Énoncés : V. Gritsenko
Corrections : J.-F. Barraud

Anneaux de polynômes I

Exercice 1

1. Soit A un anneau quelconque. Alors l'anneau de polynômes $A[x]$ n'est pas un corps.
2. Montrer que pour un anneau intègre A, les polynômes unitaires linéaires de $A[x]$ sont irréductibles.
3. Décrire tous les polynômes irréductibles de $\mathbb{C}[x]$ et de $\mathbb{R}[x]$.
4. Démontrer que pour tout corps K, l'anneau de polynômes $K[x]$ a une infinité de polynoḿes unitaires irréductibles.

Correction ▼ [002261]

Exercice 2

1. Montrer que l'idéal (x,n) où $n \in \mathbb{Z}$, $n > 1$ de l'anneau $\mathbb{Z}[x]$ n'est pas principal.
2. Soit A un anneau intègre. Montrer que $A[x]$ est principal ssi A est un corps.

Correction ▼ [002262]

Exercice 3

Soit $f(x) \in A[x]$ un polynôme sur un anneau A. Supposons que $(x-1) \mid f(x^n)$. Montrer que $(x^n-1) \mid f(x^n)$.

Correction ▼ [002263]

Exercice 4

Pour $n,m \geqslant 2$, déterminer le reste de la division euclidienne du polynôme $(x-2)^m+(x-1)^n-1$ par $(x-1)(x-2)$ dans $\mathbb{Z}[x]$.

Correction ▼ [002264]

Exercice 5

1. Si K est un corps, montrer qu'un polynôme P de degré 2 ou 3 dans $K[x]$ est irréductible si et seulement si il n'a pas de zéro dans K.
2. Trouver tous les polynômes irréductibles de degré 2, 3 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.
3. En utilisant la partie précédente, montrer que les polynômes $5x^3+8x^2+3x+15$ et $x^5+2x^3+3x^2-6x-5$ sont irréductibles dans $\mathbb{Z}[x]$.
4. Décrire tous les polynômes irréductibles de degré 4 et 5 sur $\mathbb{Z}/2\mathbb{Z}$.

Correction ▼ [002265]

Exercice 6

1. Trouver tous les polynômes irréductibles de degré 2, 3 à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.
2. Décomposer les polynômes suivants en facteurs irréductibles dans $\mathbb{F}_3[x]$.

$$x^2+x+1, \qquad x^3+x+2, \qquad x^4+x^3+x+1\ .$$

Correction ▼ [002266]

Exercice 7

En utilisant les réductions mod 2 ou mod 3 montrer que les polynômes $x^5 - 6x^3 + 2x^2 - 4x + 5$, $7x^4 + 8x^3 + 11x^2 - 24x -$ sont irréductibles dans $\mathbb{Z}[x]$.

Correction ▼ [002267]

Exercice 8

Soient

$$f(x) = (x-a_1)(x-a_2)\dots(x-a_n) - 1, \quad g(x) = (x-a_1)^2(x-a_2)^2\dots(x-a_n)^2 + 1$$

où $a_1, \dots a_n \in \mathbb{Z}$ soient deux à deux distincts. Montrer que f et g sont irréductibles dans $\mathbb{Q}[x]$.

Correction ▼ [002268]

Exercice 9

Soient $f, g \in \mathbb{Q}[x]$. Supposons que f soit irréductible et qu'il existe $\alpha \in \mathbb{C}$ tel que $f(\alpha) = g(\alpha) = 0$. Alors f divise g.

Correction ▼ [002269]

Exercice 10

Pour quel n, m dans $\mathbb{Z}$ la fraction

$$\frac{11n+2m}{18n+5m}$$

est réductible ?

Correction ▼ [002270]

Exercice 11

Trouver le pgcd$(x^n - 1, \ x^m - 1)$ dans $\mathbb{Z}[x]$.

Correction ▼ [002271]

Exercice 12

Trouver le pgcd(f, g) dans $\mathbb{Z}_2[x]$ et sa représentation linéaire $fu + gv$ où $d, u, v \in \mathbb{Z}_2[x]$:

1. $$f = x^5 + x^4 + 1, \qquad g = x^4 + x^2 + 1;$$

2. $$f = x^5 + x^3 + x + 1, \qquad g = x^4 + 1.$$

Correction ▼ [002272]

Exercice 13

Trouver le pgcd(f, g) dans $\mathbb{Z}_3[x]$ et $\mathbb{Z}_5[x]$ de $f = x^4 + 1$, $g = x^3 + x + 1$.

Correction ▼ [002273]

Exercice 14

Trouver le pgcd(f, g) dans $\mathbb{Z}[x]$ de $f = x^4 + x^3 - 3x^2 - 4x - 1$ et $g = x^3 + x^2 - x - 1$.

