enoncé)
La multiplicité de 2 en tant que racine est exactement l'entier $m \geq 1$ tel que $P(2) = \cdots = P^{(m-1)}(2) = 0$ et $P^{(m)}(2) = 0$. On calcule alors,

$$P(2) = 32 - 88 + 44 + 16 - 4 = 0,$$

$$P'(2) = 80 - 132 + 44 + 8 = 0$$

et,

$$P''(2) = 80 - 132 + 22 \neq 0$$

donc 2 est racine d'ordre 2 de P.

Solution 12. (Enoncé)
On remarque d'abord que $P(1) = 0$, donc P peut s'écrire $P = (X-1)Q$ avec $Q \in \mathbb{R}[X]$. On sait que P admet deux racines z_1, z_2 de multiplicités au moins 2, or 1 n'est pas une racine multiple de P donc $z_1 \neq 1$ et $z_2 \neq 1$. Comme $\deg(P) = 5$, z_1 et z_2 sont tous les deux de multiplicités 2 et 1 est de multiplicité 1.
On propose maintenant deux méthodes :
Première méthode : On peut écrire $Q = (X-z_1)^2(X-z_2)^2 = R^2$ avec $R \in \mathbb{R}[X]$ de degré 2 car Q est de degré 4. En faisant la division euclidienne de P par $X-1$:

$$\begin{array}{rrrrrr|l}
16X^5 & & -20X^3 & & +5X-1 & X-1 \\
\cline{6-6}
-16X^5+16X^4 & & & & & 16X^4+16X^3-4X^2-4X+1 \\
\cline{1-1}
16X^4-20X^3 & & & & & \\
-16X^4+16X^3 & & & & & \\
\cline{1-2}
-4X^3 & & & & & \\
4X^3-4X^2 & & & & & \\
\cline{2-3}
-4X^2+5X & & & & & \\
4X^2-4X & & & & & \\
\cline{3-4}
X-1 & & & & & \\
-X+1 & & & & & \\
\cline{5-6}
0 & & & & &
\end{array}$$

il vient $Q = 16X^4+16X^3-4X^2-4X+1$. En écrivant $R = aX^2+bX+c$ avec $(a,b,c) \in \mathbb{R}^3$ et en identifiant les coefficients dans la relation $R^2 = Q$ il vient le système suivant :

$$\begin{cases} a^2 & = 16 \\ 2ab & = 16 \\ 2ac+b^2 & = -4 \\ 2bc & = -4 \\ c^2 & = 1 \end{cases}$$

La première équation donne $a = \pm 4$. Si $a = 4$, alors la seconde équation donne $b = 2$ et enfin la troisième donne $c = -1$. Si $a = -4$, alors le même raisonnement donne $b = -2$ et $c = 1$. On a deux choix possibles mais c'est normal car on veut $R^2 = Q$ donc si R convient alors $-R$ aussi. On en déduit alors $R = 4X^2+2X-1$ et donc :

$$P = (X-1)(4X^2+2X-1)^2$$

en résolvant l'équation $4x^2+2x-1 = 0$ on peut alors écrire :

$$P = 16(X-1)\left(X-\frac{-1-\sqrt{5}}{4}\right)^2\left(X-\frac{-1+\sqrt{5}}{4}\right)^2.$$

Seconde méthode : On sait que z_1 et z_2 sont racines de P'. Cherchons alors les racines de P'. On a $P' = 80X^4-60X^2+5 = 5(16X^4-12X^2+1)$. L'équation $16x^4-12x^2+1 = 0$ est une équation bicarré, on la résout on posant $y = x^2$ et cela devient $16y^2-12y+1 = 0$ dont les solutions sont :

$$\frac{3-\sqrt{5}}{8} \text{ et } \frac{3+\sqrt{5}}{8}$$

donc les racines de P' sont :

$$\sqrt{\frac{3-\sqrt{5}}{8}},\ -\sqrt{\frac{3-\sqrt{5}}{8}},\ \sqrt{\frac{3+\sqrt{5}}{8}},\ -\sqrt{\frac{3+\sqrt{5}}{8}}$$

On peut vérifier en calculant que parmis ces 4 nombres, il y a les deux racines de P différentes de 1 qui sont :

$$\sqrt{\frac{3-\sqrt{5}}{8}} \text{ et } -\sqrt{\frac{3+\sqrt{5}}{8}},$$

et donc,

$$P = 16(X-1)\left(X-\sqrt{\frac{3-\sqrt{5}}{8}}\right)^2\left(X+\sqrt{\frac{3+\sqrt{5}}{8}}\right)^2,$$

ce qui conclut.
Remarque : On pourrait penser que les factorisations trouvées sont différentes mais on peut vérifier que :

$$\sqrt{\frac{3-\sqrt{5}}{8}} = \frac{-1+\sqrt{5}}{4} \text{ et } -\sqrt{\frac{3+\sqrt{5}}{8}} = \frac{-1-\sqrt{5}}{4}.$$

Solution 13. (Enoncé)
On peut écrire $X^2+2 = (X+i\sqrt{2})(X-i\sqrt{2})$ avec $X+i\sqrt{2}$ et $X-i\sqrt{2}$ premiers entre eux, donc en vertu du lemme de Gauss, X^2+2 divise P si seulement si $X+i\sqrt{2}$ et $X-i\sqrt{2}$ divisent P. Cette dernière condition se traduit par $P(i\sqrt{2}) = P(-i\sqrt{2}) = 0$ et donc X^2+2 divise P si et seulement si

$$\begin{cases} P(i\sqrt{2}) = 4 - 2i\sqrt{2} - 2\lambda + i\mu\sqrt{2} + 2 = 0 \quad (1) \\ P(-i\sqrt{2}) = 4 + 2i\sqrt{2} - 2\lambda - i\mu\sqrt{2} + 2 = 0 \quad (2) \end{cases}$$

En faisant $(1)+(2)$, il vient : $12 - 4\lambda = 0$ *i.e* $\lambda = 3$. En faisant $(1)-(2)$ il vient $-4i\sqrt{2} + 2i\mu\sqrt{2} = 0$ *i.e.* $\mu = 2$. Ainsi, X^2+2 divise P si et seulement si $\lambda = 3$ et $\mu = 2$.

Solution 14. (Enoncé)
On effectue l'algorithme d'Euclide étendu.
1. On pose $R_0 = X^3+1$, $R_1 = X^3+1$, $U_0 = 1$, $U_1 = 0$, $V_0 = 0$ et $V_1 = 1$. La première division euclidienne donne :

$$\begin{array}{r|l} X^3+1 & X^3-1 \\ \hline -X^3+1 & 1 \\ \hline 2 & \end{array}$$

donc $Q_1 = 1$ et $R_2 = 2$, on peut s'arrêter ici car le prochaine étape donnera forcément un reste nul. On calcule alors $U_2 = 1$ et $V_2 = -1$, ce qui donne la relation de Bézout suivante :

$$(1)\times(X^3+1) - (1)\times(X^3-1) = 2$$

et le pgcd entre X^3+1 et X^3-1 vaut 1 (le pgcd est pris unitaire).

2. On pose $R_0 = (X+1)^3$, $R_1 = (X-1)^3$, $U_0 = 1$, $U_1 = 0$, $V_0 = 0$ et $V_1 = 1$. La première division euclidienne donne :

$$\begin{array}{r|l} X^3+3X^2+3X+1 & X^3-3X^2+3X-1 \\ \hline -X^3+3X^2-3X+1 & 1 \\ \hline 6X^2 \qquad +2 & \end{array}$$

donc $Q_1 = 1$ et $R_2 = 6X^2 + 2$. On calcule $U_2 = 1 - 1 \times 0 = 1$ et $V_2 = 0 - 1 \times 1 = -1$. On fait ensuite la division euclidienne suivante :

$$\begin{array}{rl|l} X^3 - 3X^2 + 3X - 1 & & 6X^2 + 2 \\ \cline{3-3} -X^3 \qquad - \frac{1}{3}X & & \frac{1}{6}X - \frac{1}{2} \\ \cline{1-1} -3X^2 + \frac{8}{3}X - 1 & & \\ 3X^2 \qquad + 1 & & \\ \cline{1-1} \frac{8}{3}X & & \end{array}$$