Correction ▼ [002274]

Exercice 15

Montrer que f est irréductible dans $\mathbb{Q}[x]$:

1. $f = x^4 - 8x^3 + 12x^2 - 6x + 2$;

2. $f = x^5 - 12x^3 + 36x - 12$;
3. $f = x^4 - x^3 + 2x + 1$;
4. $f = x^{p-1} + \cdots + x + 1$, où p est premier.

Correction ▼ [002275]

Exercice 16

Soient $A = \mathbb{Z}[\sqrt{-3}]$ et K son corps de fractions. Montrer que $x^2 - x + 1$ est irréductible dans $A[x]$ sans pour autant être irréductible dans $K[x]$. Expliquer la contradiction apparente avec le corollaire du lemme de Gauss.

Correction ▼ [002276]

Exercice 17

Soit $P \in \mathbb{Z}[x]$.

1. Supposons que $P(0)$, $P(1)$ soient impairs. Montrer que P n'a pas de racine dans $\mathbb{Z}$. (*Indication :* Utiliser la réduction modulo 2.)
2. Soit $n \in \mathbb{N}$ tel qu'aucun des entiers $P(0), \dots, P(n-1)$ ne soit divisible par n. Montrer que P n'a pas de racine dans $\mathbb{Z}$.

Correction ▼ [002277]

Exercice 18

1. Soit $P \in \mathbb{Z}[x]$. Soit $\frac{a}{b}$ sa racine rationnelle : $P(\frac{a}{b}) = 0$, $\text{pgcd}(a,b) = 1$. Montrer que $\forall k \in \mathbb{Z} \quad (a - bk)$ divise $P(k)$.
2. Quelles racines rationnelles ont les polynômes $f(x) = x^3 - 6x^2 + 15x - 14$ et $g(x) = 2x^3 + 3x^2 + 6x - 4$?

Correction ▼ [002278]

Exercice 19

1. Soient $P \in \mathbb{Z}[x]$, $n \in \mathbb{N}$, $m = P(n)$. Montrer que $\forall k \in \mathbb{Z} \quad m \mid P(n + km)$.
2. En déduire qu'il n'existe aucun polynôme $P \in \mathbb{Z}[x]$, non constant, tel que, pour tout $n \in \mathbb{Z}$, $P(n)$ soit un nombre premier.

Correction ▼ [002279]

Correction de l'exercice 1 ▲

1. Le polynôme X n'est jamais inversible dans $A[X]$. Si A n'est pas intègre, comme $A \subset A[X]$, $A[X]$ ne l'est pas non plus et ne peut pas être un corps. Si A est intègre et si $X = PQ$, alors $\deg(P)+\deg(Q) = 1$ donc P ou Q est une constante. Supposons par exemple que ce soit P. $P|X$ donc $P|1$ donc P est inversible, et $Q \sim X$.
2. Soit $P = X+a$ un polynôme unitaire linéaire de $A[X]$. Supposons que $P = P_1P_2$. Comme A estintègre, on a $\deg(P_1)+\deg(P_2) = 1$, donc P_1 ou P_2 est une constante. Supposons que ce soit P_1. Alors $P_1|1$ et $P_1|a$. En particulier, P_1 est inversible, et donc $P_2 \sim P$.
3. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 (théorème de Gauss).

   Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelles. En effet, soit $P \in \mathbb{R}[X]$. P se factorise sur $\mathbb{C}[X]$ sous la forme $P = a\prod(X-\lambda_i)^{\nu_i}$ (avec $i \neq j \Rightarrow \lambda_i \neq \lambda_j$). Comme cette factorisation est unique, et que $P = \overline{P}$, on en déduit que si λ_i est racine de P avec multiplicité ν_i, alors il en va de même pour $\overline{\lambda_i}$. Ainsi, on obtient une factorisation de P dans $\mathbb{R}[X]$: $P = a\prod_{\lambda_i\in\mathbb{R}}(X-\lambda_i)^{\nu_i}\prod(X^2-2\mathrm{Re}(\lambda_i)X+|\lambda_i|^2)^{\nu_i}$.

   P est donc irréductible ssi P est de la forme $P = a(X-\lambda)$ avec $\lambda \in \mathbb{R}$ ou $P = a(X^2-2\mathrm{Re}(\lambda_i)X+|\lambda_i|^2)$ avec $\lambda \notin \mathbb{R}$.
4. Supposons que $K[X]$ ait un nombre fini de polynômes unitaires irréductibles $P_1,\dots,P_k$. Soit alors $P = \prod_{i=1}^k P_i + 1$.