donc $Q_2 = \frac{1}{6}X - \frac{1}{2}$, $R_3 = \frac{8}{3}X$. On calcule $U_3 = 0 - (\frac{1}{6}X - \frac{1}{2}) \times 1 = -\frac{1}{6}X + \frac{1}{2}$ et $V_3 = 1 + (\frac{1}{6}X - \frac{1}{2}) = \frac{1}{6}X + \frac{1}{2}$. On fait ensuite la division euclidienne suivante :

$$\begin{array}{rl|l} 6X^2 + 1 & & \frac{8}{3}X \\ \cline{3-3} -6X^2 & & \frac{9}{4}X \\ \cline{1-1} 1 & & \end{array}$$

donc $Q_3 = \frac{9}{4}$ et $R_4 = 1$, on peut s'arrêter ici car le prochaine étape donnera forcément un reste nul. On calcule $U_4 = 1 + (\frac{1}{6}X - \frac{1}{2})\frac{9}{4}X = \frac{3}{8}X^2 - \frac{9}{8}X + 1$ et $V_4 = -1 - (\frac{1}{6}X + \frac{1}{2})\frac{9}{4}X = -\frac{3}{8}X^2 - \frac{9}{8}X - 1$ ce qui donne la relation de Bézout suivante :

$$(\frac{3}{8}X^2 - \frac{9}{8}X + 1) \times (X+1)^3 + (-\frac{3}{8}X^2 - \frac{9}{8}X - 1) \times (X-1)^3 = 2$$

et le pgcd entre $(X+1)^3$ et $(X-1)^3$ vaut 1 (le pgcd est pris unitaire).

3. On pose $R_0 = X^3 + X^2 + 1$, $R_1 = X^3 + X + 1$, $U_0 = 1$, $U_1 = 0$, $V_0 = 0$ et $V_1 = 1$. La première division euclidienne donne :

$$\begin{array}{rl|l} X^3 + X^2 \qquad + 1 & & X^3 + X + 1 \\ \cline{3-3} -X^3 \qquad - X - 1 & & 1 \\ \cline{1-1} X^2 - X & & \end{array}$$

donc $Q_1 = 1$, $R_2 = X^2 - X$, $U_2 = 1$ et $V_2 = -1$. On fait ensuite la division euclidienne suivante :

$$\begin{array}{rl|l} X^3 \qquad + X + 1 & & X^2 - X \\ \cline{3-3} -X^3 + X^2 & & X + 1 \\ \cline{1-1} X^2 + X & & \\ -X^2 + X & & \\ \cline{1-1} 2X + 1 & & \end{array}$$

donc $Q_2 = X + 1$, $R_2 = 2X + 1$, $U_3 = -X - 1$ et $V_3 = 1 + X + 1 = X + 2$. La division euclidienne suivante donne :

$$\begin{array}{rl|l} X^2 \ - X & & 2X + 1 \\ \cline{3-3} -X^2 - \frac{1}{2}X & & \frac{1}{2}X - \frac{3}{4} \\ \cline{1-1} -\frac{3}{2}X & & \\ \frac{3}{2}X + \frac{3}{4} & & \\ \cline{1-1} \frac{3}{4} & & \end{array}$$

donc $Q_3 = \frac{1}{2}X - \frac{3}{4}$, $R_4 = \frac{3}{4}$ il est inutile de faire l'étape d'après car le reste sera forcément nul. On calcule alors $U_4 = 1 + (X+1)(\frac{1}{2}X - \frac{3}{4}) = \frac{1}{2}X^2 - \frac{1}{4}X + \frac{1}{4}$ et $V_4 = -1 - (X + 2)(\frac{1}{2}X - \frac{3}{4}) = -\frac{1}{2}X^2 - \frac{1}{4}X + \frac{1}{2}$ ce qui donne la relation de Bezout suivante :

$$\left(\frac{1}{2}X^2 - \frac{1}{4}X + \frac{1}{4}\right) \times \left(X^3 + X^2 + 1\right) + \left(-\frac{1}{2}X^2 - \frac{1}{4}X + \frac{1}{2}\right) \times \left(X^3 + X + 1\right) = \frac{3}{4}$$

Solution 15. (Enoncé)
Les deux polynômes sont à coefficients dans $\mathbb{Q}$, l'algorithme d'Euclide assure que le pgcd est le même dans $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$.
On utilise l'algorithme d'Euclide en faisant des divisions euclidiennes successives.

$$\begin{array}{rl|l} X^5+5X^4+9X^3+7X^2+5X+3 & & X^4+2X^3+2X^2+X+1 \\ \cline{3-3} -X^5-2X^4-2X^3\ -X^2\ -X & & X+3 \\ \cline{1-2} 3X^4+7X^3+6X^2+4X+3 & & \\ -3X^4-6X^3-6X^2-3X-3 & & \\ \cline{1-2} X^3\qquad +X & & \end{array}$$

puis,

$$\begin{array}{rl|l} X^4+2X^3+2X^2\ +X+1 & & X^3+X \\ \cline{3-3} -X^4\qquad -X^2 & & X+2 \\ \cline{1-2} 2X^3\ +X^2\ +X & & \\ -2X^3\qquad -2X & & \\ \cline{1-2} X^2\ -X+1 & & \end{array}$$

puis,

$$\begin{array}{rl|l} X^3\qquad +X & & X^2-X+1 \\ \cline{3-3} -X^3+X^2-X & & X+1 \\ \cline{1-2} X^2 & & \\ -X^2+X-1 & & \\ \cline{1-2} X-1 & & \end{array}$$

$$\begin{array}{rl|l} X^2-X+1 & & X-1 \\ \cline{3-3} -X^2+X & & X \\ \cline{1-2} 1 & & \end{array}$$

On a un reste qui vaut 1, il est inutile de continuer à l'étape d'après car le reste sera forcément nul. Le pgcd recherché vaut donc 1.
Remarque : En calculant les polynômes U_i et V_i dans l'algorithme d'Euclide on peut en déduire la relation de Bézout suivante :

$$\begin{aligned}(-X^3-3X^3-4X-2)\times(X^5+5X^4+9X^3+7X^2+5X+3)\\ +(-X^4-6X^3-14X^2-15X-7)(X^4+2X^3+2X^2+X+1)=-13\end{aligned}$$

Solution 16. (Enoncé)
Il est clair que le polynôme nul convient. Soit maintenant $P\in\mathbb{C}[X]$ de degré $n\geq 1$, tel que P' divise P. Alors il existe $Q\in\mathbb{C}[X]$ tel que $P=QP'$, l'analyse des degrés montrent que nécessairement $\deg(Q)=1$. On écrit $Q=\lambda(X-\alpha)$ avec $\alpha\in\mathbb{C}$. On propose deux méthodes :
Première méthode : Supposons que P admette une autre racine différente de α que l'on note β et l'on note $m\geq 1$ sa multiplicité. Alors β est de multiplicité $m-1$ dans P' or dans l'égalité $P=\lambda P'(X-\alpha)$, β est racine de multiplicité m à gauche et $m-1$ à droite ce qui est absurde et donc β n'existe pas.
Donc P admet une unique racine α, comme P est scindé dans $\mathbb{C}$ car $\mathbb{C}$ algébriquement clos, on peut écrire :

$$P=\lambda(X-\alpha)^n$$

avec $n \geq 1$ et $\lambda \in \mathbb{C}$. Inversement, si P est de cette forme alors P' divise P.
Seconde méthode : Si l'on écrit $P = \sum_{k=0}^{n} a_k X^n$, le coefficient dominant de P est a_n, le coefficient dominant de QP' est $n\lambda a_n$. En identifiant les coefficients dominants il vient :

$$\lambda = \frac{1}{n}.$$

On utilise maintenant la formule de Taylor en α pour P et P' *i.e.*

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k = \sum_{k=1}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \tag{1}$$

$$P' = \sum_{k=0}^{n-1} \frac{(P'(\alpha))^{(k)}}{k!}(X-\alpha)^k = \sum_{k=0}^{n-1} \frac{P^{(k+1)}(\alpha)}{k!}(X-\alpha)^k$$