   Comme K est un corps, les irréductibles sont de degré au moins 1, et donc P n'est pas l'un des P_i. Comme P est unitaire, P n'est pas irréductible. En particulier, l'un au moins des P_i divise P. Supposons par exemple que ce soit P_1 : $\exists Q \in K[X], P = P_1Q$. Alors $P_1(Q-\prod_{i=2}^k P_i) = 1$. Donc P_1 est inversible, ce qui est faux.

Correction de l'exercice 2 ▲

1. Supposons (X,n) principal dans $\mathbb{Z}[X]$: $(X,n) = (P_0)$. Alors $P_0|n$ donc $P_0 \in \mathbb{Z}$, et $P_0|X$ donc $P_0 = \pm 1$. Ainsi $(P_0) = \mathbb{Z}[X]$. Or (X,n) est l'ensemble des polynômes dont le terme constant est un multiple de n : en effet, si $P \in (X,n)$, $\exists A,B \in \mathbb{Z}[X], P = AX+Bn$ donc le terme constant de P est un multiple de n. Réciproquement, si le terme constant de $P = \sum p_iX^i$ est un multiple de n, $p_0 = p_0'n$, alors $P = X(\sum_{i\geqslant 1} p_iX^i)+p_0'n \in (X,n)$. Ainsi, $1 \notin (X,n)$. Donc (X,n) n'est pas principal.
2. Si $A[X]$ est principal, soit $a \in A\setminus\{0\}$, et $I = (X,a)$. $A[X]$ étant principal, $\exists P_0 \in A[X], I = (P_0)$. Alors $P_0|a$ donc $P_0 \in A$, et $P_0|X$ donc $P_0|1$ et P_0 est inversible. On en déduit que $I = A[X]$. En particulier $1 \in I$: $\exists U,V \in A[X], XU+aV = 1$. Le terme constant de $XU+aV$ est multiple de a et vaut 1. a est donc inversible.

   Si A est un corps, on dispose de la division euclidienne. Soit I un idéal de $A[X]$. Soit P_0 un élément de $I\setminus\{0\}$ de degré minimal. Soit $P \in I$. $\exists!(Q,R) \in A[X]^2, P = P_0Q+R$ et $\deg(R) < \deg(P)$. Comme $R = P-P_0Q$, on a $R \in I$, et comme $\deg(R) < \deg(P_0)$, on a $R = 0$. Ainsi $P \in (P_0)$. On a donc $I \subset (P_0) \subset I$.

Correction de l'exercice 3 ▲

Notons $f(x^n) = P(x-1)$. Alors $f(1) = 0\cdot P(1) = 0$ et donc $(x-1)|f$. Notons $f = Q(x-1)$. On a alors $f(x^n) = Q(x^n)(x^n-1)$. (x^n-1) divise bien f.

Correction de l'exercice 4 ▲

Notons (Q,R) le quotient et le reste de cette division euclidienne : $(x-2)^m+(x-1)^n-1 = Q(x-2)(x-1)+R$ avec $\deg(R) \leqslant 1$. Notons $R = ax+b$. En évaluant en 1, on obtient $(-1)^m-1 = a+b$, et en évaluant en 2, $2a+b = 0$. On en déduit $b = -2a$ et $a = 1-(-1)^m$, soit $R = (1-(-1)^m)(x-2)$.

Correction de l'exercice 5 ▲

1. Soit P un polynôme de degré $d=2$ ou 3 de $K[X]$.

   Si P a une racine $a \in K$, alors $(X-a)|P$, et P n'est pas irréductible.

   Réciproquement, si $P=AB$ avec $A,B \in K[X]$ et $A,B \notin K[X]^{\times}=K\setminus\{0\}$, alors $\deg(A)\geqslant 1$, $\deg(B)\geqslant 1$, et $\deg(A)+\deg(B)=d=2$ ou 3, donc l'un au moins des deux polynômes A et B est de degré 1. On peut supposer que c'est A. Notons $A=aX+b$. Alors $(X+a^{-1}b)|P$, et $-a^{-1}b$ est racine de P.

   Finalement P a une racine ssi P n'est pas irréductible.

2. Irréductibles de degré 2 de $\mathbb{Z}/2\mathbb{Z}$: Soit $P=aX^2+bX+c$ un polynôme de degré 2. $a\neq 0$ donc $a=1$.

$$\begin{aligned}
P \text{ irréductible} &\Leftrightarrow P \text{ n'a pas de racine}\\
&\Leftrightarrow \begin{cases} P(0) & \neq 0\\ P(1) & \neq 0\end{cases}\\
&\Leftrightarrow \begin{cases} P(0) & =1\\ P(1) & =1\end{cases}\\
&\Leftrightarrow \begin{cases} c & =1\\ 1+b+1 & =1\end{cases}\\
&\Leftrightarrow P=X^2+X+1
\end{aligned}$$

   Ainsi, il y a un seul irréductible de degré 2, c'est $I_2=X^2+X+1$.