De l'égalité $P = QP'$ on peut écrire :

$$\sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k = n(X-\alpha)\sum_{k=0}^{n-1} \frac{P^{(k+1)}(\alpha)}{k!}(X-\alpha)^k = \sum_{k=0}^{n-1} \frac{nP^{(k+1)}(\alpha)}{k!}(X-\alpha)^{k+1} \tag{2}$$

Par changement d'indice $j = k+1$, la seconde somme s'écrit :

$$\sum_{k=0}^{n-1} \frac{nP^{(k+1)}(\alpha)}{k!}(X-\alpha)^{k+1} = \sum_{j=1}^{n} \frac{nP^{(j)}(\alpha)}{(j-1)!}(X-\alpha)^j \tag{3}$$

Comme la famille $((X-\alpha)^k)_{k\geq 0}$ est une base de $\mathbb{C}[X]$ on peut identifier les coefficients à partir des équations 2 et 3 pour obtenir :

$$\forall k \in [\![1; n]\!], \quad \frac{P^{(k)}(\alpha)}{k!} = \frac{nP^{(k)}(\alpha)}{(k-1)!}$$

ce qui donne nécessairement $P^{(k)}(\alpha) = 0$ pour $k < n$. En reprenant l'équation 1, il vient :

$$P = \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n.$$

Inversement, si P est de cette forme alors P' divise P.
Conclusion : Les polynômes P de $\mathbb{C}[X]$ tels que P' divise P sont ceux de la forme $P = \lambda(X-\alpha)^n$ avec $n \geq 1$ et $(\lambda, \alpha) \in \mathbb{C}^2$.

Solution 17. (Enoncé)
1. On écrit $n = mk + r$ la division euclidienne de n par m. Alors :

$$X^n - 1 = X^{(km+r)} - 1 = X^{km}X^r - 1 = X^{km}X^r - X^r + X^r - 1 = X^r(X^{km} - 1) + X^r - 1$$

or comme,

$$X^{km} - 1 = (X^m - 1)\sum_{i=0}^{k-1} X^{im}$$

donc,

$$X^n - 1 = (X^m - 1)Q + X^r - 1$$

avec $Q = X^r \sum_{i=0}^{k-1} X^{im}$ et $\deg(X^r - 1) < \deg(X^m - 1)$: c'est donc la division euclidienne de $X^n - 1$ par $X^m - 1$.
2. L'algorithme d'Euclide sur $\mathbb{Z}$ nous donne deux suites $(q_n)_n$ et (r_n) telle que $r_0 = n$, $r_1 = m$ et il existe un indice k tel que $r_k = \text{pgcd}(n, m)$ et $r_{k+1} = 0$. De plus, pour tout $j \geq 1$:

$$r_{j-1} = q_j r_j + r_{j+1}.$$

En faisant l'algorithme d'EUCLIDE étendu avec X^n-1 et X^m-1, par la première question, à la i-ème étape, le reste est $R_i = X^{r_{i+1}} - 1$. donc à la k-ème étape, le reste est nul. Le pgcd est donc le dernier reste non nul qui vaut $R_{k-1} = X^{r_k} - 1 = X^{\mathrm{pgcd}(n,m)} - 1$ et donc :

$$\mathrm{pgcd}(X^n - 1, X^m - 1) = X^{\mathrm{pgcd}(n,m)} - 1.$$

Solution 18. (Enoncé)
1. Si $k = l$, alors :

$$L_k(k) = \prod_{i=1, i\neq k}^{n} \frac{k-i}{k-i} = \prod_{i=1, i\neq k} 1 = 1.$$

Si $l \neq k$, alors :

$$L_k(l) = \prod_{i=1, i\neq k}^{n} \frac{l-i}{k-i} = \frac{l-1}{k-1} \times \frac{l-2}{k-2} \times \cdots \times \frac{l-(k-1)}{k-(k-1)} \times \frac{l-(k+1)}{k-(k+1)} \times \cdots \times \frac{l-n}{k-n} = 0$$

car un des facteurs est nul (celui pour $i = l$).
2. On pose $Q(X) = P(X) - \sum_{k=1}^{n} r^k L_k(X)$, notre but va être de montrer que Q est le polynôme nul. On va utiliser une technique classique avec les polynômes : on va montrer que Q admet strictement plus de racines que son degré.
En utilisant la formule $\deg(A+B) \leq \max(\deg(A), \deg(B))$ il vient :

$$\deg(Q) \leq \max(\deg(P), \deg(-\sum_{k=1}^{n} r^k L_k(X)))$$

Or, la encore en utilisant la formule $\deg(A+B) \leq \max(\deg(A), \deg(B))$ il vient,

$$\deg\left(-\sum_{k=1}^{n} r^k L_k(X)\right) = \deg\left(\sum_{k=1}^{n} r^k L_k(X)\right) \leq \max_{k=1}^{n} \deg(r^k L_k(X)) \leq \max_{k=1}^{n} \deg(L_k(X)) \leq n-1$$

car,

$$\deg(L_k(X)) = \sum_{i=1, i\neq k}^{n} \deg\left(\frac{X-i}{k-i}\right) = \sum_{i=1, i\neq k}^{n} 1 = n-1.$$

Donc,

$$\deg(Q) \leq n-1.$$

De plus pour $l \in [\![1; n]\!]$,

$$Q(l) = P(l) - \sum_{k=1}^{n} r^k L_k(l) = P(l) - r^l = 0$$

en utilisant l'hypothèse sur P et la question 1. Donc $Q = 0$ et cela conclut la question.
3. D'après la question précédente,

$$P(n+1) = \sum_{k=1}^{n} r^k L_k(n+1)$$

Calculons $L_k(n+1)$, on suppose d'abord $2 \leq k \leq n-1$ dans les calculs qui suivent :

$$\begin{aligned} L_k(n+1) &= \frac{n+1-1}{k-1} \times \frac{n+1-2}{k-2} \times \cdots \times \frac{n+1-(k-1)}{k-(k-1)} \frac{n+1-(k+1)}{k-(k+1)} \times \cdots \times \frac{n-(n-1)}{k-n} \\ &= \frac{n}{k-1} \times \frac{n-1}{k-2} \times \cdots \times \frac{n-k+2}{1} \times \frac{n-k}{-1} \times \cdots \times \frac{1}{k-n} \end{aligned}$$

Au numérateur, on a presque du $n!$, il manque le facteur $n-k+1$, on force son apparition et le numérateur vaut alors :

$$\frac{n!}{n-k+1}$$

Le dénominateur vaut :

$$(k-1)\times\cdots\times 1\times(-1)\times\cdots\times(k-n)=(k-1)!(-1)^{n-k}(n-k)!$$

ou l'on a factorisé par (-1) dans la partie droite du produit pour faire apparaître $(n-k)!$.
On en déduit donc :

$$L_k(n+1)=\frac{n!}{(n-k+1)(k-1)!(-1)^{n-k}(n-k)!}=(-1)^{n-k}\frac{n!}{(k-1)!(n-k+1)!}=(-1)^{n-k}\binom{n}{k-1}$$

et l'on vérifie que cette formule reste vraie si $k=1$ ou $k=n$.
On peut maintenant terminer le calul de $P(n+1)$, on écrit :

$$P(n+1)=\sum_{k=1}^{n}r^kL_k(n+1)=\sum_{k=1}^{n}r^k(-1)^{n-k}\binom{n}{k-1}$$

L'idée va être de faire apparaître un binome de Newton. On fait un changement d'indice $j=k-1$ dans la somme :

$$\begin{aligned}
P(n+1)&=\sum_{j=0}^{n-1}r^{j+1}(-1)^{n+1-j}\binom{n}{j}\\
&=-r\sum_{j=0}^{n-1}\binom{n}{j}r^j(-1)^{n-j}\\
&=-r\left(\sum_{j=0}^{n-1}\binom{n}{j}r^j(-1)^{n-j}+r^n-r^n\right)\\
&=-r\left(\sum_{j=0}^{n}\binom{n}{j}r^j(-1)^{n-j}-r^n\right)\\
&=-r((r-1)^n-r^n)\\
&=r^{n+1}-r(r-1)^n
\end{aligned}$$

et cela conclut.