   Irréductibles de degré 3 de $\mathbb{Z}/2\mathbb{Z}$: Soit $P=aX^3+bX^2+cX+d$ un polynôme de degré 2. $a\neq 0$ donc $a=1$.

$$\begin{aligned}
P \text{ irréductible} &\Leftrightarrow P \text{ n'a pas de racine}\\
&\Leftrightarrow \begin{cases} d & =1\\ 1+b+c+1 & =1\end{cases}\\
&\Leftrightarrow \begin{cases} d & =1\\ (b,c) & =(1,0) \text{ ou } (b,c)=(0,1)\end{cases}\\
&\Leftrightarrow P=X^3+X+1 \text{ ou } P=X^3+X^2+1
\end{aligned}$$

   Ainsi, il y a deux irréductibles de degré 3 dans $\mathbb{Z}/3\mathbb{Z}[X]$: $I_3=X^3+X+1$ et $I_3'=X^3+X^2+1$.

3. Soit $P=5X^3+8X^2+3X+15\in\mathbb{Z}[X]$. Soient A et B deux polynômes tels que $P=AB$. L'application $\mathbb{Z}\to\mathbb{Z}/2\mathbb{Z}, n\mapsto\bar{n}$ induit une application $\mathbb{Z}[X]\to\mathbb{Z}/2\mathbb{Z}[X], P=\sum a_iX^i\mapsto\bar{P}=\sum\bar{a}_iX^i$. Cette application est compatible avec les opérations : en particulier $\overline{AB}=\bar{A}\bar{B}$ (pourquoi ?). Ainsi on a : $\bar{P}=\bar{A}\bar{B}$. Or $\bar{P}=X^3+X+1$ est irréductible, donc (quitte à échanger les rôles de A et B on peut supposer que) $\bar{A}=1$ et $\bar{B}=X^3+X+1$. On en déduit que B est au moins de degré 3, d'où $\deg(A)=0$. $A\in\mathbb{Z}$ et $A|P$, donc $A|5$, $A|8$, $A|3$, et $A|15$. On en déduit que $A=\pm1$. Finalement, $A=\pm1$ et $B\sim P$. P est donc irréductible dans $\mathbb{Z}[X]$.

   Soit $P=X^5+2X^3+3X^2-6x-5\in\mathbb{Z}[X]$. Soient A et B deux polynômes tels que $P=AB$. On a comme précédemment : $\bar{P}=\bar{A}\bar{B}$ où $\bar{P}=X^5+X^2+1$. $\bar{P}$ n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$, donc si $\bar{P}$ est réductible, il doit être le produit d'un irréductible de degré 2 et d'un irréductible de degré 3. Or $\bar{P}\neq I_2I_3$ et $\bar{P}\neq I_2I_3'$ (faire le calcul !), donc $\bar{P}$ est irréductible. Le même raisonnement montre alors que P est irréductible dans $\mathbb{Z}[X]$.

4. Un polynôme de degré 4 est réductible ssi il a une racine ou est le produit de deux irréductibles de degré

2. Soit $P = \sum_{i=0}^{4} a_i X^i \in \mathbb{Z}/2\mathbb{Z}[X]$, avec $a_4 = 1$.

$$P \text{ irréductible} \Leftrightarrow \begin{cases} P(0) \neq 0 \\ P(1) \neq 0 \\ P \neq I_2^2 \end{cases}$$
$$\Leftrightarrow \begin{cases} a_0 = 1 \\ 1 + a_3 + a_2 + a_1 + 1 = 1 \\ P \neq I_2^2 \end{cases}$$
$$\Leftrightarrow P \in \{X^4 + X^3 + 1, X^4 + X + 1, X^4 + X^3 + X^2 + X + 1\}$$

Un polynôme de degré 5 est irréductible ssi il n'a pas de racine et l'est pas le produit d'un irréductible de degré 2 et d'un irréductible de degré 3. Tous calculs fait, on obtient la liste suivante : $\{X^5 + X^2 + 1, X^5 + X^3 + 1, X^5 + X^4 + X^3 + X^2 + 1, X^5 + X^4 + X^3 + X + 1, X^5 + X^4 + X^2 + X + 1, X^5 + X^3 + X^2 + X + 1, \}$.

Correction de l'exercice 6 ▲

1. On raisonne exactement comme pour l'exercice 5. On peut réduire un peu les discussions en remarquant que puisqu'on est sur un corps, on peut se contenter de chercher les irréductibles *unitaires* : on obtient les autres en multipliant les irréductibles unitaires par les inversibles, soit ± 1.
   Les irréductibles de degré 2 sont caractérisés par $P(0) \neq 0$, $P(1) \neq 0$ et $P(-1) \neq 0$. On obtient finalement la liste suivante : $\{X^2 + 1, X^2 - X - 1, -X^2 - 1, -X^2 + X + 1\}$.

   Sans commentaire, on obtient la liste suivante pour les irréductibles de degré 3 de $\mathbb{Z}/3\mathbb{Z}[X]$: $\{\pm(X^3 + X^2 - X + 1), \pm(X^3 - X^2 + X + 1), \pm(X^3 - X^2 + 1), \pm(X^3 - X + 1), \pm(X^3 + X^2 + X - 1), \pm(X^3 - X^2 - X - 1) \pm (X^3 + X^2 - 1), \pm(X^3 - X - 1), \}$.
2. $X^2 + X + 1 = (X - 1)^2$
   $X^3 + X + 2 = (X + 1)(X^2 - X + 2)$
   $X^4 + X^3 + X + 1 = (X + 1)(X^3 + 1) = (X + 1)^4$

Correction de l'exercice 7 ▲

On raisonne comme pour l'exercice 5. Soit $P = X^5 - 6X^3 + 2X^2 - 4X + 5$, A, B deux polynômes tels que $P = AB$. En considérant la réduction modulo 2, on a $\bar{P} = X^5 + 1$ donc la décomposition en facteurs irréductibles est $\bar{P} = (X + 1)(X^4 + X^3 + X^2 + X + 1)$. Comme P est unitaire, A et B le sont aussi, et la réduction modulo 2 préserve donc le degré de A et B. On en déduit que si $\bar{A} = X + 1$, alors A est de degré 1.
La réduction modulo 3 de P devrait donc avoir une racine. Mais $P \mod 3 = X^5 - X^2 - X - 1$ n'a pas de racine dans $\mathbb{Z}/3\mathbb{Z}$. On en déduit que dans la réduction modulo 2, la factorisation $\bar{P} = `\bar{A}\bar{B}$ est triviale ($\bar{A} = 1$ et $\bar{B} = \bar{P}$ ou le contraire), puis que la factorisation $P = AB$ elle même est triviale ($A = \pm 1$ et $B = \mp P$ ou le contraire). Ainsi, P est irréductible dans $\mathbb{Z}[X]$.

Pour $P = 7X^4 + 8X^3 + 11X^2 - 24X - 455$, on procède de la même façon. Si $P = AB$, comme 7 est premier, l'un des polynômes A ou B a pour coefficient dominant ± 7 et l'autre ∓ 1. On en déduit que les réductions modulo 2 ou 3 préservent le degré de A et de B. Les décompositions en facteurs irréductibles sont les suivantes : $P \mod 2 = (X^2 + X + 1)^2$ et $P \mod 3 = (X - 1)(X^3 - X - 1)$. Si la factorisation $P = AB$ est non triviale, alors les réductions modulo 2 de A et B sont de degré 2, et donc $\deg(A) = \deg(B) = 2$. Mais la décomposition modulo 3 impose que ces degrés soient 1 et 3. La factorisation $P = AB$ est donc nécessairement triviale, et P est donc irréductible.

Correction de l'exercice 8 ▲

Commençons par montrer que ces polynômes sont irréductibles sur $\mathbb{Z}$.

-Le cas de $f = \prod_{i=1}^n (X-a_i) - 1$ Soit $P, Q \in \mathbb{Z}[X]$ tels que $f = PQ$. On peut supposer sans perte de généralité que P et Q ont des coefficients dominants positifs (i.e. sont unitaires).
On a : $\forall i, f(a_i) = P(a_i)Q(a_i) = -1$ donc

$$P(a_i) = \pm 1 \qquad \text{et} \qquad Q(a_i) = \mp 1$$

Soit $I = \{i, P(a_i) = -1\}$ et $J = \{1,\dots,n\} \setminus I$. On notera $|I|$ et $|J|$ le nombre d'éléments de I et J.
Supposons $I \neq \emptyset$ et $J \neq \emptyset$: Alors $\prod_{i\in I}(X-a_i) | (P+1)$ et $\prod_{i\in J}(X-a_i)|(Q+1)$. Ainsi $\deg(P+1) \geqslant |I|$ et $\deg(Q+1) \geqslant |J| = n - |I|$, et comme $\deg(P) + \deg(Q) = n$, on en déduit que $\deg(P) = |I|$ et $\deg(Q) = |J|$, puis que (puisque P et Q sont unitaires) :

$$P = \prod_{i\in I}(X-a_i) - 1 \qquad \text{et} \qquad Q = \prod_{i\in J}(X-a_i) - 1.$$

Ainsi $f = \prod_{k\in I\cup J}(X-a_k) - 1 = (\prod_{i\in I}(X-a_i)-1)(\prod_{j\in J}(X-a_j)-1) = f - \left(\prod_{i\in I}(X-a_i) + \prod_{j\in J}(X-a_j) - 2\right)$, donc $\prod_{i\in I}(X-a_i) + \prod_{j\in J}(X-a_j) - 2 = 0_{\mathbb{Z}[X]}$, ce qui est faux.
Ainsi $I = \emptyset$ ou $J = \emptyset$. On peut supposer sans perte de généralité que $I = \emptyset$. Alors $\forall i \in \{1,\dots,n\}, Q(a_i) = -1$. Donc les a_i sont tous racine de $Q+1$. Comme $\deg(Q+1) \leqslant n$ et $Q+1 \neq 0$, on en déduit que $Q = f$, et $P = 1$.
f est donc bien irréductible dans $\mathbb{Z}[X]$.