Solution 19. (Enoncé)
Soit $P=(X+1)^n-X^n-1$ et $Q=X^2+X+1$.
Comme ces deux polynômes sont à coefficients dans $\mathbb{Q}$, l'algorithme de division euclidienne assure que :

$$Q\mid P \text{ dans } \mathbb{C}[X]\iff Q\mid P \text{ dans } \mathbb{Q}[X].$$

On peut donc travailler maintenant dans $\mathbb{C}[X]$. Ecrivons $Q=(X-j)(X-\overline{j})$ avec $j=e^{\frac{2i\pi}{3}}$.
Comme $X-j$ et $X-\overline{j}$ sont premiers entre eux, le lemme de Gauss assure que :

$$Q\mid P\iff (X-j)\mid P \text{ et } (X-\overline{j})\mid P$$

Par le cours, cette dernière condition équivaut à $P(j)=P(\overline{j})=0$. Comme P est à coefficients dans $\mathbb{Q}\subset\mathbb{R}$, on a $P(\overline{j})=\overline{P(j)}$, donc il suffit de vérifier pour quels n on a $P(j)=0$. On calcule alors $P(j)$:

$$P(j)=(j+1)^n-j^n-1=(-1)^nj^{2n}-j^n-1$$

On calcule alors selon les valeurs de n mod 6.
Si $n\equiv 0[6]$:

$$P(j)=1-1-1=-1\neq 0.$$

Si $n\equiv 1[6]$:

$$P(j)=-j^2-j-1=0.$$

Si $n \equiv 2[6]$:

$$P(j) = j - j^2 - 1 = 2j - 2 \neq 0$$

Si $n \equiv 3[6]$:

$$P(j) = -1 - 1 - 1 = -3.$$

Si $n \equiv 4[6]$:

$$P(j) = j^2 - j - 1 = -2j - 2 \neq 0.$$

Si $n \equiv 5[6]$:

$$P(j) = -j - j^2 - 1 = 0.$$

Où l'on a utilisé la relation $j^2 + j + 1 = 0$. En conclusion Q divise P si et seulement si $n \equiv 1[6]$ ou $n \equiv 5[6]$.

Solution 20. (Enoncé)
1. On écrit $P = \sum_{l=0}^{r} a_l X^l$. On fait les calculs dans $\mathbb{Z}/m\mathbb{Z}$, il s'agit donc de montrer que $\overline{P(n+km)} = \overline{0}$ dans $\mathbb{Z}/m\mathbb{Z}$:

$$\overline{P(n+km)} = \overline{\sum_{l=0}^{r} a_l (n+km)^l} = \overline{\sum_{l=0}^{r} a_l \sum_{j=0}^{l} \binom{l}{j} n^j (km)^{l-j}} = \sum_{l=0}^{r} \overline{a_l} \sum_{j=0}^{l} \overline{\binom{l}{j}} \overline{n}^j \overline{km}^{l-j}$$

Or pour $j < l$, $\overline{km}^{l-j} = \overline{0}$ dans $\mathbb{Z}/m\mathbb{Z}$ et donc :

$$\overline{P(n+km)} \sum_{l=0}^{r} \overline{a_l n}^l = \overline{\sum_{l=0}^{r} a_l n^l} = \overline{P(n)} = \overline{m} = \overline{0}$$

et cela conclut.
2. Supposons par l'absurde l'existence d'un tel polynôme. Comme $\deg(P) \geq 1$ (P est non constant), il existe $n \geq 1$ tel que $P(n)$ soit un entier vérifiant $|P(n)| \geq 2$. On utilise la question 1. avec cet entier n. Alors par hypothèse $P(n+km)$ est premier, mais aussi divisible par $P(n)$ donc nécessairement $P(n) = 1$ ou $P(n) = P(n+km)$, le premier cas étant exclu il vient :

$$\forall k \geq 0, \quad m = P(n) = P(n+km)$$

Le polynôme $Q(X) = P(X) - m$ admet donc une infinité de racines (tous les entiers naturels de la forme $n + km$) donc c'est le polynôme nul donc P est constant : c'est absurde car l'on avait supposé P de degré ≥ 1.