-Le cas de $g = \prod_{i=1}^n (X-a_i)^2 + 1$. Supposons que $g = PQ$, avec $P, Q \in \mathbb{Z}[X]$.On a $g(a_i) = 1 = P(a_i)Q(a_i)$, donc $P(a_i) = Q(a_i) = \pm 1$.
Comme g n'a pas de racine réelle, il en va de même de P et Q, qui sont donc de signe constant (théorème des valeurs intermédiaires pour les fonctions continues sur $\mathbb{R}$!). On peut donc supposer sans perte de généralité que P et Q sont positifs.
Alors $P(a_i) = Q(a_i) = 1$. Ainsi, tous les a_i sont racines de $P-1$ et de $Q-1$. On a donc $\prod_{i=1}^n (X-a_i) | P-1$ et $\prod_{i=1}^n (X-a_i) | Q-1$.
En particulier, si $P-1 \neq 0$ et $Q-1 \neq 0$, $\deg(P) \geqslant n$ et $\deg(Q) = 2n - \deg(P) \geqslant n$. Ainsi $\deg(P) = \deg(Q) = n$. Comme en plus P et Q sont unitaires, on en déduit que

$$P - 1 = \prod_{i=1}^n (X-a_i) \qquad \text{et } Q - 1 = \prod_{i=1}^n (X-a_i).$$

On devrait donc avoir $(\prod_{i=1}^n (X-a_i) + 1)^2 = \prod_{i=1}^n (X-a_i)^2 + 1$, ce qui est faux ($\prod_{i=1}^n (X-a_i) \neq 0_{\mathbb{Z}[X]}$) !
Ainsi $P-1 = 0$ ou $Q-1 = 0$, et on en déduit bien que g est irréductible dans $\mathbb{Z}[X]$.

Irréductibilité dans $\mathbb{Q}[X]$ On a le lemme suivant :
Si $P \in \mathbb{Z}[X]$ est unitaire et irréductible dans $\mathbb{Z}[X]$, alors il l'est aussi dans $\mathbb{Q}[X]$.
L'ingrédient de base de la démonstration est la notion de *contenu* d'un polynôme $P \in \mathbb{Z}[X]$: c'est le pgcd de ses coefficients, souvent noté $c(P)$. Il satisfait la relation suivante :

$$c(PQ) = c(P)c(Q).$$

Supposons que $P = QR$, avec $Q, R \in \mathbb{Q}[X]$, Q et R unitaires. En réduisant tous leurs coefficients de au même dénominateur, on peut mettre Q et R sous la forme :

$$Q = \frac{1}{a} Q_1 \qquad \text{et} \qquad R = \frac{1}{b} R_1$$

avec $a, b \in \mathbb{Z}$, $Q_1, R_1 \in \mathbb{Z}[X]$ et $c(Q_1) = 1$, $c(R_1) = 1$.
Alors $abP = Q_1R_1$, donc $c(abP) = c(Q_1)c(R_1) = 1$. Comme $ab | c(abP)$, on a $ab = \pm 1$, et en fait $P, Q \in \mathbb{Z}[X]$.

Correction de l'exercice 9 ▲

f est irréductible, donc si f, ne divise pas g, alors f et g sont premiers entre eux. Ainsi,$\exists u, v \in \mathbb{Q}[X], uf + vg = 1$.
En évaluant en α, on obtient $u(\alpha) \cdot 0 + v(\alpha) \cdot 0 = 1$ ce qui est impossible !

Correction de l'exercice 10 ▲

Supposons que la fraction soit réductible. Alors, il existe $p,q,d \in \mathbb{Z}$ tels que

$$\begin{cases} 11n+2m & = pd \\ 18n+5m & = qd \end{cases}$$

On en déduit que

$$\begin{cases} 19n & = 5pd-2qd \\ 19m & = -18pd+1qd \end{cases}$$

En particulier, $d|19n$ et $d|19m$. Si $d \neq 19$, on a $\mathrm{pgcd}(n,m) \neq 1$. Si $d = 19$, alors

$$\begin{cases} n & = 5p-2q \\ m & = -18p+1q \end{cases} \tag{1}$$

Réciproquement, si $\mathrm{pgcd}(n,m) \neq 1$ ou si n,m sont de la forme donnée par (1), alors la fraction est réductible.

Correction de l'exercice 11 ▲

Soit $d = \mathrm{pgcd}(m,n)$. Notons $n = dn'$ et $m = dm'$. Alors $X^n - 1 = (X^d)^{n'} - 1$. Or $(Y-1)|Y^{n'}-1$ donc $(X^d-1)|(X^n-1)$. De même, $(X^d-1)|(X^m-1)$, et donc $(X^d-1)|\,\mathrm{pgcd}(X^n-1,X^m-1)$.
Par ailleurs, soit $D = \mathrm{pgcd}(X^n-1,X^m-1)$. Les racines de D dans $\mathbb{C}$ sont des racines à la fois n-iéme et m-ième de 1, qui sont touts simples : elles sont donc de la forme $\omega = e^{i2\pi\alpha}$ où $\alpha = \frac{k}{n} = \frac{k'}{m}$. Ainsi $km' = k'n'$. On a $\mathrm{pgcd}(m',n') = 1$, donc par le théorème de Gauss, on en déduit que k' est un multiple de m', soit $\frac{k'}{m} = \frac{k''}{d}$, et ω est donc une racine d-ième de 1. On en déduit que $D|X^d-1$, et finalement :

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

Correction de l'exercice 12 ▲

Utiliser l'algorithme d'Euclide. (on travaille dans $\mathbb{Z}/2\mathbb{Z}$).

$$\begin{aligned} x^5+x^4+1 &= (x^4+x^2+1)(x+1)+x^3+x^2+x \\ x^4+x^2+1 &= (x^3+x^2+x)(x+1)+x^2+x+1 \\ x^3+x^2+x &= (x^2+x+1)x+0 \end{aligned}$$

Donc $\mathrm{pgcd}(x^5+x^4+1,x^4+x^2+1) = x^2+x+1$, et

$$\begin{aligned} x^2+x+1 &= (x^4+x^2+1)+(x^3+x^2+x)(x+1) \\ &= (x^4+x^2+1)+\big((x^5+x^4+1)+(x^4+x^2+1)(x+1)\big)(x+1) \\ &= (x^4+x^2+1)(1+(x+1)^2)+(x^5+x^4+1)(x+1) \\ &= (x^4+x^2+1)(x^2)+(x^5+x^4+1)(x+1) \end{aligned}$$

De même, $\mathrm{pgcd}(x^5+x^3+x+1,x^4+1) = x^3+1$ et $x^3+1 = (x^5+x^3+x+1)+(x^4+1)x$.

Correction de l'exercice 13 ▲

Dans $\mathbb{Z}/3\mathbb{Z}$: $\mathrm{pgcd}(x^4+1,x^3+x+1) = x^2+x-1$.
Dans $\mathbb{Z}/5\mathbb{Z}$: $\mathrm{pgcd}(x^4+1,x^3+x+1) = 1$.

Correction de l'exercice 14 ▲

Sur $\mathbb{Z}[X]$, $\text{pgcd}(x^4+x^3-3x^2-4x-1, x^3+x^2-x-1) = 1$.

Correction de l'exercice 15 ▲

1. P est primitif, 2 divise tous les coefficients de P sauf le dominant, et 4 ne divise pas le terme constant : d'après le critère d'Eisenstein, on en déduit que P est irréductible dans $\mathbb{Z}[x]$ (puis dans $\mathbb{Q}[x]$ car il est unitaire...).
2. On peut appliquer le même critère, avec 3 cette fois.
3. f est primitif, et sa réduction modulo 2 est irréductible. Donc f est irréductible dans $\mathbb{Z}[x]$.
4. $f(x+1) = \sum_{k=1}^{p} C_p^k x^{k-1}$. Or $p | \frac{p!}{k!(p-k)!}$ (car p apparaît au numérateur, tandis que tous les facteurs du dénominateur sont $< p$; comme p est premier, ils sont donc premiers avec p). De plus $C_p^1 = p$, donc p^2 ne divise pas le terme constant de $f(x+1)$. D'après le critère d'Eisenstein, $f(x+1)$ est irréductible, et donc f aussi.

Correction de l'exercice 16 ▲

Soit $P = x^2 - x + 1$. Si P a une factorisation non triviale, P est divisible par un polynôme de degré 1, et comme P est unitaire, ce diviseur peut être choisi unitaire : on en déduit que P a une racine. On calcule $P(a+bi\sqrt{3}) = (a^2 - 3b^2 - a + 1) + (2ab - b)i\sqrt{3}$. Comme $1/2 \notin A = \mathbb{Z}[i\sqrt{3}]$, $2a - 1 \neq 0$, donc si $P(a+bi\sqrt{3}) = 0$, alors $b = 0$, et $P(a) = 0$. Mais $x^2 - x + 1$ est primitif et se réduction modulo 2 est irréductible, donc il est irréductible sur $\mathbb{Z}[x]$. En particulier il n'a pas de racine dans $\mathbb{Z}$. On en déduit que P n'a pas de racine sur A, et est donc irréductible.

Soit $K = \text{frac}(A) = \mathbb{Q}[i\sqrt{3}]$. On a $P(\frac{1+i\sqrt{3}}{2}) = 0$ donc P a une racine dans K, donc P est réductible sur K.

Correction de l'exercice 17 ▲

Si P a une racine α dans $\mathbb{Z}$, alors $P(\alpha) = 0$, et en considérant la réduction modulo n, $\bar{P}(\bar{\alpha}) = 0$, donc $\bar{P}$ a une racine dans $\mathbb{Z}/n\mathbb{Z}$ pour tout n.

1. Si $P(0)$ et $P(1)$ sont impairs, $\bar{P}(\bar{0}) = \bar{1}$ et $\bar{P}(\bar{1}) = \bar{1}$, donc $\bar{P}$ n'a pas de racine sur $\mathbb{Z}/2\mathbb{Z}$. Donc P n'a pas de racine sur $\mathbb{Z}$.
2. Si n ne divise aucun des $P(0), \dots, P(n-1)$, alors $\bar{P}(\bar{0}) \neq 0, \dots, \bar{P}(\overline{n-1}) \neq 0$, donc $\bar{P}$ n'a pas de racine sur $\mathbb{Z}/n\mathbb{Z}$. Donc P n'a pas de racine sur $\mathbb{Z}$.

Correction de l'exercice 18 ▲

1. $(X - \frac{a}{b}) | P$ donc $\exists Q \in \mathbb{Q}[x]$, $P = (x - \frac{a}{b})Q = (bx - a)\frac{Q}{b}$. En réduisant tous les coefficients de Q au même dénominateur, on peut mettre Q sous la forme : $Q = \frac{1}{m}Q_1$, avec $Q_1 \in \mathbb{Z}[X]$ primitif. Alors $bdP = (bx - a)Q_1$. En considérant les contenus de ces polynômes, on a $c(bx - a) = \text{pgcd}(a, b) = 1$, $c(Q_1) = 1$ donc $c(bdP) = bd\,c(P) = 1$. Ainsi $bd = \pm 1$, et $(bx - a) | P$.
2. On considère par exemple les cas $k = 0, \dots, 3$. (Pour $k = 2$, on constate que $P(2) = 0$: on peut diviser P par $(X - 2)$ et déterminer les trois racines complexes de P...). On obtient que

$$\begin{array}{ccc} (*) & a|14 & (k=0), \\ (**) & (a-b)|4 & (k=1), \\ (***) & (a-3b)|2^3 5 & (k=3). \end{array}$$

Au passage On peut remarquer que si $\alpha \leqslant 0$, $P(\alpha) < 0$, donc on peut supposer $a > 0$ et $b > 0$.

— Si $a=1$: $(**) \Rightarrow b \in \{2,3,5\}$. Aucune de ces possibilités n'est compatible avec $(***)$.

— Si $a=2$: $(**) \Rightarrow b \in \{1,3,4,6\}$. Comme $\text{pgcd}(a,b)=1$, 4et 6 sont exclus. 3 n'est pas compatible avec $(***)$. Pour 2, on vérifie que $P(2)=0$.

— Si $a=7$: $(**) \Rightarrow b \in \{3,5,9,11\}$. Mais aucune de ces solution ne convient.

— Si $a=14$: $(**) \Rightarrow b \in \{10,12,16,18\}$ mais $\text{pgcd}(a,b)=1$ exclu toutes ces possibilités.

Finalement, 2 est la seule racine rationnelle de P.

Correction de l'exercice 19 ▲

1. Notons $P=\sum_{i=0}^{d} a_i X^i$. Dans le calcul de $P(n+km)$, en développant tous les termes $(n+km)^i$ à l'aide du binôme, on obtient que $P(n+km)=\sum_{0\leqslant j\leqslant i\leqslant d} a_i C_i^j n^j (km)^{i-j} = P(n)+mN$ où $N=\sum_{0\leqslant j<i\leqslant d} a_i C_i^j n^j (km)^{i-j} - 1 \in \mathbb{Z}$. Donc $m|P(n+km)$.
2. Supposons qu'un tel polynôme existe : soit $m=P(0)$. $\forall k \in \mathbb{Z}, m|P(km)$. Comme $P(km)$ est premier, on en déduit que $P(km)=\pm m$. Ceci est en contradiction avec $\lim_{k\to+\infty} P(km)=\pm\infty$.
